Agenda
Reliability and Security Technical Committee

September 20, 2023 | 8:30 a.m. – 4:00 p.m. Mountain
Hybrid

WECC
155 North 400 West, Suite 200
Salt Lake City, Utah 84103

Join WebEx

Call to Order

NERC Antitrust Compliance Guidelines and Public Announcement

Introduction and Chair's Remarks

Agenda

1. **Administrative items**
   a. Arrangements
      Announcement of Quorum
   b. Reliability and Security Technical Committee (RSTC) Membership 2022-2025*
      i. RSTC Roster
      ii. RSTC Organization
      iii. RSTC Charter
      iv. Participant Conduct Policy

Consent Agenda

2. **Consent Items* – Approve**
   a. June 20-22, 2023 RSTC Meeting Minutes
   b. Event Analysis Subcommittee Scope

Regular Agenda

3. **Remarks and Reports**
   a. Subcommittee Reports*
   b. RSTC Work Plan
   c. Report of August 16, 2023 Member Representatives Committee (MRC) Meeting and August 17, 2023 Board of Trustees Meeting
4. **Nominating Subcommittee Member Election* – Approve -** Chair Hydzik
5. **RSTC SAR Development Process – Approve –** Rich Hydzik, RSTC Chair

6. **EMP Working Group Disbandment – Accept –** Aaron Shaw, AEP
7. **Event Analysis Process – Accept –** James Hanson, EAS Vice Chair | Srinivas Kappagantula, Sponsor
8. **White Paper: Grid Forming Functional Specifications for BPS-Connected Battery* – Approve –** Julia Matevosyan IRPS Chair | Jody Green, Sponsor
9. **White Paper: Bulk Electric System Operations in Cloud – Approve –** Larry Collier, NERC Staff | Marc Child, Sponsor
10. **Frequency Response Annual Analysis – Accept –** Greg Park, RS Chair | Jessica Harris, NERC Staff | Rich Hydzik, Sponsor
11. **Primary Frequency Control Reliability Guideline* – Approve –** Greg Park, RS Chair | Rich Hydzik, Sponsor
12. **White Paper: Privacy and Security Impacts of DER and DER Aggregators – Approve –** Shayan Rizvi, SPIDERWG Chair | Wayne Guttormson, Sponsor
13. **SARs for Revisions to EOP-004 Standard* – Endorse –** Shayan Rizvi, SPIDERWG Chair | Wayne Guttormson, Sponsor
14. **Support Study: Reviewing Fuel Availability for Regional Flexible Resources to Support System Variability * – Approve -** Mike Knowland, Chair EGWG
15. **Reliability Guideline: Fuel Assurance and Fuel-Related Reliability Risk Analysis for the Bulk Power System* – Approve –** Mike Knowland, Chair EGWG | Venona Greaff, Sponsor
16. **Product Security Sourcing Guide and Reference Guide Security Guideline* – Accept to Posting for 45-day Comment Period –** Tobias Whitney, SCWG | Christine Ericson, Sponsor
17. **Inverter-Based Resources Registration – Information –** Candice Castaneda/Jim Stuart NERC Staff
18. **Transmission Planning Energy Scenarios SAR – Information –** Mohamed Osman, NERC Staff
19. **Interregional Transfer Capability Study – Information –** John Moura, NERC Staff
20. **RSTC Charter Revisions* – Request RSTC Comments –** Candice Castaneda, NERC Staff
21. **Chair's Closing Remarks and Adjournment**

*Background materials included.

Event Analysis Subcommittee Scope Document

Action

Approve

Background

The Event Analysis Subcommittee (EAS) is seeking approval for the EAS Scope Document. This scope has undergone updates as part of the periodic review process. The EAS has endorsed the current scope in advance of requesting RSTC approval.

Summary

This EAS Scope document reflects several notable enhancements intended to provide clarity and increase participation by industry stakeholders. These enhancements include, but are not limited to, the following:

- Update the Functions and Deliverables sections.
- Revise the Membership section to allow for a maximum of five at-large members based on their industry expertise.
- Revise the Membership section to allow for the chair of each EAS sub-group (i.e. Energy Management System Working Group and Failure Modes and Mechanisms Task Force) to be voting members of the EAS for the duration of their term.
- Add a Proxy section.
- Add provisions to allow, but not require, the formation of an EAS Executive Committee.
- Update the Meeting Procedures section to add meeting procedure documents (i.e. Antitrust Compliance Guidelines, Participant Conduct Policy, Robert’s Rules of Order).
- Update the Meeting Procedures section to provide clarity regarding EAS voting procedures.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Event Analysis Subcommittee Scope

Purpose

The Event Analysis Subcommittee (EAS) assists the NERC Reliability and Security Technical Committee (RSTC) in enhancing Bulk Power System (BPS) reliability by implementing the goals and objectives of the RSTC Strategic Plan.

The EAS is a cross-functional group of industry experts that will support and maintain a cohesive and coordinated event analysis (EA) process across North America with industry stakeholders. The EAS will support development of lessons learned, promote industry-wide sharing of event causal factors, and assist NERC in implementation of related initiatives to lessen reliability risks to the BPS.

Functions

1. The EAS, in coordination with NERC Staff, will:
    a. Support the periodic review and EAS acceptance of the ERO Event Analysis Process document.
    b. Support, recruit, and encourage the development and publishing of Lessons Learned.
    c. Identify potential improvements to event analysis reporting.
    d. Provide feedback to and solicit feedback from industry stakeholders on the ERO Event Analysis Process.
2. The EAS will coordinate the sharing of information with the NERC RSTC and its subcommittees/working groups. The EAS will:
    a. Facilitate registered entity event analysis presentations at EAS and RSTC meetings.
    b. Provide information regarding the development and publishing of Lessons Learned.
    c. Provide collaboration necessary to communicate BPS reliability trends identified through the ERO Event Analysis Process.
3. The EAS, in coordination with NERC subcommittees and working groups, will share information, identify trends, and make recommendations to the industry related to reliability risk topics that could include:
    a. Human and Organizational Performance
    b. Need for and development of training
    c. Lessons Learned
    d. Good industry practices and recommendations
    e. Other related topics as needed.

4. The EAS will partner with Regional Entities, registered entities and other industry forums to:
    a. Obtain input of Regional Entity personnel and reliability stakeholder groups as resources to the EAS, leveraging their experience and knowledge.
    b. Assist in the identification of BPS reliability risks.
    c. Recommend enhancement to existing Reliability Standards or development of new Reliability Guidelines or Reliability Standards where gaps are identified.
    d. Look for opportunities to assess the value of published Lessons Learned.

Deliverables

- Conduct a review of the ERO Event Analysis Process document every three years or as needed.
- Recommend the need for and participate in the development of industry training.
- Acceptance of Lessons Learned for publishing by the ERO.
- Prepare and facilitate Lessons Learned webinars in coordination with the ERO.
- Develop and review of Reliability Guidelines and Technical Reference Documents.
- Support the identification of significant risks to BPS reliability and the need for NERC Alerts.
- Provide updates to the RSTC as needed.
- Support the development of NERC’s annual State of Reliability Report in coordination with the Performance Analysis Subcommittee (PAS).
- Provide information and recommendations related to the ERO Event Analysis Process.
- Support and coordinate with other NERC subcommittees and their subgroups.

Reporting

The EAS reports to the RSTC, and shall maintain communications with the RSTC, EAS Sponsor, and other groups as necessary on relevant issues. The EAS will regularly submit a work plan for approval of tasks. The EAS will review its Scope every three years or as otherwise needed.

All RSTC approved and/or assigned work products intended for industry use (such as a Scope document, Work Plans, Reliability Guidelines, Reference Documents, Compliance Implementation Guidance, reports, whitepapers, etc.) should be approved by the RSTC.

The EAS will report to the RSTC for the completion of work associated with the scope items outlined above, and final work products of the EAS will be reviewed and considered by the RSTC and or the NERC Board of Trustees. The EAS chair will periodically apprise the RSTC on the subcommittee’s activities, assignments, and recommendations.

Officers

The RSTC Chair appoints/approves the EAS officers (Chair and Vice Chair) for a specific term (generally two-years). The subcommittee officers may be reappointed for additional terms. The vice chair is considered an important part of succession planning with the anticipation that the vice chair will most often assume the position of subcommittee chair for the next term. The EAS may recommend officer candidates for the RSTC Chair's consideration following a supporting motion.

The subcommittee Chair or Vice chair should attend the regular RSTC meetings to report on assignments, or provide a summary report of the group's activities, and advise the RSTC on important issues as needed.

The EAS officers are considered members of the EAS and may vote.

Membership

The EAS shall have sufficient expertise and diversity to be able to speak knowledgably for the industry and provide meaningful and useful guidance to assist the industry in the carrying out of its reliability responsibilities. NERC segment membership balance resides with the parent committee (RSTC), allowing the subcommittee to focus on the expertise required to carry out its functions.

EAS members must be committed to their service on the subcommittee. Members must prepare for and actively participate in all subcommittee meetings in person or on conference calls. As needed, members must also write and review draft reports, serve on standard authorization request and standard drafting teams if selected. Members should be prepared to ascend to an EAS leadership position if needed.

The voting members of the EAS will consist of:

- One (1) voting member from each of the Regional Entities, approved by the RSTC.
- One (1) voting member from registered entities within each of the Regions to represent industry stakeholder interests
- A maximum of (5) at-large members with industry expertise that could include BPS planning, protection & control, operations, and/or security.
- The Chair of each of the EAS sub-groups (i.e. EMSWG, FMMTF) are voting members of the EAS by default for the duration of their term.

New members will be nominated by a current EAS or RSTC member and must be approved by the EAS.

Members must have a signed NERC Non-Disclosure Agreement in effect.

Proxies

A voting member may select a proxy who attends and votes during all or a portion of a committee meeting in lieu of a voting member, provided that the absent voting representatives notifies the EAS chair, vice chair, or secretary of the proxy. A proxy may not be given to another EAS member. A proxy must meet the EAS's membership eligibility requirements, including affiliate restrictions.

To permit time to determine a proxy's eligibility, all proxies must be submitted to the secretary in writing prior to the meeting (electronic transmittal is acceptable) for approval by the chair. Any proxy submitted after that time will be accepted at the chair's discretion.

Non-voting members — Guests and Observers

EAS meetings are open to others who wish to attend as a guest of the subcommittee. The chair will provide guests and observers the opportunity to contribute to the subcommittee's discussions, provided the subcommittee's voting members have sufficient time to:

- Complete the debate of their motions, and
- Complete the meeting agenda.

Replacing Members

The subcommittee may request a replacement for a member that repeatedly fails to attend regularly scheduled meetings without sending a proxy.

Executive Committee

The EAS may form an Executive Committee. The Executive Committee of the EAS is empowered by the EAS to act on its behalf between subcommittee meetings on matters where urgent actions are crucial and full subcommittee discussion is not practical. Ultimate EAS responsibility resides with its full membership whose decisions cannot be overturned by the Executive Committee, but retains the authority to ratify, modify or annul Executive Committee actions. The Executive Committee will be comprised of the EAS Chair, Vice Chair, and three additional EAS voting members that are selected by the EAS Chair and may not be from the same Region. The Executive Committee members will serve for a two year term and may serve for additional terms.

Meeting Procedures

The EAS follows the meeting procedures in accordance with the following documents:

- NERC Antitrust Compliance Guidelines,
- Participant Conduct Policy Applicable to NERC Operating Committee and its Subgroups, and
- Robert's Rules of Order, Newly Revised.

The desire is to strive for consensus in normal EAS business. If consensus cannot be achieved, the EAS will hold a vote as noted below. If strong minority opinions exist, those opinions may be documented as a minority dissenting opinion in the meeting minutes.

- Quorum: 50% of subcommittee members eligible to vote.
- Actions requiring a vote shall require a quorum and a simple majority vote of those members present or by unanimous consent.
- All other procedures follow those of the RSTC Charter and Standard Operating Procedure.

Confidential Sessions

The chair of the subcommittee may limit attendance at a meeting or portion of a meeting, based on confidentiality of the information to be disclosed at the meeting. Such limitations should be applied sparingly and on a non-discriminatory basis as needed to protect information that is sensitive to one or more parties.

Subgroups

The EAS may form working groups and task forces as needed to assist the subcommittee in carrying out standing or ad hoc assignments. Task group chairs (or delegates) are expected to attend the regular subcommittee meetings to report on assignments or provide a summary report of the group's activities.

Meetings

Four to six open meetings per year, or as needed, with supplemental telephone conferences.

Periodic Review

The EAS Scope should be reviewed at least every three years but may be revised more frequently if needed.

Version	Date	Reviewers/Approval	Revision Description
1.0	6/19/2013	Developed by: Event Analysis Working Group Approved by the OC: September 10, 2013	Transitioned the EAWG into the EAS.
1.1	10/10/2013	Developed by: Event Analysis Subcommittee Approved by the OC: December 10 2013	Updated EAS Scope to reflect changes in the OC Strategic Plan.
1.2	6/4/2018	Developed by: Event Analysis Subcommittee Approved by the OC: September 11, 2018	Updated EAS Scope to reflect seven NERC Regions due to the dissolution of SPP RE.
1.3	02/09/2021	Developed by: Event Analysis Subcommittee Approved by the RSTC: March 3, 2021	Updated EAS Scope to reflect transformation of the RSTC
1.4	xx/xx/2023	Developed by: Event Analysis Subcommittee Approved by the RSTC:	Updated EAS Scope to reflect changes to EAS membership and other enhancements

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Event Analysis Subcommittee Scope

Purpose

The Event Analysis Subcommittee (EAS) assists the NERC Reliability and Security Technical Committee (RSTC) in enhancing ~~Bulk Electric System (BES)~~Bulk Power System (BPS) reliability by implementing the goals and objectives of the RSTC Strategic Plan.

The EAS is a cross-functional group of industry experts that will support and maintain a cohesive and coordinated event analysis (EA) process across North America with industry stakeholders. The EAS will support development of lessons learned, promote industry-wide sharing of event causal factors, and assist NERC in implementation of related initiatives to lessen reliability risks to the ~~BES~~BPS.

Functions

1. The EAS, in coordination with NERC Staff, will:
    a. Support the ~~Manage~~ periodic review and EAS acceptance of the ERO Event Analysis Process document~~ updates and annual review~~.
    b. ~~Manage and coordinate~~Support, recruit, and encourage the development and publishing of Lessons Learned.
    c. Identify potential improvements to event analysis reporting.
    ~~d.~~ Provide feedback to and solicit feedback from industry stakeholders on the ~~the~~ ERO Event Analysis Process~~ topics~~.
    ~~e.~~d. ~~Solicit feedback from industry stakeholders to improve the ERO Event Analysis Process.~~
2. ~~To~~ The EAS will ~~facilitate~~ coordinate the sharing of~~ EA~~ information with the NERC RSTC and its subcommittees/working groups.~~,~~ ~~the~~ The EAS will:
    a. Facilitate registered entity event analysis presentations at EAS and RSTC meetings.
    b. Provide information regarding the~~status of~~ ~~and direction on implementation~~develop~~ing~~ment and publishing of Lessons Learned.
    c. Provide collaboration necessary~~Collaborate~~ to ~~Pprovide~~communicate BPS reliability trends~~ing~~ ~~updates~~ identified through the ERO Event Analysis Process.~~ as needed~~~~when needed and/or appropriate.~~
3. The EAS, in coordination with NERC subcommittees and working groups, will share information, identify trends, ~~through analysis of events,~~ and make recommendations to the industry related to reliability risk topics that could include~~which address~~:
    ~~a. Reliability risks~~

~~b.~~a. Human and Organizational ~~p~~Performance

~~c.~~b. Need for and development of training

~~d.~~c. Lessons Learned

d. Good industry practices and recommendations

e. Other related topics as needed.

4. The EAS will partner with Regional Entities, registered entities and other industry forums to:
   a. Obtain input of Regional Entity personnel and reliability stakeholder groups as resources to the EAS, leveraging their experience and knowledge.
   b. ~~Address~~ Assist in the identification of BPS reliability ~~issues~~ risks~~s and trends~~ ~~informed by event reportingfrom reported events~~.
   c. ~~Based on Lessons Learned and trends drawn from events,~~ R~~r~~ecommend enhancement to existing Reliability Standards or development of new Reliability Guidelines or Reliability Standards where gaps are identified.
   ~~c.~~d. Look for opportunities to assess the value of published Lessons Learned.
   ~~d. Annually survey the Regional Entities to assess the value of published Lessons Learned.~~

Deliverables

- Conduct ~~an annual~~a review of the ERO Event Analysis Process document every three years or as needed.~~.~~
- Recommend the need for and participate in the development of industry training.
- ~~Publish~~ Acceptance of Lessons Learned for publishing by the ERO.
- Prepare and facilitate Lessons Learned webinars in coordination with the ERO.
- Develop and review of Reliability Guidelines ~~as directed by the RSTC~~and Technical Reference Documents.
- ~~Identify~~ Support the identification of significant risks to BPS reliability and the need for NERC Alerts.
- Provide updates to the RSTC as needed.~~.~~
- ~~Provide input to the NERC Performance Analysis Subcommittee's (PAS) annual~~Support the development of NERC's annual State of Reliability Report in coordination with the Performance Analysis Subcommittee (PAS).
- Provide ~~event~~ information and recommendations related to the ERO Event Analysis Process.
- Support and coordinate with other NERC subcommittees and their subgroups.

Reporting

The EAS reports to the RSTC, and shall maintain communications with the RSTC, EAS Sponsor, and other groups as necessary on relevant issues. The EAS will regularly submit a work plan for approval of tasks. The EAS will review its ~~scope and work plan regularly~~Scope every three years or as otherwise needed.

All RSTC approved and/or assigned work products ~~(with the exception of Lessons Learned and Failure Modes & Mechanisms)~~ intended for industry use (such as a Scope document, Work Plans, Reliability Guidelines, Reference Documents, Compliance Implementation Guidance, reports, whitepapers, etc.) should be approved by the RSTC.

The EAS will report to the RSTC for the completion of work associated with the scope items outlined above, and final work products of the EAS will be reviewed and considered by the RSTC and or the NERC Board of Trustees. The EAS chair will periodically apprise the RSTC on the subcommittee’s activities, assignments, and recommendations.

Officers

The RSTC Chair appoints/approves the EAS officers (Chair and Vice Chair) for a specific term (generally two-years). The subcommittee officers may be reappointed for additional terms. The vice chair is considered an important part of succession planning with the anticipation that the vice chair will most often ~~be appointed~~assume the position ~~as~~ of subcommittee chair for the next term. The EAS may recommend officer candidates for the RSTC Chair's consideration following a supporting motion.

The subcommittee Chair or Vice chair should attend the regular RSTC meetings to report on assignments, or provide a summary report of the group's activities, and advise the RSTC on important issues as needed.

The EAS officers are considered members of the EAS and may vote.

Membership

The EAS shall have sufficient expertise and diversity to be able to speak knowledgably for the industry and provide meaningful and useful guidance to assist the industry in the carrying out of its reliability responsibilities. NERC segment membership balance resides with the parent committee (RSTC), allowing the subcommittee to focus on the expertise required to carry out its functions.

EAS members must be committed to their service on the subcommittee. Members must prepare for and actively participate in all subcommittee meetings in person or on conference calls. As needed, members must also write and review draft reports, serve on standard authorization request and standard drafting teams if selected. Members should be prepared to ascend to an EAS leadership position if needed.

The voting members of the EAS will consist of:

- One (1) voting member from each of the Regional Entities, approved by the RSTC.
- One (1) voting member ~~from each of the Regions to represent industry stakeholder interests. Members may be recommended by the EAS and will be approved by the RSTC~~from registered entities within each of the Regions to represent industry stakeholder interests
- ~~.~~A maximum of (5) at-large members with industry expertise that could include BPS planning, protection & control, operations, and/or security.
- The Chair of each of the EAS sub-groups (i.e. EMSWG, FMMTF) are voting members of the EAS by default for the duration of their term.

New members will be nominated by a current EAS or RSTC member and must be approved by the EAS.

Members must have a signed ~~organizational~~NERC Non-Disclosure Agreement ~~on file~~in effect.

  - ~~These members must have a signed Non-Disclosure Agreement on file in order to participate in the confidential sessions described below.~~

Proxies

A voting member may select a proxy who attends and votes during all or a portion of a committee meeting in lieu of a voting member, provided that the absent voting representatives notifies the EAS chair, vice chair, or secretary of the proxy. A proxy may not be given to another EAS member. A proxy must meet the EAS's membership eligibility requirements, including affiliate restrictions.

To permit time to determine a proxy's eligibility, all proxies must be submitted to the secretary in writing prior to the meeting (electronic transmittal is acceptable) for approval by the chair. Any proxy submitted after that time will be accepted at the chair's discretion.

Non-voting members — Guests and Observers

EAS meetings are open to others who wish to attend as a guest of the subcommittee. The chair will provide guests and observers the opportunity to contribute to the subcommittee's discussions, provided the subcommittee's voting members have sufficient time to:

- Complete the debate of their motions, and
- Complete the meeting agenda.

Replacing Members

The subcommittee may request a replacement for a member that repeatedly fails to attend regularly scheduled meetings without sending a proxy.

Executive Committee

The EAS may form an Executive Committee. The Executive Committee of the EAS is empowered by the EAS to act on its behalf between subcommittee meetings on matters where urgent actions are crucial and full subcommittee discussion is not practical. Ultimate EAS responsibility resides with its full membership whose decisions cannot be overturned by the Executive Committee, but retains the authority to ratify, modify or annul Executive Committee actions. The Executive Committee will be comprised of the EAS Chair, Vice Chair, and three additional EAS voting members that are selected by the EAS Chair and may not be from the same Region. The Executive Committee members will serve for a two year term and may serve for additional terms.

Meeting Procedures

The EAS follows the meeting procedures in accordance with the following documents:

- NERC Antitrust Compliance Guidelines,
- Participant Conduct Policy Applicable to NERC Operating Committee and its Subgroups, and
- Robert's Rules of Order, Newly Revised.

The desire is to strive for consensus in normal EAS business. If consensus cannot be achieved, the EAS will hold a vote as noted below. If ~~any~~ strong minority opinions ~~develop~~exist, those opinions may be documented ~~as desired by the minority and forwarded to the RSTC Chair for future meeting consideration~~as a minority dissenting opinion in the meeting minutes.

- Quorum: 50% of subcommittee members eligible to vote.
- Actions requiring a vote shall require a quorum and a simple majority vote of those members present or by unanimous consent.
- All other procedures follow those of the RSTC Charter and Standard Operating Procedure.
- ~~Quorum: 50% of subcommittee members eligible to vote.~~
- ~~Actions requiring a vote shall require a quorum and a simple majority vote of those members present.~~
- ~~All other procedures follow those of the RSTC Charter and Standard Operating Procedure.~~

Confidential Sessions

The chair of the subcommittee may limit attendance at a meeting or portion of a meeting, based on confidentiality of the information to be disclosed at the meeting. Such limitations should be applied sparingly and on a non-discriminatory basis as needed to protect information that is sensitive to one or more parties.

Subgroups

The EAS may form working groups and task forces as needed to assist the subcommittee in carrying out standing or ad hoc assignments. Task group chairs (or delegates) are expected to attend the regular subcommittee meetings to report on assignments or provide a summary report of the group's activities.

Meetings

Four to six open meetings per year, or as needed, with supplemental telephone conferences.

Periodic Review

The EAS Scope should be reviewed at least every three years but may be revised more frequently if needed.

Version	Date	Reviewers/Approval	Revision Description
1.0	6/19/2013	Developed by: Event Analysis Working Group Approved by the OC: September 10, 2013	Transitioned the EAWG into the EAS.
1.1	10/10/2013	Developed by: Event Analysis Subcommittee Approved by the OC: December 10 2013	Updated EAS Scope to reflect changes in the OC Strategic Plan.

1.2	6/4/2018	Developed by: Event Analysis Subcommittee Approved by the OC: September 11, 2018	Updated EAS Scope to reflect seven NERC Regions due to the dissolution of SPP RE.
1.3	02/09/2021	Developed by: Event Analysis Subcommittee Approved by the RSTC: March 3, 2021	Updated EAS Scope to reflect transformation of the RSTC
1.4	x~~X~~x/xx/2023	Developed by: Event Analysis Subcommittee Approved by the RSTC:	Updated EAS Scope to reflect changes to EAS membership and other enhancements

RSTC Status Report 6 GHZ Task Force (6GHZTF)

Chair: Jennifer Flandermeyer
Vice Chair: Larry Butts
September 20-21, 2023

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Purpose: Provide to the RSTC: determine scope of issue, gather information related to risk of harmful interference in the 6 GHz spectrum, evaluate options for industry outreach, and recommendations related to the issue

Items for RSTC Approval/Discussion:

- **Approve**: *Interference Preparedness Whitepaper*

Recent Activity

Upcoming Activities

- Conduct a webinar to raise awareness for the industry
- Support development of a Level 2 Alert that encompasses the above recommendations as well as recommendations from the extent of condition whitepaper;
- Develop transition plan for the 6GHZTF (potential Telecom WG or disband)

Workplan Status *(6-month look-ahead)*

Milestone	Status	Comments
Publish Extent of Condition Whitepaper	🟢	Completed
Publish 6GHZ Interference Preparedness Whitepaper	🟢	Approval phase Q3/2023
Develop materials for Webinar	🟢	Planning phase Q4/2023
Support the NERC Level 2 Alert	🟢	Planning phase Q4/2023
Develop Transition Plan to Potential TWG or Disband	🟢	Q4/2023

RSTC Status Report – Event Analysis Subcommittee (EAS)

Chair: Chris Moran
Vice-Chair: James Hanson
September 19-21, 2023

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Purpose: The EAS will support and maintain a cohesive and coordinated event analysis (EA) process across North America with industry stakeholders. EAS will develop lessons learned, promote industry-wide sharing of event causal factors and assist NERC in implementation of related initiatives to reduce reliability risks to the Bulk Electric System.

Items for RSTC Action:

- Approve Event Analysis Process document
- Approve Event Analysis Subcommittee Scope document

Recent 2023 Activity

- Ongoing Development of Lessons Learned
- Endorsed ERO Event Analysis document
- Reliability Guideline review completed; Guideline posted
- Endorsed EAS Scope document
- Winter Weather Webinar
- June in-person joint meeting w/ EAS, EMSWG, FMMTF, & SPCWG

Ongoing & Upcoming Activities

- ERO EAP Periodic Review
- EAS Scope Periodic Review
- Develop EAP Industry Webinar
- Winter Weather Webinar
- Monitoring & Situational Awareness Conference (EMSWG)
- Development of Lessons Learned
- FMMTF Development of Failure Mode & Mechanism Diagrams

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
ERO EAP Periodic Review	🟢	Completed
Event Analysis Data & Trends for 2023 SOR	🟢	Completed
Winter Weather Webinar	🟢	Upcoming Sept 2023
Lessons Learned for 2023	🟢	On-Going
11th Annual SA Conference	🟢	Upcoming Fall 2023
FMM Diagrams for 2023	🟢	On-Going

RSTC Status Report – Electric Gas Working Group (EGWG)

Chair: Mike Knowland
Vice-Chair: Daniel Farmer
September 20 - 21, 2023

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Purpose: The EGWG was formed to address fuel assurance issues as a result of the RISC identified Grid Transformation.

Items for RSTC Approval/Discussion:
N/A

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
FERC/NERC joint inquiry coordination	🟢	On track

Recent Activity

- The 45-day informal comment period ended on August 14.
- Completed addressing the industry comments during the week of August 14.

Upcoming Activity

- Develop Coordination Plan for potential electric related risks/objectives in natural gas related standards as well as follow up to complete and assess results of survey for Fuel Assurance Guideline.

RSTC Status Report – Energy Reliability Assessment Working Group (ERAWG)

Chair: Mike Knowland
September 20 - 21, 2023

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Purpose: The ERAWG is tasked with assessing risks associated with unassured energy supplies stemming from the variability and uncertainty from renewable energy resources, limitations of the natural gas system and transportation procurement agreements, and other energy-limitations that inherently exist in the future resource mix.

Recent Activity:

- The Tiger Team started to draft Volume 2, a technical paper that documents detailed scenarios on conducting energy reliability assessments in the operations time horizon and the planning time horizon.

Items for RSTC Approval/Discussion:

- *None.*

Upcoming Activity:

- Review and comment on draft requirements from SDT.
- Provide technical assistance for the SDT, as needed.
- Continue the Tiger team meetings on drafting Volume 2.
- The next ERAWG team call is scheduled for October 4, 2023.

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Supporting SDT for Project 2022-03.	🟢	On track.
The Tiger team is currently drafting the Volume 2 document on conducting an energy reliability assessment.	🟢	On track.

RSTC Status Report: Facility Ratings Task Force (FRTF)

Chair: Tim Ponseti
Vice-Chair: Jennifer Flandermeyer

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Purpose: The NERC RSTC Facility Ratings Task Force (FRTF) will address risks and technical analyses associated with Facility Ratings.

Items for RSTC Approval/Discussion:
- None

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Item 1 – Implementation Guidance on sustaining accurate facility Ratings	🟢	In Progress
Item 2 – Support Project 2021-08 Modifications to FAC-008 SDT	🟢	In Progress
Item 3 – Whitepaper on Sampling for Facility Rating programs	🟢	In Progress

Recent Activity
- Hold regular leadership meetings to discuss progress and strategy on deliverables.
- All three sub-teams holding regular meetings and working on deliverables.
- Tim Ponseti and Howard Gugel presented and discussed Facility Ratings issues with the Operations Leadership Team.
- Held meeting with full task force April 28th to provide updates on the individual work plan items.

Upcoming Activity
- Sub-teams working on deliverables.
- Bi-monthly FRTF meetings to discuss progress on work plan initiatives and other relevant topics.

RSTC Status Report – Inverter-Based Resource Performance Subcommittee (IRPS)

Chair: Julia Matevosyan
Vice-Chair: Rajat Majumder

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Purpose: To explore the performance characteristics of utility-scale inverter-based resources (e.g., solar photovoltaic (PV) and wind power resources) directly connected to the bulk power system (BPS).

Items for RSTC Approval/Discussion:

- Item 22: Grid Forming White Paper

Recent Activity

- Technical Presentation on Leveraging Real-Time Simulation Technology to Accelerate EMT Simulations with Scalable RealCode Controller Integration for Advanced IBR Integration Studies
- Technical Presentation on Large System Stability Analysis and Planning Using Impedance-Based Analysis

Upcoming Activity

- Work Plan Item #8: Reliability Guideline: Recommended Approach to Interconnection Studies for BPS-Connected Inverter-Based Resources
- Work Plan Item #20: Assessment: Gap Analysis of Any IBR-Related Issues Not Addressed by NERC Standards.
- Work Plan Item #24: Commissioning Best Practices for IBRs

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Item 8 - Reliability Guideline: Recommended Approach to Interconnection Studies for BPS-Connected Inverter-Based Resources	🟢	In Progress
Item 20 - Assessment: Gap Analysis of Any IBR-Related Issues Not Addressed by NERC Standards	🟢	In Progress
Item 22 - Grid Forming White Paper	🟢	In Progress
Item 24 - White Paper: BPS-Connected IBR Commissioning Best Practices	🟢	In Progress

RSTC Status Report – Load Modeling Working Group (LMWG)

Chair: Kannan Sreenivasachar,
Vice-Chair: Robert J O'Keefe

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Purpose:
The LMWG is preparing modeling for the emerging loads and transitioning utilities from the CLOD model to the CMLD Composite Load Model.

Items for RSTC Approval/Discussion:

- **Approve**: LMWG *Work Plan*

Recent Activity

- *Sent Data Center Questionnaire*
- Created and Revised LMWG Strategy Document for Emerging Loads
- Attended LMWG Summit on Emerging Loads at BPA
- Developed Initial Draft outline for EV TRD
- *Obtained EV Forecasts*
- *Developed Electric Vehicle Charger Models*
- *Coordinated with SPIDERWG on DER Models*

Upcoming Activity

- Obtain *EV Forecasts*
- Complete EV TRD
- Revise LMWG Strategy Document for Emerging Loads as Required.
- Attend RSTC Summit
- *Develop Electric Vehicle Charger Models*
- Review Response to Data Center Questionnaire
- *Coordinate with SPIDERWG on DER Models*

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Develop Final Draft outline for EV TRD	🟢	In progress
Develop Electric Vehicle Charger Models	🟢	In progress
Data Center Modeling	🟢	In progress
Modular Implementation of the CMLD Model	🟢	In progress
Coordination with SPIDERWG on DER Models	🟢	In progress

RSTC Status Report – Performance Analysis Subcommittee (PAS)

Chair: David Penney
Vice-Chair: Heide Caswell

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed
○ Not started
🔵 Complete

Purpose: The PAS reviews, assesses, and reports on reliability of the North American Bulk Power System (BPS) based on historic performance, risk and measures of resilience.

Items for RSTC Approval/Discussion:

- N/A

Recent Activity

- Completed the 2023 State of Reliability Report.
- Presented the load loss data collection white paper at the June meeting for information.

Upcoming Activity

- Develop the Data Reporting Instructions for the load loss data collection initiative.
- Develop criteria for security metric.
- Review weighting of the Severity Risk Index (SRI) components and identify additional data inputs currently available.

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
2023 State of Reliability Report	🔵	SOR issued June 22
Load loss data Section 1600 Data Request	🟢	Begin DRI and Section 1600 data request materials for load loss data
Review proposed new metrics	🟢	Cyber and physical security metrics under development
Review SRI components	🟢	Review weighting and components

RSTC Status Report – Reliability Assessment Subcommittee (RAS)

Chair: Andreas Klaube (12/2022)
Vice-Chair: Amanda Sargent (12/2022)
September 19-21, 2023

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Purpose: The RAS reviews, assesses, and reports on the overall reliability (adequacy and security) of the BPS, both existing and as planned. The Reliability Assessment program is governed by the NERC RoP Section 800.

Recent Activity:

- RAS Meeting July 11-13: topics included: 2023 LTRA Preliminary Findings, 2023 LTRA Peer Reviews, 2023-2024 WRA Request Materials review, PAWG Work Plan Review, and the 2023 State of Reliability Report

- RAS Meeting August 30 – 31: topics included: joint session with the PAWG, RAS work plan, 2023 LTRA initial review, Energy Assessments planning, and 2023-2024 WRA planning

Items for RSTC Approval/Discussion:

- LTRA Preliminary Findings and Issues Discussion (Sept 21)

Upcoming (RSTC) Activity:

Workplan Status *(6-month look ahead)*

Milestone	Status	Comments
2023 Long-Term Reliability Assessment (LTRA)	🟢	RSTC Review planned for September 26 – October 12.
2023-2024 Winter Reliability Assessment (WRA)	🟢	RSTC Review planned for October 18 – 30.
Reliability Assessment Inputs and Grid Transformation	🟢	Coordinating with other RSTC groups/SMEs
Special Reliability Assessments Scope and Prioritization	🟢	Draft scope in development; for RSTC review and assignment to a task force

RSTC Status Report – Resources Subcommittee (RS)

Chair: Greg Park
Vice-Chair: William Henson
September 2023

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Purpose: The RS assists the NERC RSTC in enhancing Bulk Electric System reliability by implementing the goals and objectives of the RSTC Strategic Plan with respect to issues in the areas of balancing resources and demand, interconnection frequency, and control performance.

Recent Activity

- Quarterly review of interconnection performance
- Reviewed and Approved the 2023 Frequency Response Annual Analysis
- Reporting ACE and Associated Terms Standard Drafting Team – Ace Diversity Interchange will be out for informational ballot in September. SDT addressed comments from first informational ballot

Items for RSTC Approval/Discussion:

- *Reliability Guideline: Primary Frequency Control*

Upcoming Activity

- In Person/Hybrid Meetings Scheduled
  - October 25th – 26th Charleston, South Carolina. Hosted by Dominion Energy South Carolina
- Persistent High Frequency
  - EI Inadvertent Pause: All EI BA's to pause unilateral Inadvertent Payback for one month to observe effects on persistent high frequency. Likely to occur in October 2023
  - WI ATEC Pause: Based upon the results of the EI, the RS is considering a similar "pause" in the WI to determine if a common failure is occurring driving high frequency that perhaps the ATEC process is masking. Schedule: TBD

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Support ERSWG Measures 1,2,4, and 6	🟢	Periodic review and consultation with NERC staff ongoing
Reliability Guideline: Loss of Communications	🔴	Preparing for Public Comment
Reliability Guideline: Primary Frequency Control	🔴	Approval Item

RSTC Status Report – Real Time Operating Subcommittee (RTOS)

Chair: Jimmy Hartmann
Vice-Chair: Tim Beach
September 2023

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Purpose: The RTOS assists in enhancing BES reliability by providing operational guidance to industry; oversight to the management of NERC-sponsored IT tools and services which support operational coordination, and providing technical support and advice as requested.

Recent Activity

- RTOS endorsed minor updates on the following Reliability Plans due to minor updates and their three-year review:
  - MISO Reliability Plan
  - FRCC Reliability Plan
  - VACAR-S Reliability Plan
  - BCRC Reliability Plan
  - RC West Reliability Plan
- RSTC approved: :
  - Time Monitor Reference Document

Items for RSTC Approval/Discussion:

N/A

Upcoming Activity

Continued work related to the Cold Weather Report

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Monitor development of common tools and act as point of contact for EIDSN.	🟢	On-going
Frequency Monitor Reporting (Standing RTOS agenda item to discuss).	🟢	On-going
Reference Document: Time Monitor Reference Document	🟢	Complete
Reliability Guideline: Methods for Establishing IROLs	🟢	In-progress

RSTC Status Report – Supply Chain Working Group (SCWG)

Chair: Christopher Strain
Vice-Chair: Dr. Tom Duffey
September 2023

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Purpose: To Identify known supply chain risks and address through guidance documentation or other appropriate vehicles. Partner with National Laboratories to address supply chain risk.

Items for RSTC Approval/Discussion:

- **Request RSTC approval of a new Security Guideline: Procurement Sourcing**

Recent Activity

- Two revised guidelines (Vendor Incident Response and Procurement Language) are complete and will be sent for public comment.
- Procurement Sourcing guideline package has been submitted to the RSTC for approval and subsequent public comment period
- Leadership participated in a discussion with other group leaders regarding cloud computing activities that are currently underway.

Upcoming Activity

- The gap assessment for supply chain security standards has identified volunteers to participate in the effort; activities are to commence soon.
- WG members are expected to be among the participants in coordinated efforts by various groups that are addressing cloud computing topics.

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Periodic Review of Supply Chain Security Guidelines	🟢	Complete
Guidance documentation on supply chain risk management issues and topics (Procurement Sourcing guideline)	🟢	Ready for public comment
Gap assessment for supply chain security standards	🟢	In progress

RSTC Status Report
Security Integration and Technology Enablement Subcommittee (SITES)

Chair: Brian Burnett
Vice Chair: Thomas Peterson
September 2023

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Purpose: To identify, assess, recommend, and support the integration of technologies on the bulk power system (BPS) in a secure, reliable, and effective manner.

Items for RSTC Approval/Discussion:

- **Approve**: *Whitepaper: BES Ops in Cloud*
- **Approve**: Joint Whitepaper: Privacy & Security Impacts of DERA (item submitted by SPIDERWG)

Recent Work Plan Activity

- Whitepaper: Zero Trust for Electric OT (PUBLISHED)
- Joint Whitepaper: Privacy & Security Impacts of DERA, final draft complete and submitted to Sept RSTC agenda for Request for Approval
- Whitepaper: BES Ops in Cloud final draft complete and submitted to Sept RSTC agenda for Request for Approval

Recent Activity – Cont.

- Whitepaper: New Technology Enablement & Field Testing in ongoing drafting

Upcoming Activity

- Joint SWG, SCWG, SITES leadership meeting to coordinate / strategize on work plan priorities and overlaps
- Tentative kickoff of new SITES work plan item

Workplan Status *(6-month look-ahead)*

Milestone	Status	Comments
BES Operations in the Cloud	🟢	Final draft completed
New Tech Enablement	🟢	Drafting Ongoing
Privacy & Security for DER and DER Aggregators	🟢	Final draft completed
Next Work Plan Item Tentative	🟡	TBD

RSTC Status Report – Synchronized Measurement Working Group (SMWG)

Chair: Qiang "Frankie" Zhang
Vice-Chair: Clifton Black
September 2023

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Purpose: The purpose of the SMWG is to provide technical guidance and support for the use of synchronized and high-resolution measurements to enhance the reliability and resilience of the bulk power system (BPS) across North America.

Items for RSTC Approval/Discussion:

Recent Activity

- Published the 3/21 oscillation event report.
- Held July SMWG virtual meeting (7/12).

Upcoming Activity

- Add oscillation as a category in RCIS.
- Hold September SMWG Hybrid Meeting
- Draft a Synchrophasor Data Accuracy Maintenance Manual – Joint Effort with EMSWG.
- Draft a Roadmap for Integrating Synchrophasors into Real-time Operations.
- Supporting/Collaborating with SWG and SITES on developing a CIP implementation guidance for synchrophasors.

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Add Oscillation as a Category in RCIS	🟢	Initiated
September SMWG Hybrid Meeting	🟢	Planning
Synchrophasor Data Accuracy Maintenance Manual (with EMSWG)	🟢	Scheduled
Roadmap for Operationalizing Synchrophasor Technology	🟢	Initiated
CIP Implementation Guidance for Synchrophasors	🟢	Initiated

RSTC Status Report – System Protection and Control Working Group (SPCWG)

Chair: Lynn Schroeder
Vice-Chair: Manish Patel
As of August 17, 2023

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Purpose: The SPCWG will promote the reliable and efficient operation of the North American power system through technical excellence in protection and control system design, coordination, and practices.

Items for RSTC Approval/Discussion:

- **none**

Recent Activity

- Review and update documents: Determination of Practical Transmission Relaying Loadability Settings
- Review TRD: Transmission System Phase Backup Protections
- Develop Technical Reference document for Ethernet based P&C.
- Steady-state approach for PRC-024-3 Evaluation for Inverter-Based Resources" white paper

Upcoming Activity

- Work on projects

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Practical Relay Loadability	🟢	Draft created, under review by SPCWG. Expect to submit to RSTC at December meeting
Ethernet P&C TRD	🟢	Outline and scope of work is nearing completion, writing assignments expected at the October meeting
Review and update Transmission System Phase Backup Protections	🟢	Work continues, we expect an update at the October meeting
Steady-state approach for PRC-024-3 Evaluation for Inverter-Based Resources" white paper	🟢	Work ongoing, Goal is to submit to RSTC at their December Meeting

RSTC Status Report – System Planning Impacts from DER Working Group (SPIDERWG)

Chair: Shayan Rizvi
Vice-Chair: John Schmall
Sept XX, 2023

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Purpose: *Historically, the NERC Planning Committee (PC) identified key points of interest that should be addressed related to a growing penetration of distributed energy resources (DER). The purpose of the System Planning Impacts from Distributed Energy Resources)SPIDERWG) is to address aspects of these key points of interest related to system planning, modeling, and reliability impacts to the Bulk Power System (BPS). This effort builds off of the work accomplished by the NERC Distributed Energy Resources Task Force (DERTF) and the NERC Essential Reliability Services Task Force/Working Group (ERSTF/ERSWG), and addresses some of the key goals in the ERO Enterprise Operating Plan.*

Items for RSTC Approval/Discussion:

- **Approval**: *White Paper: Privacy and Security Impacts of DER and DER Aggregators*
- **Endorse:** *SAR EOP-005*

Workplan Status *(6 month look-ahead)*

See next slide for details

Workplan posted: *https://www.nerc.com/comm/RSTC/Pages/SPIDERWG.aspx*

Recent Activity

- Met in early August 2023 to update work products and focus on high priority items.
- Engaging RTOS and SPCWG for future SARs. Met with leadership to identify paths forward
- Joint SITES/SPIDERWG effort to return RSTC comments successful

Upcoming Activity

- *SPIDERWG meeting in October to:*
    - *Return responses to past meeting's review*
    - *Revising and Collaborating with other RSTC groups on SAR developments*
    - *Continue drafting of SARs*
    - *Focus on Studies RG, planning to seek RSTC EC for auth to post in Oct.*
    - *Drafting DER Aggregator/DERMS impacts and variability*

Work Look Ahead – non-SAR

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Workplan Status (6 month look-ahead)

Milestone	Status	Comments
S1 – Reliability Guideline: Bulk Power system Planning under Increasing Penetration of Distributed Energy Resources	🟡	Seeking RSTC EC action to authorize posting in Oct 2023. In SPIDERWG review
C11 – White Paper: Variability, Uncertainty, and Data Collection for the BPS with DER Aggregators	🟡	In progress for Q4 2023 RSTC review request, delay requested as SPIDERWG survey extended.
A3 – White Paper: Modeling of DER Aggregator and DERMS Functional Impacts	🟡	In draft. Seeking RSTC review in Q4.
C2 – White Paper: Communication and Coordination strategies for Transmission Entities and Distribution Entities regarding Distributed Energy Resources	🟢	In draft. Major involvement with external stakeholders underway. Coming to RSTC in Q4 2023

Work Look Ahead - SAR

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Workplan Status (6 month look-ahead)

Milestone	Status	Comments
C15 – SAR EOP-004	🟢	In draft. In RSTC Sept agenda
C16 – SAR EOP-005	🟢	In draft. Delayed from initial milestone due to industry comment period. Coming for RSTC review in Q4 2023
C17 – SAR BAL-003	🔴	In draft. Delayed from initial milestone. Coming for RSTC review in Q4 2023. Still within total SAR development scope.
C18 – SAR PRC-006	🔴	In draft. Delayed from initial milestone. Coming for RSTC review in Q4 2023. Still within total SAR development scope.
C19 – SAR on OPAs and RTAs	🔴	In draft. Delayed from initial milestone. Coming for RSTC review in Q1 2024. Still within total SAR development scope.

RSTC Status Report – Security Working Group (SWG)

Co-Chair: Brent Sessions
Co-Chair: Katherine Street
September 2023

🟢 On Track
🟡 Schedule at risk
🔴 Milestone delayed

Purpose: Provides a formal input process to enhance collaboration between the ERO and industry with an ongoing working group. Provides technical expertise and feedback to the ERO with security compliance-related products.

Recent Activity

- Completed
  - BCSI TTX
  - OLIR mapping CIP to CSF
  - FERC LL CIP-002
- ERO Compliance Approval
  - Cloud Encryption Guidance
- Coordinating
  - EGWG Utility Essentials Whitepaper
- New Activity
  - Surveys complete for Guideline Reviews
  - SMWG Request on Synchrophasor data
  - New Co-Chair John Tracy (TVA

Items for RSTC Approval/Discussion:

- None

Upcoming Activity

- Scoping/Research for
  1. Planning to Reduce Critical Facilities
  2. Communication Protection Systems Guideline
  3. Comprehensive physical security assessment
  4. EISAC Physical Issue Reporting – Lows Guideline

Workplan Status *(6 month look-ahead)*

Milestone	Status	Comments
Planning to Reduce Critical Facilities	🟢	
Ongoing ERT comments	🟢	
Comm. Protection systems Guideline	🟢	
Comprehensive Physical Security assessment	🟢	
Cloud Encryption Guidance Document	🟢	ERO Approval

RSTC Nominating Subcommittee

Action

Approve

Summary

Per the RSTC Charter, the Nominating Subcommittee (NS) will consist of seven (7) members (the RSTC vice chair and six (6) members drawing from different sectors and at-large representatives). Apart from the vice chair, members of the RSTC Executive Committee (RSTC EC) shall not serve on the RSTC NS. The NS members are nominated by the RSTC chair and voted on by the full RSTC membership. The term for members of the NS is one (1) year.

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability and Security Technical Committee Nominating Subcommittee

Rich Hydzik – RSTC Chair
Reliability and Security Technical Committee Meeting
September 20, 2023

RELIABILITY | RESILIENCE | SECURITY

Nominating Subcommittee Overview

- The Nominating Subcommittee (RSTC NS) will consist of seven (7) members (the RSTC Vice-Chair and six (6) members drawing from different sectors and at-large representatives). Apart from the Vice-Chair, members of the RSTC Executive Committee (RSTC EC) shall not serve on the RSTC NS.
- The NS members are nominated by the RSTC chair and voted on by the full RSTC membership.
- The term for members of the NS is one (1) year.

Nominating Subcommittee Overview

- The RSTC NS is responsible for (a) recommending individuals for at-large representative seats, and, (b) managing the process to select the chair and/or vice chair of the RSTC. The RSTC vice-chair shall recuse him or herself from this process unless he or she is not seeking re-election. At-large members on the RSTC NS shall recuse themselves from recommendations for at-large representative seats if they are seeking reappointment.
- Open nomination period for RSTC NS July 21-August 4, 2023
- Chair Hydzik reviewed nominations and present a proposed slate for RSTC NS members for full RSTC vote at the September 2023 RSTC meeting

Election Process

- The Chair presents the candidates.
- Elections will be held as follows:
  - The Committee will vote on the presented candidates. If the presented candidates are approved with a 2/3 majority, the presented candidates are selected and the election is closed.
  - Should the presented candidates not get elected the Chair will do the following:
    - Reconvene a review of the nominations already submitted;
    - Open for a second, shortened nomination process for additional submissions; and,
    - Convene a second meeting to evaluate the nominations and present candidates to be considered at the next RSTC meeting.

Recommended Slate

- Current Nominating Subcommittee members:
    - John Stephens – RSTC Vice Chair
    - Truong Le – Sector 6
    - William Allen – At-large
    - Wayne Guttormson – At-large, Canadian
    - Ian Grant – At-large
    - Srinivas Kapagantula – At-large

Recommended Slate

- For the Nominating Subcommittee members, the Chair nominates:
  - Brett Kruse – At-large

Questions and Answers

RSTC Standard Authorization Request (SAR) Development Process

Action

Approve

Summary

As part of the Framework to Address Known and Emerging Reliability and Security Risks[1], the RSTC reviews and provides guidance in developing deliverables[2] critical to ERO functions, such as Reliability Standards. In performing this function, the RSTC or its groups may develop SARs[3].

Additionally, the RSTC may endorse a SAR proposed by one of its subcommittees, work groups or task forces (RSTC Group) prior to any submission to the NERC Reliability Standards Staff or the NERC Standards Committee. RSTC endorsement of a SAR supports initial vetting of the technical material and the development of a sound technical justification to mitigate the identified risk.

NERC Staff reviewed RSTC comments received and made conforming revisions to the SAR Development Process. We are seeking RSTC approval of the revised process.

---

[1] See https://www.nerc.com/comm/RISC/Related%20Files%20DL/Framework-Address%20Known-Emerging%20Reliabilit-Securit%20%20Risks_ERRATTA_V1.pdf

[2] NERC provides White Papers, Technical Reference Documents, Reliability Guidance, and other resource documents that can assist registered entities with the identification and addressing of risks within their systems.

[3] See https://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf

Reliability and Security Technical Committee Standard Authorization Request (SAR) Process

The Reliability and Security Technical Committee ("RSTC") is a standing committee of the North American Electric Reliability Corporation ("NERC"). As stated in the RSTC Charter, the committee strives to advance the reliability and security of the interconnected Bulk Power System ("BPS") of North America by:

- Creating a forum for aggregating ideas and interests, drawing from diverse industry stakeholder expertise, to support the ERO Enterprise's mission;
- Leveraging such expertise to identify solutions to study, mitigate, and/or eliminate emerging risks to the BPS for the benefit of industry stakeholders, the NERC Board of Trustees ("Board") and ERO Enterprise staff and leadership; and,
- Overseeing the implementation of group work plans that drive risk-mitigating technical solutions.

SAR Development Process

As part of the Framework to Address Known and Emerging Reliability and Security Risks[1], the RSTC reviews and provides guidance in developing deliverables[2] critical to ERO functions, such as Reliability Standards. In performing this function, the RSTC or its groups may develop Standard Authorization Request(s) ("SAR")[3].

Additionally, the RSTC subcommittees, working groups or task forces ("RSTC Group") may develop a SAR for RSTC action prior to any submission to the NERC Reliability Standards Staff or the NERC Standards Committee. RSTC endorsement of a SAR supports initial vetting of the technical material and the development of a sound technical justification to mitigate the identified risk.

RSTC Group SAR Development Steps: (See Figure 1)

1. Identify Risk Reliability Gap (problem statement) and clearly articulate risk to Reliability, Resilience or Security through any of the following:
    a. White Paper
    b. Event Analysis or Disturbance Report
    c. RISC Report
    d. Assessment

---

[1] See https://www.nerc.com/comm/RISC/Related%20Files%20DL/Framework-Address%20Known-Emerging%20Reliabilit-Securit%20%20Risks_ERRATTA_V1.pdf

[2] NERC provides White Papers, Technical Reference Documents, Reliability Guidance, and other resource documents that can assist registered entities with the identification and addressing of risks within their systems.

[3] See https://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf

   e. Other documents or reports

2. Develop technical justification for SAR development for subsequent approval by the RSTC to proceed with SAR development. This step will be conducted during a regular RSTC meeting or through the electronic ballot process.
   a. Include assessment of other mitigation measures (reliability guideline, reference document, etc.) vs SAR. Why was a SAR chosen as the risk mitigation measure?
   b. Clearly articulate the reliability gap with the associated risks.
   c. Develop proposed SAR Prioritization based on risk level to the BES (High/Medium/Low) associated with the reliability gap.
   d. Assess level of residual (or acceptable) risk once the project is complete or identify any areas related to the identified risk that will not be addressed by the SAR.
   e. Ensure the SAR doesn’t duplicate the efforts that would be part of the Standards Drafting Team responsibility (solutions to the problem and drafting requirement language).
3. Obtain RSTC approval to develop a SAR (per Notional Work Product Flow Process[4]).
4. Develop SAR and present to RSTC for RSTC comment. RSTC comments should be submitted via the public announcement of a comment period to ensure all comments are gathered by the RSTC Group.
   a. RSTC members to share the draft SAR with industry stakeholders within their sector, organization or trade group for their review and comments
   b. Post draft SAR for a 30-day public comment period. This comment period may overlap or coincide with the RSTC member comment period.
5. RSTC Group to respond to comments and update SAR
6. Present SAR for RSTC Endorsement
7. Based on prioritization, submit SAR to Standards Committee, to ensure higher risk items can be addressed first.
8. Upon Standards Committee approval, the RSTC Sponsor will coordinate with the RSTC Group leadership to liaise with the Standard Drafting Team for technical input and assistance.

---

[4] https://www.nerc.com/comm/RSTC/Documents/RSTC%20Work%20Plan%20Notional%20Process_Approved_Sept_2020.pdf

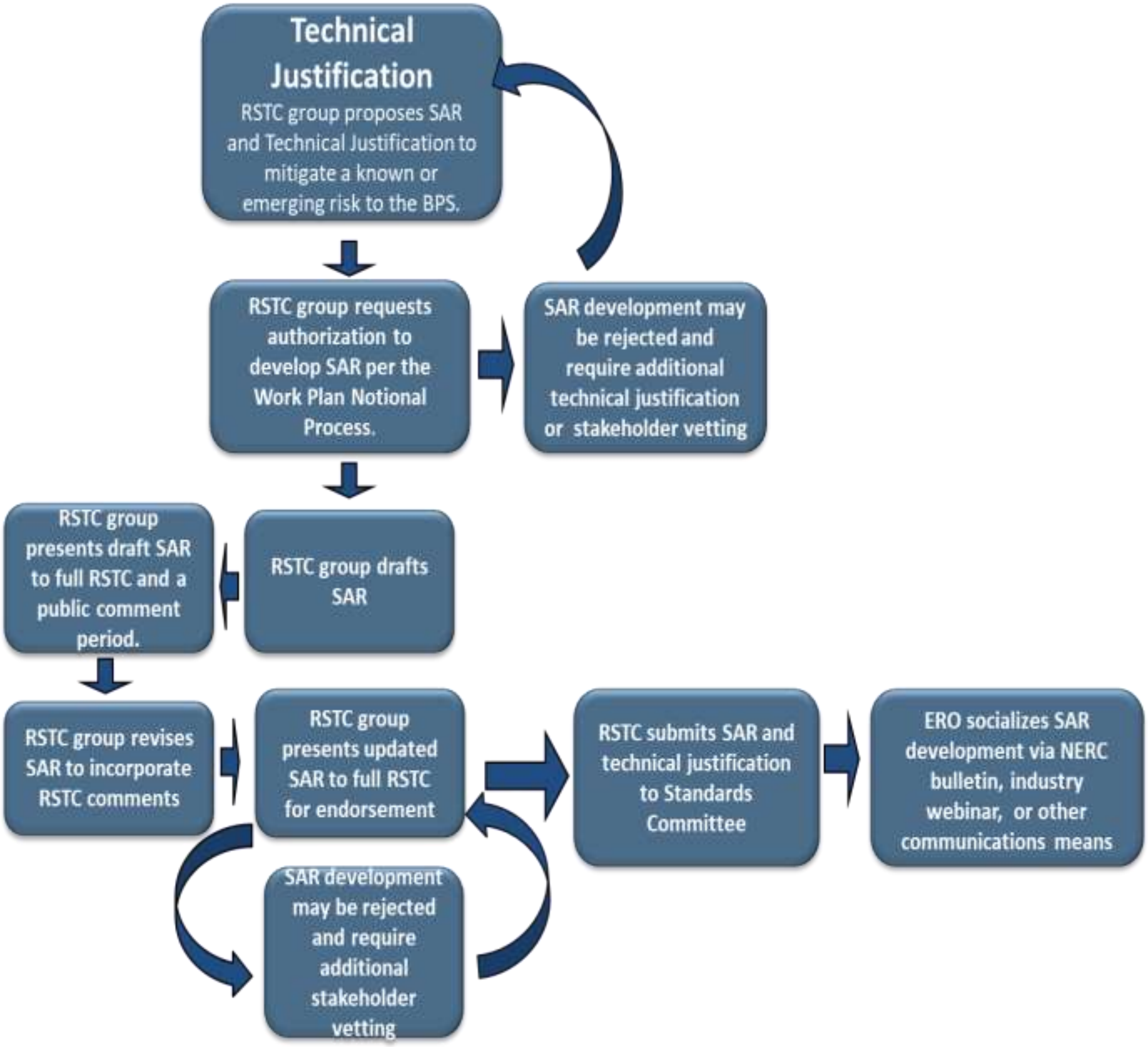


Figure 1: SAR Development Process Flow Diagram

SAR Development Process - Checklist

Checklist should be included with SAR during each stage of development and review.

☐ Do you have a technical basis document from NERC, industry, or an approved RSTC document that justifies the creation of a SAR?

  a. Include assessment of other mitigation measures (reliability guideline, reference document, etc.) vs SAR? Why was a SAR chosen as the risk mitigation measure?
  b. Clearly articulate the reliability gap with the associated risks.
  c. Develop proposed SAR Prioritization (High/Medium/Low)?
  d. Assess level of residual (or acceptable) risk once the project is complete?
  e. Ensure the SAR doesn’t duplicate the efforts that would be part of the Standards Drafting Team responsibility (solutions to the problem and drafting requirement language)?

☐ Has the RSTC authorized the RSTC Group to create the SAR?

☐ Has the SAR been added to the RSTC Group work plan?

☐ Have you created and vetted the SAR with industry stakeholders (internal to the RSTC Group or with external outreach)? Examples of outreach include:

  a. RSTC Group Membership
  b. RSTC Group RSTC Sponsor
  c. Other/Related RSTC group
  d. Webinar/Other Engagement
  e. Trade Associations
  f. Government/Regulatory
  g. RSTC Strategic Planning Process
  h. SCCG

☐ Has the SAR been presented to the RSTC as a first draft within its review/comment period?

☐ Have RSTC comments been reviewed and conforming revisions made to the SAR to address those comments?

☐ Has the SAR been presented as a final draft to industry for information? (Optional as circumstances warrant)

☐ Has a final draft of the SAR been presented to the RSTC, with a response to comments received?

☐ Has the RSTC endorsed the SAR, including priority? The RSTC may also reject the SAR or remand the SAR for further action by the RSTC Group originating the SAR.

☐ Has the endorsed SAR been submitted to the Standards Committee through NERC Staff?

DRAFT

Reliability and Security Technical Committee Standard Authorization Request (SAR) Process

The Reliability and Security Technical Committee ("RSTC") is a standing committee of the North American Electric Reliability Corporation ("NERC"). As stated in the RSTC Charter, the committee strives to advance the reliability and security of the interconnected Bulk Power System ("BPS") of North America by:

- Creating a forum for aggregating ideas and interests, drawing from diverse industry stakeholder expertise, to support the ERO Enterprise's mission;
- Leveraging such expertise to identify solutions to study, mitigate, and/or eliminate emerging risks to the BPS for the benefit of industry stakeholders, the NERC Board of Trustees ("Board") and ERO Enterprise staff and leadership; and,
- Overseeing the implementation of group work plans that drive risk-mitigating technical solutions.

SAR Development Process

As part of the Framework to Address Known and Emerging Reliability and Security Risks[1], the RSTC reviews and provides guidance in developing deliverables[2] critical to ERO functions, such as Reliability Standards. In performing this function, the RSTC or its groups may develop Standard Authorization Request(s) ("SAR")[3].

Additionally, the RSTC subcommittees, working groups or task forces ("RSTC Group") may develop a SAR for RSTC action ~~may endorse a SAR proposed by one of its subcommittees, work groups or task forces ("RSTC Group")~~ prior to any submission to the NERC Reliability Standards Staff or the NERC Standards Committee. RSTC endorsement of a SAR supports initial vetting of the technical material and the development of a sound technical justification to mitigate the identified risk.

RSTC Group SAR Development Steps: (See Figure 1)

1 Identify Risk Reliability Gap (problem statement) and clearly articulate risk to Reliability, Resilience or Security through any of the following:
  - a. White Paper
  - b. Event Analysis or Disturbance Report
  - c. RISC Report
  - d. Assessment
  - e. Other documents or reports

---

[1] See https://www.nerc.com/comm/RISC/Related%20Files%20DL/Framework-Address%20Known-Emerging%20Reliabilit-Securit%20%20Risks_ERRATTA_V1.pdf

[2] NERC provides White Papers, Technical Reference Documents, Reliability Guidance, and other resource documents that can assist registered entities with the identification and addressing of risks within their systems.

[3] See https://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf

2 Develop technical justification for SAR development for subsequent approval by the RSTC to proceed with SAR development. This step will be conducted during a regular RSTC meeting or through the electronic ballot process.

   a. Include assessment of other mitigation measures (reliability guideline, reference document, etc.) vs SAR. Why was a SAR chosen as the risk mitigation measure?
   b. Clearly articulate the reliability gap with the associated risks.
   c. Develop proposed SAR Prioritization based on risk level to the BES (High/Medium/Low) associated with the reliability gap. ~~(High/Medium/Low)~~
   d. Assess level of residual (or acceptable) risk once the project is complete or identify any areas related to the identified risk that will not be addressed by the SAR.
   e. Ensure the SAR doesn't duplicate the efforts that would be part of the Standards Drafting Team responsibility (solutions to the problem and drafting requirement language).

3 Obtain RSTC ~~or RSTC EC~~ approval to develop a SAR (per Notional Work Product Flow Process[4]).

4 Develop SAR and present to RSTC for RSTC comment. RSTC comments should be submitted via the public announcement of a comment period to ensure all comments are gathered by the RSTC Group.

   a. RSTC members to share the draft SAR with industry stakeholders within their sector, organization or trade group for their review and comments
   b. Post draft SAR for a 30-day public comment period. This comment period may overlap or coincide with the RSTC member comment period.

5 RSTC Group to respond to comments and update SAR

6 Present SAR for RSTC Endorsement

7 Based on prioritization, submit SAR to Standards Committee, to ensure higher risk items can be addressed first

8 Upon Standards Committee approval, the RSTC Sponsor will coordinate with the RSTC Group leadership to liaise with the Standard Drafting Team for technical input and assistance.

Commented [A1]: Can we clarify where this will be approved? Is this part of a RSTC meeting, as part of work plan process, or something else?

I do agree that having the technical justification developed first is a good idea rather than presented at same time as the SAR.

Commented [SC2R1]: Added language to be approved by RSCT during regular meeting or electronic ballot between meetings.

Commented [A3]: Rather than SAR prioritization, the RSTC could weigh in on the risk level to the BES (High/Medium/Low) associated with the reliability gap. This could then be used by the Standards Committee when scheduling work on the SAR.

Commented [SC4R3]: Added language as suggested.

Commented [A5]: Hypothetical? Estimate of what the residual risk may be after the standard is written. Of value when certain metrics are known. For example, the retirement of the LSE function, LSE was replaced with DP however, this is not a one-for-one replacement.
Change to: "Assess any remaining reliability gaps that the project won't address."

Commented [SC6R5]: This language could be very broadly interpreted. Revised to add areas related to the risk that the SAR will not address.

Commented [A7]: Is this deletion intentional? If so, the graphic below needs to be updated. Also, the graphic below does not include an industry comment period.

Commented [SC8R7]: It was intentional. Comments were received that the full RSTC should vote on developing a SAR. The graphic was corrected and we added public comment along with RSTC comment.

Commented [9]: Doesn't the Notional Work Product Flow Process support EC approval for SAR development?

Commented [SC10R9]: Comments were received that the full RSTC should vote on developing a SAR.

Commented [A11]: Clarify whether there is a preferred way for entities to engage in the process. Some entities can comment via their RSTC Sector Rep, public comment or both avenues? Could end up being duplicative for NERC. For example: submit to NERC directly and cc: RSTC Sector Rep?

Commented [SC12R11]: Added statement to submit comments through the public announcement.

Commented [A13]: I suggest adding an additional step to specifically seek comments from other RSTC groups that are relevant as well as RSTC members. I think that peer review process would be useful and help communicate between the groups more.

Commented [A14]: Recommend Draft SARs be posted to Reliability Standards Under Development (nerc.com) as a new category; e.g. "Projects Under RSTC Consideration" to retain a one-stop shop.

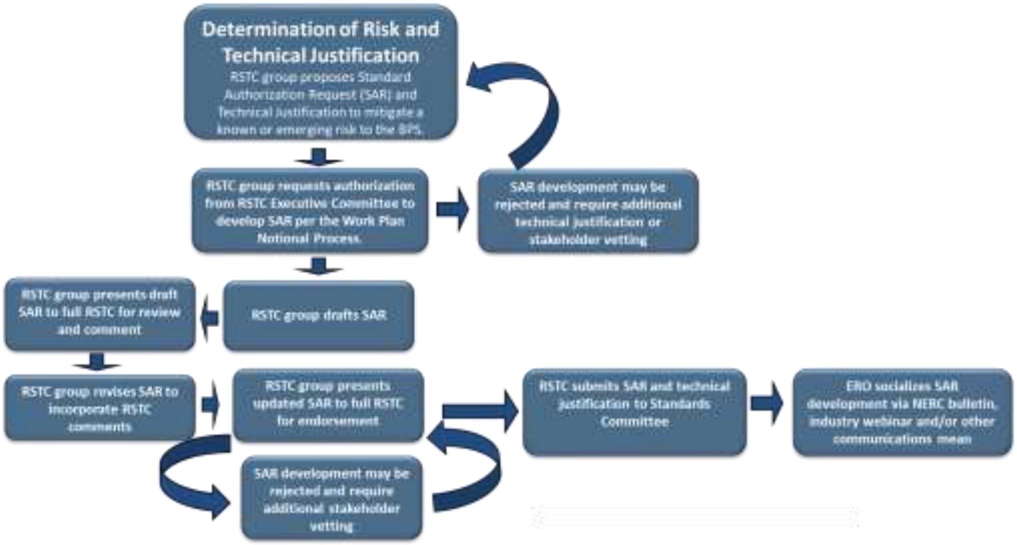
Commented [A15]: What if the RSTC rejects the SAR? Should the process include a box to terminate?

Commented [A16]: Is this step setting the RSTC Sponsor as the liaison between SDT and RSTC group? I am not sure that the Sponsor is the best person for that since the Sponsor is not neccesarily as technically proficient in the subject matter as group members.

Would it be better to have a Group member work between the group and SDT? Often, at least some group members would be on the committee any way.

---

[4] https://www.nerc.com/comm/RSTC/Documents/RSTC%20Work%20Plan%20Notional%20Process_Approved_Sept_2020.pdf ~~https://www.nerc.com/comm/RSTC/Documents/RSTC%20Work%20Plan%20Notional%20Process_Approved_Sept_2020.pdf~~


Determination of Risk and Technical Justification
RSTC group proposes Standard Authorization Request (SAR) and Technical Justification to mitigate a known or emerging risk to the BPS.
RSTC group requests authorization from RSTC Executive Committee to develop SAR per the Work Plan Notional Process.
SAR development may be rejected and require additional technical justification or stakeholder vetting
RSTC group presents draft SAR to full RSTC for review and comment
RSTC group drafts SAR
RSTC group revises SAR to incorporate RSTC comments
RSTC group presents updated SAR to full RSTC for endorsement
RSTC submits SAR and technical justification to Standards Committee
ERO socializes SAR development via NERC bulletin, industry webinar and/or other communications mean
SAR development may be rejected and require additional stakeholder vetting

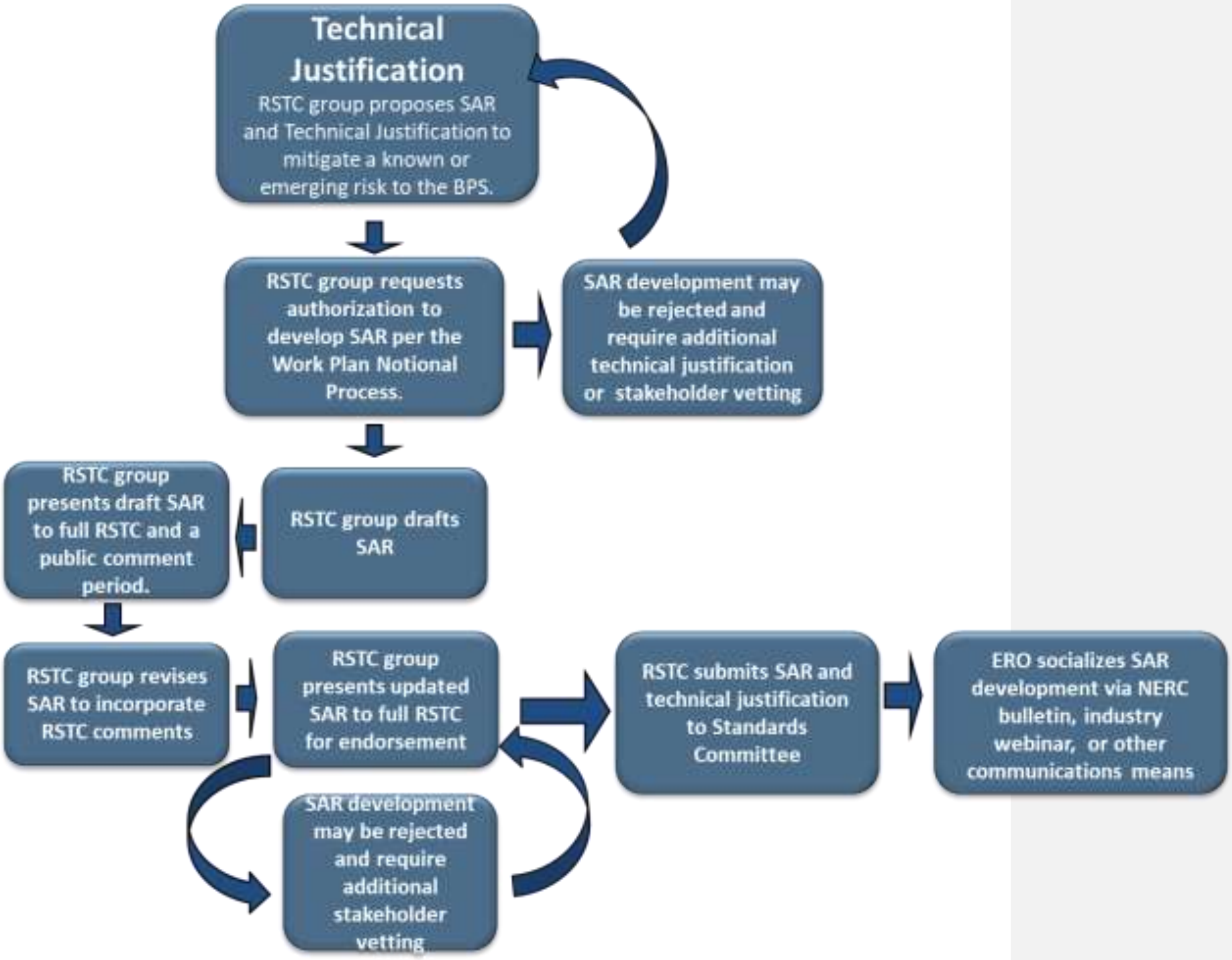


Figure 1~~2~~: SAR Development Process Flow Diagram

SAR Development Process - Checklist

Checklist should be included with SAR during each stage of development and review.

☐ Do you have a technical basis document from NERC, industry, or an approved RSTC document that justifies the creation of a SAR?
  a. Include assessment of other mitigation measures (reliability guideline, reference document, etc.) vs SAR? Why was a SAR chosen as the risk mitigation measure?
  b. Clearly articulate the reliability gap with the associated risks?
  c. Develop proposed SAR Prioritization (High/Medium/Low)?
  d. Assess level of residual (or acceptable) risk once the project is complete?
  e. Ensure the SAR doesn't duplicate the efforts that would be part of the Standards Drafting Team responsibility (solutions to the problem and drafting requirement language)?

☐ Has the RSTC ~~or RSTC EC~~ authorized the RSTC Group to create the SAR?

☐ Has the SAR been added to the RSTC Group work plan?

☐ Have you created and vetted the SAR with industry stakeholders (internal to the RSTC Group or with external outreach)? Examples of outreach include:
  a. RSTC Group Membership
  b. RSTC Group RSTC Sponsor
  c. Other/Related RSTC group
  d. Webinar/Other Engagement
  e. Trade Associations
  f. Government/Regulatory
  g. RSTC Strategic Planning Process
  ~~a.~~h. SCCG

	~~Author~~	~~Outreach~~
~~RSTC Group Membership~~	~~X~~	
~~RSTC Group RSTC Sponsor~~		~~X~~
~~Other/Related RSTC group~~		~~X~~
~~Webinar/Other Engagement~~		~~X~~
~~Trade Associations~~		~~X~~
~~Government/Regulatory~~		~~X~~
~~RSTC Strategic Planning Process~~		~~X~~
~~SCCG~~		~~X~~

☐ Has the SAR been presented to the RSTC as a first draft within its review/comment period?

☐ Have RSTC comments been reviewed and conforming revisions made to the SAR to address those comments?

Commented [SS17]: Who sees this checklist? The checklist contains information that would be valuable to all reviewers of the SAR. This checklist should accompany the SAR during each stage of development & review.

Commented [SC18R17]: Agreed.

Commented [SS19]: The checklist should include the five sub-requirements needed for a technical justification. Ie. Did you:
  a. Include assessment of other mitigation measures (reliability guideline, reference document, etc.) vs SAR? Why was a SAR chosen as the risk mitigation measure?
  b. Clearly articulate the reliability gap with the associated risks?
  c. Develop proposed SAR Prioritization (High/Medium/Low)?
  d. Assess level of residual (or acceptable) risk once the project is complete?
  e. Ensure the SAR doesn't duplicate the efforts that would be part of the Standards Drafting Team responsibility (solutions to the problem and drafting requirement language)?
Each of these sub-requirements should be specifically verified.

Commented [SC20R19]: Added per comment.

Commented [A21]: This should be consistent with 3 above.

Commented [SC22R21]: Removed EC

Commented [23]: Ensure consistenRSTCcy with Step 3 (Page 2)--RSTC Group SAR development process.

Also appears in Figure 1 flow diagram

Commented [SC24R23]: Removed EC

Commented [A25]: Can you explain this table? Are these tasks to do or responsibilities of members and sponsors? Are committees required to do all the steps?

Commented [SC26R25]: This was intended to provide examples for outreach. It doesn't add clarity so it was changed to a list of options.

Commented [A27]: I assume not all Outreach is required for each SAR? If so, should that be made clear?

Commented [SC28R27]: Correct. Changed table to list of example.

☐ Has the SAR been presented as a final draft to industry for information? (Optional as circumstances warrant)

☐ Has a final draft of the SAR been presented to the RSTC, with a response to comments received?

☐ Has the RSTC endorsed the SAR, including priority? The RSTC may also reject the SAR or remand the SAR for further action by the RSTC Group originating the SAR.

Commented [A29]: This should trigger the "off ramp" where the SAR does not move to the SC.

Commented [SC30R29]: Added language for other options for RSTC action.

☐ Has the endorsed SAR been submitted to the Standards Committee through NERC Staff?

Agenda Item 6
RSTC Meeting
September 20, 2023

Electromagnetic Pulse (EMP) Working Group Disbandment

Action

Accept

Background

A Presidential Order in March 2019 established a government-wide policy to protect key systems, networks, and assets from EMP signals that can disrupt, degrade, and damage technology and critical infrastructure systems across large areas[1]. The following month, the Electric Power Research Institute (EPRI)[2] published a technical report[3] that laid the groundwork for developing analyses, guides, and/or assessments that could identify where and how the bulk power system (BPS) could be vulnerable to a High Altitude EMP (HEMP) attack. It included recommendations for mitigating the risks to reliability from such an attack, and suggestions for recovering from one.

In April 2019, the NERC Board of Trustees appointed an EMP Task Force (EMPTF) to assess whether a reliability guideline or standard was needed to address the HEMP risks to BPS reliability. The EMPTF used data from EPRI and other sources to prepare a report that included several strategic recommendations for mitigating that risk.[4] The Board assigned those items to the Reliability and Security Technical Committee (RSTC) for implementation, and the RSTC appointed the EMP Working Group (EMPWG) to act on them.

Summary

The EMPWG scope and work plan were approved by RSTC in late 2020. The EMPWG assigned five teams to address the recommendations in the EMPTF's report. The EMPWG teams began their work in earnest and while there were various reasons for overall participation to diminish over time, they produced over 50 pages of material that will be published as a technical reference document.

As the EMPWG's teams worked on their respective tasks, it became increasingly apparent that while the group as a whole was serving as an information exchange, that role was difficult to sustain because the group's resources were needed for more urgent issues. Efforts to address the complex nature of a HEMP's interaction with the grid, the perception that there was a low probability of such an attack, the emergence of new information such as that generated by EPRI's research, and the variety of response and remediation measures that are available made it clear that pursuing further action was premature.

There are a number of entities that are undertaking pioneering efforts to address EMP resiliency, using a variety of approaches. Interaction between these companies appears to be excellent,

---

[1] President Trump Signs Executive Order for Resilience Against Electromagnetic Pulses | Department of Energy

[2] High-Altitude Electromagnetic Pulse and the Bulk Power System: Potential Impacts and Mitigation Strategies. EPRI, Palo Alto, CA: 2019 (Product ID 3002014979)

[3] https://www.epri.com/research/products/3002014979

[4] https://www.nerc.com/pa/Stand/EMP%20Task%20Force%20Posting%20DL/NERC_EMP_Task_Force_Report.pdf

aided by organizations such as the EIS Council and the North American Transmission Forum (NATF), complemented by EPRI's continuing work.[5]

As the risk landscape has evolved and industry is grappling with various high priority risk issues such as inverter-based resources performance and analysis, extreme weather, cyber and physical security threats, etc., EMPWG participation has diminished and the group is not sustainable. For this reason and given the change of risk prioritization by industry stakeholders, EMPWG is recommending disbanding the group. Membership rosters and mailing lists will be maintained, and the group can be reactivated relatively quickly, if needed at a later date. However, resources within NERC and at industry stakeholders need to be prioritized toward higher priority risk issues at this time.

NERC staff will compile available materials on the EMPWG webpage (which will be moved to the disbanded section of the RSTC page) and post any relevant materials developed by the group thus far for industry reference. However, these materials will not be approved or endorsed by the RSTC; rather, only housed for reference if needed.

---

[5] EPRI and other groups continue research activities to address EMP, including providing unclassified information that can be used by system planners, products and services that support EMP protection and preparation, and research into EMP effects on distribution systems, generating plants, and communications.

ERO Event Analysis Process Document

Action

Accept

Background

The Event Analysis Subcommittee (EAS) is currently seeking acceptance for the ERO Event Analysis Process (EAP) v5 document. This EAP document has recently undergone updates after being posted for a 45-day industry comment period. The EAS has addressed all comments received during this review process. The EAS has endorsed the ERO EAP v5.

Summary

This ERO EAP v5 document reflects several notable enhancements intended to provide clarity and increase participation by industry stakeholders. These enhancements include, but are not limited to, the following.

- Update the Introduction section to provide additional background information regarding the Event Analysis Program.
- Update the Process Overview section to provide additional background information regarding the Event Analysis Process.
- Revise the ERO Event Analysis Process section to provide clarity and describe changes to event categorization definitions that include the following.
    - Retire Category 1b
    - Retire Category 1d
    - Revise Category 1e definition to provide clarity
    - Revise Category 1h definition in accordance with the recommendation of the Energy Management Systems Working Group to provide clarity
    - Revise Category 2e definition to provide clarity
    - Revise Category 2f definition to provide clarity
    - Revise Category 2g definition to provide clarity
    - Combine Categories 3, 4, and 5 into a single Category 3

Electric Reliability Organization Event Analysis Process

Version 5.0

Approved: September xx, 2023

Effective Date: January 1, 2024

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

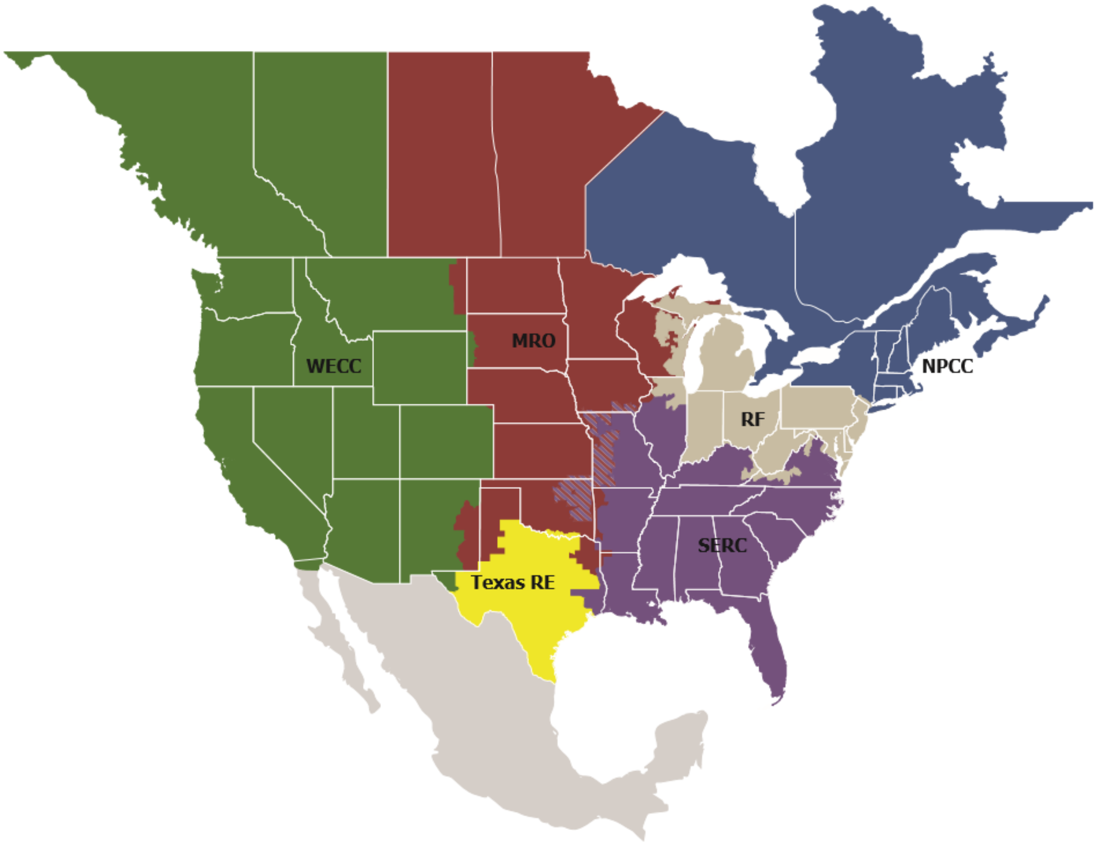
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

The ERO Event Analysis Process (EAP) document is intended to be used as a guideline to promote a structured and consistent approach to performing event analyses in North America. This document outlines a process that will facilitate greater communication and information exchange between registered entities, Regional Entities, and NERC.

The ERO Event Analysis Program exists for review of major system events and other off-normal system occurrences. The program is forensic in nature and focuses on the near-term to real-time operating horizons. The program is derived from the NERC Rules of Procedure (ROP) authorities/requirements outlined in Section 800 – Reliability Assessment and Performance Analysis. Section 800 specifies the need for analysis of off-normal occurrences on the Bulk Electric System (BES) that do not rise to the level of major events as described in the ROP. For purposes of the Event Analysis Program an event is defined as a single incident or linked incidents due to a common initiating cause resulting in an undesirable impact to the bulk electric system (BES).

The EAP is an approach specifically designed to address categorized events defined by the Event Analysis Subcommittee (EAS) in concert with the ERO that could result in adverse impacts to the BES, provide indication of future system risks, and/or confirm known risks to the BES. The process is a systematic approach to handle data collection and analysis of events as defined by the EAP category criteria. The main objective is for the ERO and industry to learn from the events and to develop corrective actions to prevent recurrence. Continuous improvement is the mindset that the process is designed to instill in industry design and operating practices.

The primary reason for participating in an event analysis is to determine if there are lessons to be learned and potential recommendations that can be shared with industry to mitigate the risk of recurrence. An effective EAP requires industry participation and support to assist in continuous improvement of BES performance.

Analyzed events feed the ERO Cause Code Assignment Process[1], which is used to identify trends. Trends help the ERO confirm known and expected reliability risks and identify emerging risks. Resulting mitigation efforts could include NERC Alerts[1] and/or recommended changes to Reliability Standards and/or disturbance reporting.

The NERC Reliability and Security Technical Committee (RSTC) will oversee the maintenance of the EAP document through the EAS and existing ERO documentation processes. The document will be periodically reviewed and updated by the EAS every three years or as needed. The RSTC may solicit comments from industry during the review process.

The EAP does not exempt the registered entity from mandatory reporting requirements governed by regulatory authorities or NERC Reliability Standards.[2]

---

[1] https://www.nerc.com/pa/rrm/ea/EA%20Program%20Document%20Library/CCAP_Manual_2023.pdf

[2] Rules of Procedure (ROP) Section 810

Process Overview

The EAP maintains three categories of pre-defined criteria that serve to drive data collection efforts for use in identifying system impacts and risks. Each category describes the impact to the BES and the EAP provides industry with the level of analysis necessary to accurately report the event to the ERO.

The event analysis process most often begins when the ERO receives notification of a potential event via receipt of an OE-417 or EOP-004 or receipt of a brief report. A foundation for success of EAP is in the initial communication and coordination between the registered entity and the RE described in the steps below. A primary reason for participating in an event analysis is to determine if there are practices and lessons to be learned and shared with the industry. The six steps below support this objective.

Step 1: The registered entity assesses an event, proposes the event category in accordance with the EAP, and reports the event to the RE.

Step 2: A planning meeting or coordination call (Appendix B) is held between the registered entity and the RE when possible.

Step 3: The registered entity submits a Brief Report (Appendix C) to the RE.

Step 4: The registered entity submits an Event Analysis Report (EAR) (Appendix D) to the RE, if needed.

Step 5: Lessons learned (Appendix E) are developed and shared with industry as appropriate.

Step 6: The EAP is closed.

Categorizing Events (Step 1)

When a registered entity experiences an event, that entity will propose an initial category for the event as outlined in this section. The categories listed in this section do not cover all possible events. The need for analysis may be discussed by all affected registered entities, the appropriate REs, and NERC.

Registered entities that reside in multiple RE footprints should notify all relevant REs of an event that spans those Regions. NERC and the REs will determine a lead RE for the event, and further communication will take place between the registered entity and the lead RE.[3]

If an event is experienced that meets Category 1-3 criteria the primary focus should be restoration and then communication with the RE on reporting per appendix A. Qualifying events are assigned to one of three categories based on potential reliability impact to the BES. The event categories are intended to allow the registered entity and RE to objectively identify event thresholds. The highest category that characterizes an event should be used.

The categories listed in this section do not cover all possible events. Events of interest that do not meet EAP reporting criteria may be identified by NERC, the RE, or the registered entity. In these cases a report may be submitted or requested in an effort to share experiences and lessons learned with the industry. These unqualified events will be categorized as Category 0.

Category 1: An Event that Results in One or More of the Following:

a. An outage, contrary to design, of three or more BES Facilities caused by an event:
    i. The outage of a combination of three or more BES Facilities (excluding successful automatic reclosing)
    ii. The outage of an entire generation station of three or more generators (aggregate generation of 500 MW to 1,999 MW)[4]; each combined-cycle unit is counted as one generator.

b. ~~Intended and controlled system separation by the proper operation of a remedial action scheme (RAS) in New Brunswick or Florida from the Eastern Interconnection~~ Retired on January 1, 2023

c. Failure or misoperation of a BES Remedial Action Scheme (RAS)

d. ~~System-wide voltage reduction of 3% or more that lasts more than 15 continuous minutes due to a BES Emergency~~ Retired on January 1, 2023

e. BES system separation contrary to design that results in an island of 100 MW to 999 MW. This excludes BES radial connections and non-BES (distribution) level islanding

f. ~~Unplanned evacuation from a control center facility with BPS SCADA functionality for 30 minutes or more.~~ Retired on January 1, 2016

g. In ERCOT, loss of generation of 1,400 MW to 1,999 MW

---

[3] ERO Enterprise Guide for the Multi-Region Registered Entity Coordinated Oversight Program, March 2018, Section IX: System Events

[4] Gross MW output of the generators at the time of the outage.

h. Loss of monitoring[5] and/or control[6] at a Control Center such that it degrades[7] the entity's ability to make Real-time operating decisions that are necessary to maintain reliability of the BES in the entity's footprint for 30 continuous minutes or more

   Some examples that should be considered for EA reporting include, but are not limited to the following. Additional cases are provided in the Addendum for Category 1h Events found under reference materials for event analysis on the EA Program website.[8]

   i. Loss of operator ability to remotely monitor or control BES elements
   ii. Loss of communications from SCADA remote terminal units (RTU)
   iii. Unavailability of ICCP links, which reduces BES visibility
   iv. Loss of the ability to remotely monitor and control generating units via automatic generation control (AGC)
   v. Unacceptable state estimator or real time contingency analysis solutions

i. A non-consequential interruption[9] of inverter type resources[10] aggregated to 500MW or more not caused by a fault on its inverters, or its ac terminal equipment.

j. A non-consequential interruption[11] of a DC tie(s), between two separate asynchronous systems, loaded at 500 MW or more, when the outage is not caused by a fault on the dc tie, its inverters, or its ac terminal equipment.

Category 2: An Event that Results in One or More of the Following:

a. Complete loss of interpersonal communication and alternative interpersonal communication capability affecting its staffed BES control center for 30 continuous minutes or more.

b. ~~Complete loss of SCADA, control or monitoring functionality for 30 minutes or more.~~ Retired on January 01, 2016 refer to Category 1h

c. BES Emergency resulting in a voltage deviation of ≥ 10% difference of nominal voltage sustained for ≥ 15 continuous minutes.

d. Complete loss of off-site power (LOOP) to a nuclear generating station per the Nuclear Plant Interface Requirement
e. System separation contrary to design, that results in an island of 1,000 MW to 4,999 MW
f. Simultaneous loss of 300 MW or more of firm load due to a BES event, contrary to design, for more than 15 minutes

---

[5] The ability to accurately receive relevant information about the BES in Real Time and evaluate system conditions using Real-time data to assess existing (pre-Contingency) and potential (post-Contingency) operating conditions to maintain reliability of the BES

[6] The ability to take and/or direct actions to maintain the reliability of the BES in Real Time via entity actions or by issuing Operating Instructions

[7] For purposes of 1h categorization “degrades” means less-than required functioning of any monitoring/control component, process, or capability.

[8] https://www.nerc.com/pa/rrm/ea/Pages/EA-Program.aspx

[9] Interruption of resources caused by action of control systems on the resources in response to perturbations in voltage and/or frequency on the Interconnection, not including the control actions of a RAS.

[10] In most cases, inverter-based generating resources refer to Type 3 and Type 4 wind power plants, and solar photovoltaic (PV) resources. Battery energy storage is also considered an inverter-based resource. Many transmission-connected reactive devices such as STATCOMs and SVCs are also inverter-based. Similarly, HVDC circuits also interface with the AC network though converters.

[11] Interruption of resources caused by action of control systems on the resources in response to perturbations in voltage and/or frequency on the Interconnection, not including the control actions of a RAS

g. Interconnection Reliability Operating Limit (IROL) exceedance for greater than 30 minutes

Category 3: An Event That Results in One or More of the Following:

a. Loss of firm load, contrary to design, of 2,000 MW or more.
b. System separation contrary to design, that results in an island of 5,000 MW or more
c. System separation (without load loss) contrary to design, that islands Florida from the Eastern Interconnection
d. Loss of 2,000 MW or more provided by DC tie(s) connected to asynchronous resources
e. Loss of generation (including inverter-based resources) of 2,000 MW or more. This excludes RAS action that performed as designed.

Event Analysis Planning Meeting/Coordination Call (Step 2)

Following an event, the RE and/or NERC will determine if a planning or coordination meeting is required between the registered entity(ies) and the applicable RE. More than one planning meeting may be conducted based on the registered entity's experience level with the EAP, the scope of the event, or the number of registered entities involved.

The planning meeting (when held) should:

1. confirm the event category;
2. determine the level of analysis;[12]
3. identify the roles for the registered entity(ies), REs, and NERC;
4. establish milestones, coordination of target dates, and determine reporting entity(ies) for completing reports, lessons learned, and other necessary analysis for events requiring detailed analysis, or the analysis itself would take longer to complete than the target dates set in the appendices. Should additional time be needed beyond the target dates to complete the analysis, this can be granted by the RE on a case-by-case basis as necessary;
5. identify the need for a data retention hold; and
6. identify data and information confidentiality issues.

Registered entities should capture relevant data for the event analysis. REs will formally send a Data Retention Hold[13] Notice for events in Category 3, if deemed necessary by the RE(s) or NERC.

The Appendix B: Planning Meeting Scope Template can be used as an outline in the planning meeting.

Event Analysis Process Reports (Steps 3 and 4)

Timeframes for submitting the requisite reports are found in Appendix A: Target Timeframes for Completion of Brief Reports, EARs, and Lessons Learned.

---

[12] Although the category of the event provides general guidance on the level of analysis needed, these guidelines may be adjusted by the EA team, based on the overall significance of the event and the potential for valuable lessons learned.

[13] BPS users, owners, and operators are required, upon request, to produce any requested data pursuant to Title 18 of the Code of Federal Regulations (CFR) Part 39.

The brief report is prepared by the impacted registered entities for all qualifying events and then sent to the applicable RE for review. The RE then forwards it to NERC. A brief report includes items identified in Appendix C: Brief Report Template. The brief report template may also be used for non-qualifying events that produce useful lessons learned for the industry.

An EAR is required for Category 3 events and may be requested for lower-level events. An EAR is prepared by the impacted entity, a group of impacted entities, or relevant members of an event analysis team as defined in the planning meeting. It addresses in detail the sequence of events as they happened, the identified causal factors, and the appropriate corrective actions. Appendix D: Event Analysis Report Template can be used as a guideline. Once completed, the EAR is sent to the applicable REs for review. These documents are sent to NERC upon completion.

In the brief report or EAR, registered entities are encouraged to include one-line diagrams or other diagrams and representations of the facility(ies) involved in the event.

The final EAR should address corrective actions and recommendations related to the event's causal factors and any identified lessons learned. Positive outcomes identified during an event should be documented.

If any applicable governmental authorities (AGAs) initiate a formal review process in conjunction with NERC,[14] the decision on the composition of the event analysis team, the team lead, the information needed from affected registered entities, and the required scope of the analysis will be discussed and agreed upon by the AGAs and NERC executive staff.

Lessons Learned from Events (Step 5)

Lessons learned as a result of an event analysis should be shared with the industry in accordance with timing, as referenced in Appendix A. Proposed lessons learned should be drafted by a registered entity utilizing Appendix E: Lessons Learned Template, and should be submitted to the applicable RE. The lessons learned should be detailed enough to be of value to others, but should not contain data or information that is deemed confidential. When possible, one-line diagrams or other representations should be included to enhance the information provided in the lessons learned. Vendor-specific information should not be included unless it is discussed and coordinated with the vendor. If dissemination of vendor-specific information is beneficial, it may be pursued outside the EAP.

Lessons learned will be reviewed by selected technical groups and NERC staff for completeness and appropriateness prior to posting.

Event Closure (Step 6)

Following the receipt of final reports, NERC and the RE will evaluate and close the event upon review and analysis of brief reports, EARs, and lessons learned. The RE will notify the registered entity(ies) involved that an event has been closed upon notification from NERC.

Lessons Learned from Other Occurrences

Any occurrence on the BES may yield lessons of value to the industry. Lessons learned can include the adoption of unique operating procedures, the identification of generic equipment problems, or the need for enhanced personnel training. In such cases, an event analysis would not be required, but the ERO EAP encourages registered entities to share with their RE any potential lessons learned that could be useful to others in the industry.

---

[14] As specified in the ERO ROP, Section 807.f, the NERC president and chief executive officer has the authority to determine whether any event warrants analysis at the NERC level. A Regional Entity may request that NERC elevate an analysis of a major event to the NERC level.

Confidentiality Considerations

Information and data designated as confidential by the entity supplying the data/information in the course of an event analysis shall be treated as confidential. In addition, all Critical Energy Infrastructure Information (CEII) shall be treated accordingly and may be designated as CEII by the entity supplying the information or by NERC or its REs. By participating in the EAP, a United States entity acknowledges that any of its brief reports, EARs, or both may be disseminated to an AGA, upon request, in accordance with Section 1500 of the Rules of Procedure.

Appendices and Other Suggested References

Appendix A: Target Time Frames for Completion of Brief Reports, EARs, and Lessons Learned

Appendix B: Planning Meeting Scope Template

Appendix C: Brief Report Template

Appendix D: Event Analysis Report Template

Appendix E: Lessons Learned Template

Other References:

- Attributes of a Quality Event Analysis Report
- Attributes of a Quality Lessons Learned
- NERC Blackout and Disturbance Analysis Objectives, Analysis Approach, Schedule, and Status – Attachment D from Appendix 8 of NERC Rules of Procedure
- Cause Analysis Methods for NERC, Regional Entities and Registered Entities

For additional data submission information regarding particular event categories see the supporting documents below on the EA Program page under reference materials.

- Addendum for Category 1h Events
- Addendum for Category 1a Events
- Addendum for Events with Failed Station Equipment
- NEI-NERC White Paper: Nuclear Power Plant Loss of Offsite Power Events - NERC Reporting Guidelines
- Addendum for Determining Event Category)

The EAP, appendices, and reference documents are posted on the EA Program page on the NERC website. To access the EA Program page on the NERC website, click on the Program Areas & Departments tab at the top of the NERC home page, then Event Analysis, Reliability Assessment, and Performance Analysis on the left side of the page, then EA Program under Event Analysis. The latest versions of the appendices are posted under the Current Event Analysis Process Documents tab.

Revision History

Rev.	Date	Reviewers	Revision Description
1	December 2011	Event Analysis Working Group (EAWG), NERC Management, Operating and Planning Committees.	Document endorsed by Operating and Planning Committees January 2012. Document endorsed by NERC Board of Trustees February 2012.
2	July 2013	Event Analysis Subcommittee (EAS), NERC Management, NERC Operating Committee.	Document endorsed by Operating Committees June 18, 2013.
3	September 2015	Event Analysis Subcommittee (EAS), NERC Management, NERC Operating Committee.	Document endorsed by Operating Committees September 16, 2015.
3.1	December 2016	Event Analysis Subcommittee (EAS), NERC Management, NERC Operating Committee.	Document endorsed by Operating Committees December 13, 2016.
4	December 2019	Event Analysis Subcommittee (EAS), NERC Management, NERC Operating Committee.	Document endorsed by Operating Committees December 10, 2019
5	September 2023	Event Analysis Subcommittee (EAS), Reliability & Security Technical Committee (RSTC)	

Document	ERO Event Analysis Process and Appendices - Version 5.0
Instructions	**Please use this form to submit comments on the draft Event Analysis Process and Appendices. Comments must be submitted within the review period below to NERC (brad.gordon@nerc.net) with the words "Version 5.0 ERO EAP and Appendices Comments" in the subject line. Only comments submitted in this Microsoft Excel format will be accepted. Both general and specific comments should be provided within this form. Red-line document changes, PDF versions of this document, or email comments will NOT be accepted.** Comments may be submitted by individuals or organizations. Please provide the requested information in Row 6. If comments are submitted on behalf of multiple organizations, list all organizations in Row 6. Please provide the Industry Segment and Region (if applicable) in Rows 7 and 8 and provide the requested contact information in Rows 9 and 10. If you have any questions regarding this process, please contact Stephen Crutchfield (Stephen.Crutchfield@nerc.net) or Brad Gordon (Brad.Gordon@nerc.net)
Review Period	**April 5, 2023 - May 19, 2023** ***Comments must be submitted using this comment form by 5:00 p.m. ET on May 19, 2023***

Name of Individual or Organization(s) (list multiple if submitted by a group):	Consolidated Comments with EAS Responses
Industry Segment (if applicable)	
Region (if applicable)	
Contact Telephone	
Contact Email	

Organization(s)	**Page #**	**Document Name/Line #**	**Comment**	**Proposed Change**	**NERC Response**
Thomas E. Foltz on behalf of American Electric Power	N/A	Entire Document	Please note, all page numbers noted in our comments are those shown in the page footers of the redlined draft.	N/A	
Thomas E. Foltz on behalf of American Electric Power	Page 3	Lines 171-173	The phrase "a common disturbance" was struck, however these words provided the context and clarity needed for this category.	Please replace "An event" with "a common disturbance" so that it instead reads "An outage contrary to design, of three or more BES Facilities caused by a common disturbance."	An event is defined as "a single incident or multiple incidents due to a common electrical initiating cause that results in an undesirable impact to the BES" in the Categorizing Events section on page 2 of the EAP.
Thomas E. Foltz on behalf of American Electric Power	Page 3	Category 1A	This category, along with its subparts, does not align with related text in Form DOE-417, the EOP-004 standard, the Brief Report Template (Appendix C), or the Event Analysis Report Template (Appendix D) . Passages from the first two are provided below. Please revise Category 1A to align with all these references. Examples include the following... DOE-417: "Unexpected Transmission loss within its area, contrary to design, of three or more Bulk Electric System Facilities caused by a common disturbance (excluding successful automatic reclosing)." EOP-004: Transmission Loss is defined as "Unexpected loss within its area, contrary to design, of three or more BES Facilities caused by a common disturbance (excluding successful automatic reclosing)."	Please revise Category 1A to align with all the references specified in our comments.	Thank you for your comment. While the OE-417 or EOP-004 reporting provides notification to the ERO EA of a potential event the EAP is not intended to mirror the exact language or criteria from the aforementioned reporting documents. The EAP stands on its own merits from a categorization standpoint.

Thomas E. Foltz on behalf of American Electric Power	Page 4	Lines 200-204	AEP seeks clarity on exactly which registered entity is required to create report(s) for items I and j, as these asset types cross transmission and generation boundaries. For example, the GO entity that owns a windfarm is likely not the same entity that owns the assets to which the windfarm is interconnecting to. Additional clarity would serve to prevent reports from not being submitted, due to one entity presuming the other entity provided the report.		Thank you for your comment. If there is a question regarding the appropriate reporting entity then the Regional Entity should be consulted.
Thomas E. Foltz on behalf of American Electric Power	Page 4	Line 224	Item 3a: Due to the separation of Registered Entities (GO, TO), only the RC/RTO has the information of the total aggregated loss of generation. Provide clarification to clearly indicate which entity has the responsibility to report.		Thank you for your comment. If there is a question regarding the appropriate reporting entity then the Regional Entity should be consulted.
Edison Electric Institute	N/A	N/A	General Comments: EEI appreciates the opportunity to provide comments on the ERO Event Analysis Process (EAP). We note that the document line numbers used in this spreadsheet link to the Redline Version, noting the redline and clean version line numbers do not align.	No proposed change, simply clarifications.	Thank you for your comments.
Edison Electric Institute	N/A	N/A	General Comment: Changes to the EAP will impact registered entities internal processes and procedures.	This process should include an implementation period to allow entities to change their internal processes to align with the proposed changes.	The EAP version 5 will not become effective without time for industry to assess the changes.
Edison Electric Institute	iv	56 - 58	Off-normal occurrences (ref. Section 808 of the Rules of Procedure) appear to have been added to the Event Analysis Process (EAP), however, there is no definition or process defined.	EEI asks that the term be defined and adjustments to the process be added to this document so that entities can understand their responsibilities related to this change.	Thank you for your comment. The definition and context of "off-normal occurrances" is provided in Section 808 of the NERC Rules of Procedure. There have been no changes to the scope of the EAP event categorization due to this addition.
Edison Electric Institute	iv	60 - 64	The proposed revision adds new text that introduces confusion and uncertainty. Refer to lines 60 through 64, where the revised text highlights the ERO's expectation – that registered entities participate and report certain events – while simultaneously declaring that the EAP is not mandatory. The EAS should affirm that a registered entities participation in the EAP is voluntary, not mandatory.	The EAS should remove text referring to the ERO's expectations for participation and reporting.	Thank you for your comment. The Introduction has been revised to address this concern and to provide clarity.
Edison Electric Institute	iv	65	The revised EAP speaks to the analysis of "criterion-based events" which is an undefined term.	EEI asks that "criterion-based events" either be defined or removed from the EAP.	Thank you for your comment. The term "criterion-based event" is referring to the category definitions of the EAP. The Introduction has been revised to address this concern and to provide clarity.

Edison Electric Institute	iv	68	The revised EAP states that the EAP reviews "discretionary occurrences", which is a new term within the EAP. It is unclear what "discretionary occurrences" are now in scope.	Please provide some context to the reference to "discretionary occurrences" so that registered entities might better understand their responsibilities relative to reporting and providing data.	Thank you for your comment. The aforementioned referencee is to the ERO Event Analysis Program of which the Event Analysis Process is a subset. The Introduction has been revised to address this comment and to provide clarity.
Edison Electric Institute	iv	69	The revised EAP states that the EAP is a criterion-based process. EEI assumes that this refers to the identified categories used to trigger event analysis.	Please confirm our understanding of the EAP reference to criterion-based process conforms to the EAS intent and please add the criteria that will be used for "off normal occurrences" that now appear to be a part of the EAP process.	Thank you for your comment. The term "criterion-based event" is referring to the category definitions of the EAP. The Introduction has been revised to address this concern and to provide clarity.
Edison Electric Institute	iv	68 - 69	The revised EAP states that "EAP is to provide the ERO a way to identify operating patterns and technical anomalies that potentially place the system in peril or indicate the potential for future at risk scenarios. Trending of event impacts that meet risk-based criteria serve to inform patterns in entity design and operating practices".	Please provide some context to the process that will be used to identify the "operating patterns and technical anomalies" that the EAP intends to analyze, along with some background to support this expansion of the process so that registered entities can better understand their responsibilities relative to this change. We also ask that the "risk-based criteria" that will be used be defined. Lastly, EEI would like to better understand what is intended by the interest in entity "design and operating practices". The NERC Reliability Standards define certain designs and operating practices. Are we to understand that the ERO will be expanding their review of entity designs and operating practices beyond those Reliability Standards? Please explain what is intended so that registered entities can better understand this scope change.	Thank you for your comment. The revisions in version 5 of the EAP do not represent a change of the current scope. The Introduction has been revised to address this comment and to provide clarity.
Edison Electric Institute	iv	77	While we agree that it is important to understand how an event occurs, we do not agree that this should replace the analysis of why the event occurred.	EEI supports adding "how" to the analysis process but we do not agree this should replace the analysis of "why" the event occurred in the process.	Thank you for your comment. The revisions in version 5 of the EAP do not represent a change of the current scope. The Introduction has been revised to address this comment and to provide clarity.
Edison Electric Institute	iv	79	In the context of identifying the sequence of events, it remains important to understand "what happened".	EEI suggests that "what happened" be restored to the text of the EAP.	Thank you for your comment. The revisions in version 5 of the EAP do not represent a change of the current scope. The Introduction has been revised to address this comment and to provide clarity.
Edison Electric Institute	iv	80	EEI supports the added reference to the ERO Cause Code Assignment Process but there should also be a link to that process document.	EEI recommends adding a hyperlink (or footnote) to the ERO Cause Code Assignment Process document.	Thank you for your comment. The EAS agrees with your comment and a footnote has been added.
Edison Electric Institute	1	96 - 99	It is unclear why the existing 5 categories were reduced to a 3 categories. While there were likely good reasons to make this change, this should be explained to the industry as a way to better inform registered entities to the changes in this process.	EEI recommends that the EAS hold a webinar to explain the changes to the ERO EAP process. This would help registered entities to better understand the reasons for the changes, while providing a forum for the exchange of thoughts and ideas beyond the EAS committee meetings.	Thank you for your comment. The EAS will be conducting informational webinar(s) to review and discuss changes to the EAP.

Edison Electric Institute	1	102 - 103	EEI suggests that references made regarding "discrete incident or linked incidents with a common electrical initiating cause" should be clarified and incorporated into the categories where this applies so that registered entities who experience such an event will understand how to link such incidents and appropriately report such an event.	EEI asks for additional clarity on the identified "discrete incidents or linked incidents with a common electrical initiating cause". We are assuming this is a reference to IBR events associated with a common disturbance but this should be clarified and identified in the specific categories.	Thank you for your comment. An event is defined as "as a single incident or multiple incidents due to a common electrical initiating cause that results in an undesirable impact to the BES". This definition has been revised to address this comment and provide clarity in the ERO Event Analysis Process section on page 2.
Edison Electric Institute	1	105 - 106	The changes in the EAP document introduce confusion regarding the initiation of the event analysis process. As drafted, the EAP ignores the possibility that an OE-417 or EOP-004 report may not be appropriate if no EOP-004 reportable event has occurred. For reportable but non-major events such as those required by EOP-004, we believe a modified Brief Report that includes a sufficient level of detail under a voluntary reporting program can be prepared with minimal burden and support the EAP's objectives. Additionally, the modified Brief Report can be submitted quarterly through the Align portal.	Beginning at line 105, suggested modifications include the following text and footnote: The event analysis process can begin when (1) the ERO receives notification of a potential event via receipt of an OE-417 or EOP-004; (2) the registered entity submits a Brief Report to the Regional Entity; or (3) the registered entity submits a modified Brief Report via the Align Portal and the ERO or Regional Entity request a full Brief Report. [Insert Footnote ##] The foundation for success of the notification and reporting processes is with the initial communication and coordination between the registered entity and the Regional Entity in Steps 1-3. [Footnote ##: OE-417 or EOP-004 reports are submitted when an event is reportable as both an EAP event and as an EOP event. A Brief Report should be submitted if a Registered Entity experiences non-major event that meets the EAP criteria AND the Registered Entity believes there is opportunity for industry learning and best practices. A modified Brief Report should be uploaded to the Align Portal if the Registered Entity experiences non-major event that meets the EAP criteria BUT does not believe there is	Thank you for your comment. While the OE-417 or EOP-004 reporting typically provides notification to the ERO EA of a potential qualified event the EAP is not intended to mirror the exact language or criteria from the aforementioned reporting documents. The EAP stands on its own merits from an categorization standpoint. In the event that an entity is unsure whether a report should be submitted in accordance with the EAP the Regional Entity should be consulted as referenced in Step 2 on page 1. Further, the Align Portal is a CMEP tool and it is not appropriate to be used for EAP purposes.

Edison Electric Institute	1	102 - 110	EEI notes that "Off-normal Occurrences" are not currently identified in the process.	Off-normal occurrences should be clearly identified in the process (and defined & explained) if they are to be included in the EAP.	Thank you for your comment. The definition and context of "off-normal occurrances" is provided in Section 808 of the NERC Rules of Procedure. There have been no changes to the scope of the EAP event categorization due to this addition. Off-normal occurrences, for EAP purposes, are defined in the ERO Event Analysis Process section of the EAP on pages 2 & 3.
Edison Electric Institute	1	112 - 113	Step 1 changes do not appear to align with the process as described later in this document. We further note that the focus on registered entity analysis has been diminished through the proposed change.	EEI suggest restoring the original Step 1 language or consider the following suggested language: Step 1: The registered entity will assess an event. If the registered entity determines an event meets Category 1-3 criteria, the registered entity will report the event.	Thank you for your comments. Step 1 in the Process Overview section on page 1 has been revised to address this comment and provide clarity.
Edison Electric Institute	2	123 - 157	EEI notes that "Off-normal Occurrences" are not mentioned in Step 1.	Please identify who, how and under what circumstances a registered entity is to report "Off-normal occurrences". We are of the belief this should be thre responsibility of NERC or the RE.	Thank you for your comment. The definition and context of "off-normal occurrances" is provided in Section 808 of the NERC Rules of Procedure. There have been no changes to the scope of the EAP event categorization due to this addition. Off-normal occurrences, for EAP purposes, are defined in the ERO Event Analysis Process section of the EAP on pages 2 & 3.
Edison Electric Institute	2	138 - 139	The EAP states that "If an event is experienced that meets Category 1-3 criteria the primary focus should be restoration and then communication with the Regional Entity on reporting per appendix A ."	Appendix A provides 10 days for sending the interim report to the Regional Entity. No consideration is given for time spent on system restoration efforts. Please clarify what is intended here.	Thank you for your comment. The aforementioned reference simply states that EAP submittals should not be performed at the expense of restoration efforts. Further, Appendix A Target Timeframes Template states on page 1 footnote 1 that "All timeframes are subject to extension to ensure accurate and complete information with agreement of the applicable Regional Entity."
Edison Electric Institute	3	171 - 176	The previous version of the EAP linked closely to the EOP-004 Reliability Standard, however, Category 1a now uses language that differs from that Reliability Standard.	Please explain why the defined term "disturbance" has been replaced with the undefined term "event". Moreover, it is unclear why the EAS chose language that does not align with EOP-004 or OE-417. Please clarify the change broadly.	Thank you for your comment. An event, for EAP purposes, is defined in the ERO Event Analysis Process section of the EAP document. The EAP is not a compliance standard and the terms therein need not be terms defined in the NERC Glossary. An event is defined as "a single incident or multiple incidents due to a common electrical initiating cause that results in an undesirable impact to the BES" in the Categorizing Events section on page 2 of the EAP.
Edison Electric Institute	3, 4	182, 215, 229	EEI notes that "unintended" has been removed from Categories 1e, 2e and 3e.	EEI asks for clarification as to why "unintended" was removed from these categories.	Thank you for your comment. The term "unintended" was often subjective in interpretation and was replaced with the term "contrary to design" to add clarity.
Edison Electric Institute	4	217 - 218	EEI questions the removal of "contrary to design" from Category 2f.	EEI asks for clarification as to why this language was removed.	Thank you for your comment. The definition of a Category 2f has been revised to address this comment and provide clarity.

Edison Electric Institute	4	233 - 234	EEI believes that Category 3e should contain a "Bright-Line" to assist entities in the gathering of data. It is widely understood that unregistered IBR owner have no reporting obligations.	To address this concern, we offer the following edits to Cat. 3e for EAS consideration: Loss of NERC registered transmission connected generation (including inverter-based resources) in any one interconnection of 2,000 MW or more. This excludes RAS action that performed as designed. This excludes distribution connected resources.	Thank you for your comment. The EAS believes that all resources have a potential impact on the reliability of the BES. If the reporting entity (i.e. BA, RC, etc.) has visibility of IBR resources in their balancing area they should be included in the Category 3e thresholds.
FirstEnergy	N/A	N/A	FirstEnergy supports EEI's comments and additionally offers these comments.	General comment.	Thank you for your comments.
FirstEnergy	iv	Line 63 and 64	The EAP is not a mandatory process but participation is expected." The word "expected" can imply a requirement, which would contradict the first part of the sentence. I recommend using the word "encouraged" instead of "expected"	FE questions why this was changed to expected. Our understanding is this is not a mandatory process. If intent is optional, then Line 63 could read " The EAP is not a mandatory process but participation and reporting is encouraged."	Thank you for your comment. The Introduction has been revised to address this concern and to provide clarity.
FirstEnergy	iv	68	Line 68-69 reads "The Event Analysis Program reviews discretionary occurrences, major events and other off-normal system occurrences in conjunction with the criterion-based EAP". The term"discretionary occurrences" is objective and not clearly defined.	FE recommends EAS to define term used or remove from Guide.	Thank you for your comment. The aforementioned referencee is to the ERO Event Analysis Program of which the Event Analysis Process is a subset. The Introduction has been revised to address this comment and to provide clarity.
FirstEnergy	iv	Line 83	"including, such as a NERC Alert,…" is a poor sentence structure. It should be revised to be more clear.	FirstEnergy suggest Lines 80 - 82 to read "The analysis of an event drives the ERO Cause Code Assignment Process which can then be used to identify trends that can support changes to Reliability Standards or disturbance reporting."	Thank you for your comment. The aforementioned reference in the Introduction section has been revised to improve sentence structure and provide clarity.
FirstEnergy	1	Line 112	The affected registered entity no longer assesses the event and determines the category, they just report the event.	FirstEnergy suggest Line 112 read "Step 1: The registered entity will report the event and assesses the Category of the event determined by the ERO Event Analysis Process guide provided."	Thank you for your comment. Step 1 in the Process Overview section on page 1 has been revised to provide clarity.
FirstEnergy	3	Line 171-176	In the past NERC and DOE looked to align the reporting categories in the EAP, EOP-004 and DOE's OE-417. Some of the V5 proposed changes are drifting away from that alignment. EOP-004 and OE-417 still use the "unexpected" and "disturbance" terms.	FirstEnergy supports EEI's comments to ensure alignment of EOP-004 and DOE's OE-417 documents and processes.	Thank you for your comment. While the OE-417 or EOP-004 reporting provides notification to the ERO EA of a potential qualified event the EAP is not intended to mirror the exact language or criteria from the aforementioned reporting documents. The EAP stands on its own merits from an categorization standpoint. In the event that an entity is unsure whether a report should be submitted in accordance with the EAP the Regional Entity should be consulted as referenced in Step 2 on page 1.
FirstEnergy			General Comment: Changes to the EAP will impact registered entities internal processes and procedures.	FirstEnergy recommends a minimum of 6 months for a period of implementing these updates.	The EAP version 5 will not become effective without time for industry to assess the changes.

FirstEnergy	1	105-106	The changes in the EAP document introduce confusion regarding the initiation of the event analysis process. As drafted, the EAP ignores the possibility that an OE-417 or EOP-004 report may not be appropriate if no EOP-004 reportable event has occurred.	FirstEnergy supports EEI's comments to ensure alignment of EOP-004 and DOE's OE-417 documents and processes. Beginning at line 105, suggested modifications include the following text and footnote: The event analysis process can begin when (1) the ERO receives notification of a potential event via receipt of an OE-417 or EOP-004; (2) the registered entity submits a Brief Report to the Regional Entity; or (3) the registered entity submits a modified Brief Report via the Align Portal and the ERO or Regional Entity request a full Brief Report. [Insert Footnote ##] The foundation for success of the notification and reporting processes is with the initial communication and coordination between the registered entity and the Regional Entity in Steps 1-3. [Footnote ##: OE-417 or EOP-004 reports are submitted when an event is reportable as both an EAP event and as an EOP event. A Brief Report should be submitted if a Registered Entity experiences non-major event that meets the EAP criteria AND the Registered Entity believes there is opportunity for industry learning and best practices. A modified Brief Report should be	Thank you for your comment. While the OE-417 or EOP-004 reporting typically provides notification to the ERO EA of a potential qualified event the EAP is not intended to mirror the exact language or criteria from the aforementioned reporting documents. The EAP stands on its own merits from an categorization standpoint. In the event that an entity is unsure whether a report should be submitted in accordance with the EAP the Regional Entity should be consulted as referenced in Step 2 on page 1. Further, the Align Portal is a CMEP tool and it is not appropriate to be used for EAP purposes.
ATC	NA	ERO Event Analysis Process Document Version 5.0- Redline	ATC supports the comments of EEI		Thank you for your comments.
ATC	NA	ERO Event Analysis Process Document Version 5.0- Redline- Line #217	Category 2.f reference to “extreme weather event” may cause confusion ATC recommends dropping that caveat. Also, this does not read as requiring a report for 300 MW or more of firm load shed; it speaks to loss of load, which means unexpected loss or unintended loss. If that is the not the author’s intent, more clarity is needed.		Thank you for your comment. The definition of a Category 2f has been revised to address this comment and provide clarity.
Bonneville Power Administration	1	EAP	New language states “electrical initiating cause”. Does this mean that events initiated by non-electrical causes such as misoperation of transformer sudden pressure relays are excluded from reporting?	No proposed changes. BPA is seeking clarity from the document drafting team.	Thank you for your comment. An event is defined as "as a single incident or multiple incidents due to a common electrical initiating cause that results in an undesirable impact to the BES". This definition has been revised to address this comment and provide clarity in the ERO Event Analysis Process section on page 2. The specific category definitions are found in the ERO Event Analysis Process section on pages 2 & 3.
Manitoba Hydro	3	Category #1c/Line #179	Is there such a thing called "non-BES RAS"?	Failure or misoperation of a BES RAS that introduces unintentional or unacceptable reliability risk to the BES, as per PRC-012-2	Thank you for your comment. Remedial Action Scheme (RAS) is a term defined in the NERC Glossary. This definition is applicable for use in the EAP.
Manitoba Hydro	4	Category #2f/Line #217	What is considered as firm load?		Thank you for your comment. Firm Demand (i.e. Firm Load) is a term defined in the NERC Glossary. This definition is applicable for use in the EAP.

Manitoba Hydro	4	Category #2f/Line #218	What is considered as extreme weather event?		Thank you for your comment. The criteria for category 2f has been revised to provide clarity and reference to weather has been removed.
Manitoba Hydro	4	Category #3d/Line #232	Does the "dc tie" here mean the complete DC connection between the asynchronous resources and the system? If this DC connection includes more than one bipoles for example, and we lose only of the the bipoles, does this meet the category 3d criteria? If the other bipoles can pick up the load and no generation is lost, does this still qualify? Does 2000MW indicate total capacity or what's in service at the time?		Thank you for your comment. The criteria defined in category 3d has been revised to address this comment and provide clarity. The threshold is the total loss of MW and could include one or more bipoles.
Manitoba Hydro	2	Category #1a/Line #171-176	Can you further clarify sub point a. ii. Does this indicates if the generation loss if less than 500 MW, it should not be reported? What is the difference between i and ii? BES Facilities include BES Generators already in the definition. Does 1.a.i refer to BES Transmission Facilties? Does i and ii need to be separated by "or"?		Thank you for your comment. In Category 1a.ii if the generation loss is less than 500 MW it does not need to be reported. Category 1a.i could include BES transmission, substation, and/or generation elements while category 1a.ii is specific to generation.
NPCC	1	ERO_EAP_Appendices_v5.0_Redline/6	In column 3 row 3 of the table, there is a missing space. Currently: 'Within90 business days of the event' Note: you need to look at the clean copy to see the missing space	Add a space: 'Within 90 business days of the event'	Thank you for your comment. This has been corrected in Appendix A.
NPCC	5	ERO_EAP_Appendices_v5.0_Redline/20	The added sentence is incomplete: 'Interim reporting can be used'	Suggest changing to: 'Interim reporting can be used as the initial report until the final report can be submitted'	Thank you for your comment. This has been corrected in Appendix A.
NPCC	15	ERO_EAP_Appendices_v5.0_Redline/53	I thought that we were removing the Region information from the LL form. The Region information hasn't shown up on the published LL since 2020.	Suggest removing: 'Region Contact Information' and 'Source of Lesson Learned: Region Name'	Thank you for your comment.
NPCC	13	ERO_EAP_v5.0_Redline/357	The referenced document doesn't exist: Addendum for Category 1a Events	Remove line 99: Addendum for Category 1a Events	Thank you for your comment.
Evergy			Evergy supports and incorporates by reference the comments of the Edison Electric Insitute (EEI).		Thank you for your comments.
Exelon Corp	N/A	N/A	General Comments: Exelon appreciates the opportunity to provide comments on the ERO Event Analysis Process. We note that the document line numbers used in this spreadsheet, link to the Redline Version.	No change, clarification	Thank you for your comments.

Exelon Corp	N/A	N/A	General Comment: The alignment of EOP-004/DOE-417 reporting and the EAP is desirable. Common language/terminology specifically for event types in both programs makes it easier for our personnel and our internal documents as in many cases these are parallel related programs for some event types. Some of the subtle changes with category terminology appears to be moving away from this alignment.	Further suggestions regarding this needed alignment is suggested in the comments below; however, other event types that are not being changed in this revision remain inconsistent with the DOE-417 event types. Exelon suggests a revisit of all event types to determine if further alignment between the two programs can be pursued.	Thank you for your comment. While the OE-417 or EOP-004 reporting provides notification to the ERO EA of a potential qualified event the EAP is not intended to mirror the exact language or criteria from the aforementioned reporting documents. The EAP stands on its own merits from an categorization standpoint. In the event that an entity is unsure whether a report should be submitted in accordance with the EAP the Regional Entity should be consulted as referenced in Step 2 on page 1.
Exelon Corp	N/A	N/A	General Comment: Changes to the EAP will impact registered entities internal processes and procedures.	The process change should include an implementation period to allow entities time to update their internal processes to align with the proposed changes.	The EAP version 5 will not become effective without time for industry to assess the changes.
Exelon Corp	3	171-176	The previous version of the EAP linked closely to the terminology in the EOP-004 Reliability Standard, however, Category 1a uses language that differs from that Reliability Standard.	Please explain why the defined term "disturbance" has been replaced with the undefined term "event". It is suggested that the EAS language remain aligned with the EOP-004/DOE-417 event language.	Thank you for your comment. An event, for EAP purposes, is defined in the ERO Event Analysis Process section of the EAP document. The EAP is not a compliance standard and the terms therein need not be terms defined in the NERC Glossary. An event is defined as "a single incident or multiple incidents due to a common electrical initiating cause that results in an undesirable impact to the BES" in the Categorizing Events section on page 2 of the EAP.
Exelon Corp	1	102-103	Exelon suggests that references made regarding "discrete incident or linked incidents with a common electrical initiating cause" should be clarified and incorporated into the categories where this applies so that registered entities who experience such an event will understand how to link such incidents and appropriately report such an event.	Exelon asks for additional clarity on the identified "discrete incidents or linked incidents with a common electrical initiating cause". This may be a reference to IBR events associated with a common disturbance but this should be clarified and identified in the specific categories.	Thank you for your comment. An event is defined as "as a single incident or multiple incidents due to a common electrical initiating cause that results in an undesirable impact to the BES". This definition has been revised to address this comment and provide clarity in the ERO Event Analysis Process section on page 2.
Exelon Corp	1	112-113	Step 1 changes do not appear to align with the process as described later in this document. It is further noted that the focus on registered entity analysis has been diminished through the proposed change.	Exelon suggests restoring the original Step 1 language or consider the following suggested language: Step 1: The registered entity will assess an event. If the registered entity determines an event meets Category 1-3 criteria, the registered entity will report the event.	Thank you for your comments. Step 1 in the Process Overview section on page 1 has been revised to address this comment and provide clarity.

Exelon Corp	2	155 - 157	In the last paragraph of Step 1 EAP Process it states "NERC encourages registered entities to report events of significance in an effort to share experiences and lessons learned with the industry. When such events are reported, these events will be categorized as unqualified or category 0." EEI assumes that "Off-normal occurrences" would also be "unqualified or category 0" events. Generally, unqualified or category 0 events are not routinely reported by registered entities because they are uncategorized, except in cases where they were initially believed to be a categorized event as a result of being "contrary to the design" but later assessed to be consistent with the design. Meaning, that in most cases the registered entity would not report an uncategorized event unless they were otherwise requested to do so by the responsible Regional Entity or NERC.	Exelon asks that the EAP be updated to clearly state that NERC and the Regional Entities are responsible for notifying the responsible entity when reporting is required for "unqualified or Category 0" events (i.e., off-normal occurrences).	Thank you for your comment. The aforementioned paragraph on page 2 of the ERO Event Analysis Process section has been revised to address your comment and provide clarity.
Southern Company			Southern Company supports comments submitted by EEI		Thank you for your comments.

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Electric Reliability Organization Event Analysis Process

Version ~~4~~5.0

Approved: ~~December~~ September ~~10~~xx, ~~2019~~2023

Effective Date: January 1, ~~2020~~2024

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.

MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

The ERO Event Analysis Process (EAP) document is intended to be used as a guideline to promote a structured and consistent approach to performing event analyses in North America. This document outlines a process that will facilitate greater communication and information exchange between registered entities, Regional Entities, and NERC.

The ERO Event Analysis Program exists for review of major system events and other off-normal system occurrences. The program is forensic in nature and focuses on the near-term to real-time operating horizons. The program is derived from the NERC Rules of Procedure (ROP) authorities/requirements outlined in Section 800 – Reliability Assessment and Performance Analysis. Section 800 specifies the need for analysis of off-normal occurrences on the Bulk Electric System (BES) that do not rise to the level of major events as described in the ~~section~~ROP. For purposes of the Event Analysis Program an event is defined as a single incident or linked incidents due to a common initiating cause resulting in an undesirable impact to the bulk electric system (BES). ~~Off-normal are those occurrences that include system operating outcomes other than expected by design and/or operating principles/methodologies during day-to-day operations.~~

The EAP is an approach specifically designed to address categorized events defined by the Event Analysis Subcommittee (EAS) in concert with the ERO that ~~potentially~~ could result in adverse impact~~(s) of significance~~ to the ~~system~~BES, provide ~~weak signals~~indication of future system risks, and/or ~~corroborate~~confirm ~~current~~known risks ~~of concern~~ to the BES. The process is a systematic approach to handle data collection and analysis of ~~criterion-based events~~events as defined by the EAP category criteria. The main objective is for the ERO and industry to learn from the events and to develop corrective actions to prevent recurrence. ~~– c~~Continuous improvement is the mindset that the process is designed to instill in industry design and operating practices.

The primary reason for participating in an event analysis is to determine if there are lessons to be learned and potential recommendations that can be shared with industry to mitigate the risk of recurrence. An effective EAP requires industry participation and support to assist ~~the ERO in fulfilling its obligations and providing industry actionable feedback~~in continuous improvement of BES performance.

Analyzed events feed the ERO Cause Code Assignment Process[1], which is used to identify trends. Trends help the ERO confirm known and expected reliability risks and identify~~inform ERO~~ emerging ~~reliability~~ risks. ~~and~~Resulting mitigation efforts ~~including~~could include NERC Alerts[1] and/or~~,~~ recommended changes to Reliability Standards and/or disturbance reporting.

The NERC Reliability and Security Technical Committee (RSTC) will oversee the ~~mainta~~maintenance of~~in~~ the EAP document through the EAS and~~under the~~ existing ERO documentation processes. The document will be periodically reviewed and updated by the EAS every three years or~~,~~ as needed. The ~~NERC~~ RSTC ~~will~~may solicit comments from industry during the review process.

The EAP does not exempt the registered entity from mandatory reporting requirements governed by regulatory authorities or NERC Reliability Standards.~~[2]~~[2]

~~The ERO Event Analysis Process (EAP) document is intended to be used as a guideline to promote a structured and consistent approach to performing event analyses in North America. This document outlines a process that will facilitate greater communication and information exchange between registered entities, REs, and NERC.~~ The ~~process is derived from the NERC Rules of Procedure (ROP) authorities/requirements outlined in Section 800 --~~

---

[1] https://www.nerc.com/pa/rrm/ea/EA%20Program%20Document%20Library/CCAP_Manual_2023.pdf

[2] Rules of Procedure (ROP) Section 810

~~Reliability Assessment and Performance Analysis. The section specifies the need for analysis off-normal occurrences on the bulk electric system that do not rise to the level of major events as described in the section.~~

~~The EAP is an approach used to focus on occurrences identified by the ERO that potentially could result in impact of significance to the system, weak signals of future system risks and/or corroborate current risks of concern. The ERO expects NERC registered entities to report system events in general with the EAP outlining specific event categories of interest that support current risk profiles of concern to the ERO. The EAP is not a mandatory process but participation and reporting is expected. The EAP is a systematic approach to handle data collection and analysis of criterion-based events within the ERO Event Analysis Program. The main objective is for the ERO and industry to learn from the events and to develop corrective actions to prevent recurrence -- continuous improvement is the mindset that the process is designed to instill in industry design and operating practices. The Event Analysis Program reviews discretionary occurrences, major events and other off-normal system occurrences in conjunction with the criterion-based EAP. The program is forensic in nature and focuses on the real-time to near-term operating horizons. The primary purpose of the EAP is to provide the ERO a way to identify operating patterns and technical anomalies that potentially place the system in peril or indicate the potential for future at-risk scenarios. Trending of event impacts that meet risk-based criteria serve to inform patterns in entity design and operating practices that may lead to the limits of acceptable impact/risk to the system.~~

~~The primary reason for participating in an event analysis is to determine if there are lessons to be learned and shared with the industry. The analysis process involves identifying what happened, why how it happened, and determining appropriate actions towhat can be done to prevent reoccurrence. Identification of the sequence of events answers the “how it happenedwhat happened” question and determination of the root cause of an event answers the “why” question. . The analysis of an event drives the ERO Cause Code Assignment ProcessIt also allows for events to have cause codes or characteristics and attributes assigned, which can then be used by the Event Analysis Subcommittee (EAS) to identify trends. Trends inform ERO reliability risk and mitigation efforts includingmay identify the need to take action, such as a NERC Alert[3], or may support changes to Reliability Standards or disturbance reporting.~~

~~The NERC Reliability and Security Technical Committee (RSTC) Operating Committee (OC)EAS will maintain the EAP document under the existing ERO documentation process. The document will be reviewed and updated by the EAS, as needed. The NERC OC RSTC or EAS? will solicit comments from industry during the review process.~~

~~The EAP does not exempt the registered entity from mandatory reporting requirements governed by regulatory authorities or NERC Reliability Standards.~~[4]

---

[3] ~~Rules of Procedure (ROP), Section 810~~

[4] ~~The purpose of the voluntary EAP is to determine the how, what, and why of an event vs. the notification process required in the current version of NERC Standard EOP-004. This difference in the purpose of the EAP vs. EOP explains the similar but different reporting criteria in part. Reporting (notification) under EOP is mandatory, immediate, and brief, and is intended to notify other entities that an event has taken place on the Bulk Electric System (BES) or BES control facilities. Reporting through the EAP is intentional, analytic, methodic, and detailed.~~

Process Overview

The EAP maintains three categories of pre-defined criteria that serve to drive data collection efforts for use in identifying ~~the aforementioned~~ system impacts and risks. Each category describes the ~~level of perceived system~~ impact to the BES and the EAP provides industry with the ~~expected~~ level of analysis ~~required by industry~~necessary ~~in preparation for~~to accurately report~~ing~~ ~~on~~ the event to the ERO~~ through the EAP~~. ~~To ensure consistency, the EAP uses the following top-level ERO EA Program definition for an individual event:~~ :

~~A discrete incident or linked incidents with a common electrical initiating cause that results in an undesirable impact to the bulk electric system contrary to design or operating practices and procedures.~~

The event analysis process most often begins when the ERO receives notification of a potential event via receipt of an OE-417 or EOP-004 or receipt of a brief report. ~~The~~A foundation for success of ~~the notification and reporting processes~~EAP is ~~with~~in the initial communication and coordination between the registered entity and the RE described in ~~Steps 1-3~~the steps below. A primary reason for participating in an event analysis is to determine if there are ~~good~~ practices and lessons to be learned and shared with the industry. The six steps below support this objective. ~~and this must be remembered during each of the six steps listed:~~

Step 1: The registered entity assesses an event, proposes the event category in accordance with the EAP, and reports the event to the RE.~~The registered entity assesses an event, determines the event categorywill report the event, and notifies the RE.~~ .

Step 2: A planning meeting or coordination call (Appendix B) is held between the registered entity and the RE when possible.

Step 3: The registered entity submits a Brief Report (Appendix C) to the RE.

Step 4: The registered entity submits an Event Analysis Report (EAR) (Appendix D) to the RE, if needed.

Step 5: Lessons learned (Appendix E) are developed and shared with industry as appropriate.

Step 6: The EAP is closed.

Categorizing Events (Step 1)

When a registered entity experiences an event, that entity will ~~recommend~~ propose an initial category for the event as outlined in ~~the Categorization of Events~~this section. The categories listed in ~~the Categorization of Events~~this section do not cover all possible events. The need for analysis may be discussed by all affected registered entities, the appropriate REs, and NERC.

Registered entities that reside in multiple RE footprints should notify all relevant REs of an event that spans those Regions. NERC and the REs will determine a lead RE for the event, and further communication will take place between the registered entity and the lead RE.[5]

If an event is experienced that meets Category 1-3 criteria the primary focus should be restoration and then communication with the RE on reporting per appendix A. ~~If a weather-related occurrence falls within any of the categories, it should be communicated to the RE. The affected registered entities should focus on restoration efforts. For weather-related events,~~ the ~~highest category that characterizes an event should be used, even though the cause may be determined to be limited to weather.~~

~~For Category 3 and above weather-related occurrences, the RE will collaborate with affected registered entities to determine if any additional information or event analysis steps are needed for the purposes of learning from these events.~~

~~For weather-related events, the primary reason for participating in an event analysis is to determine if there are good practices and lessons to be learned and shared with the industry.~~

Qualifying events are assigned to one of ~~five~~ three categories based on potential reliability impact to the BES. The event categories are intended to allow the registered entity and RE to objectively identify event thresholds. The highest category that characterizes an event should be used.

The categories listed in this section do not cover all possible events. Events of interest that do not meet EAP reporting criteria may be identified by NERC, the RE, or the registered entity. In these cases a report may be submitted or requested in an effort to share experiences and lessons learned with the industry. These unqualified events will be categorized as Category 0.
~~NERC encourages registered entities to report events of significance in an effort to share experiences and lessons learned with the industry. When such events are reported, these events will be categorized as unqualified or category 0.~~

---

[5] ERO Enterprise Guide for the Multi-Region Registered Entity Coordinated Oversight Program, March 2018, Section IX: System Events

Category 1: An Event that Results in One or More of the Following:

a. An outage, contrary to design~~,~~ of three or more BES Facilities caused by an ~~E~~event:

~~a. An unexpected outage, that is contrary to design, of three or more BES Facilities caused by a common disturbance[6]:~~

  ~~ii.~~i. The outage of a combination of three or more BES Facilities (excluding successful automatic reclosing)

  ~~iii.~~ii. The outage of an entire generation station of three or more generators (aggregate generation of 500 MW to 1,999 MW)[7]; each combined-cycle unit is counted as one generator.

b. ~~Intended and controlled system separation by the proper operation of a remedial action scheme (RAS) in New Brunswick or Florida from the Eastern Interconnection~~ ~~Intended and controlled system separation by the proper operation of a remedial action scheme (RAS) in New Brunswick or Florida from the Eastern Interconnection~~Retired on January 1, 2023

c. Failure or misoperation of a BES Remedial Action Scheme (RAS)

d. ~~System-wide voltage reduction of 3% or more that lasts more than 15 continuous minutes due to a BES Emergency~~ Retired on January 1, 2023

e. BES system separation contrary to design that results in an island of 100 MW to 999 MW. This excludes BES radial connections and non-BES (distribution) level islanding

~~e. Unintended BES system separation that results in an island of 100 MW to 999 MW. This excludes BES radial connections and non-BES (distribution) level islanding~~

f. ~~Unplanned evacuation from a control center facility with BPS SCADA functionality for 30 minutes or more.~~ Retired on January 1, 2016

g. In ERCOT, ~~unintended~~ loss of generation of 1,400 MW to 1,999 MW

h. Loss of monitoring[8] and/or control[9] at a Control Center such that it degrades[10] the entity's ability to make Real-time operating decisions that are necessary to maintain reliability of the BES in the entity's footprint for 30 continuous minutes or more

~~Loss of monitoring or control at a control center such that it significantly affects the entity's ability to make operating decisions for 30 continuous minutes or more.~~

~~[6] As defined in the NERC Glossary of Terms: Disturbance – 1. An unplanned event that produces an abnormal system condition. 2. Any perturbation to the electric system. 3. The unexpected change in ACE that is caused by the sudden failure of generation or interruption of load.~~

[7] Gross MW output of the generators at the time of the outage.

[8] The ability to accurately receive relevant information about the BES in Real Time and evaluate system conditions using Real-time data to assess existing (pre-Contingency) and potential (post-Contingency) operating conditions to maintain reliability of the BES

[9] The ability to take and/or direct actions to maintain the reliability of the BES in Real Time via entity actions or by issuing Operating Instructions

[10] For purposes of 1h categorization "degrades" means less-than required functioning of any monitoring/control component, process, or capability.

Some examples that should be considered for EA reporting include, but are not limited to the following. ~~:~~Additional cases are provided in the Addendum for Category 1h Events found under reference materials for event analysis on the EA Program website.[11]

1. Loss of operator ability to remotely monitor or control BES elements
2. Loss of communications from SCADA remote terminal units (RTU)
3. Unavailability of ICCP links, which reduces BES visibility
4. Loss of the ability to remotely monitor and control generating units via automatic generation control (AGC)
5. Unacceptable state estimator or real time contingency analysis solutions

~~h.~~i. A non-consequential interruption[12] of inverter type resources[13] aggregated to 500MW or more not caused by a fault on its inverters, or its ac terminal equipment.

~~i.~~j. A non-consequential interruption[14]~~[6]~~ of a ~~dc~~ DC tie(s), between two separate asynchronous systems, loaded at 500 MW or more, when the outage is not caused by a fault on the dc tie, its inverters, or its ac terminal equipment.

Category 2: An Event that Results in One or More of the Following:

a. Complete loss of interpersonal communication and alternative interpersonal communication capability affecting its staffed BES control center for 30 continuous minutes or more.

b. ~~Complete loss of SCADA, control or monitoring functionality for 30 minutes or more.~~ Retired on January 01, 2016 refer to Category 1h

c. BES Emergency resulting in a voltage deviation of ≥ 10% difference of nominal voltage sustained for ≥ 15 continuous minutes.

d. Complete loss of off-site power (LOOP) to a nuclear generating station per the Nuclear Plant Interface Requirement

e. System separation contrary to design, that results in an island of 1,000 MW to 4,999 MW

~~e. Unintended system separation that results in an island of 1,000 MW to 4,999 MW~~

f. Simultaneous loss of 300 MW or more of firm load due to a BES event, contrary to design,~~, for~~ for more than 15 minutes~~, not related to an extreme weather event~~

~~f. Unintended loss of 300 MW or more of firm load for more than 15 minutes~~

g. Interconnection Reliability Operating Limit (IROL) ~~violation~~ exceedance for ~~time~~ greater than ~~T_v~~ 30 minutes

Category 3: An Event That Results in One or More of the Following:

a. Loss of firm load, contrary to design, of 2,000 MW or more.

---

[11] https://www.nerc.com/pa/rrm/ea/Pages/EA-Program.aspx

[12] Interruption of resources caused by action of control systems on the resources in response to perturbations in voltage and/or frequency on the Interconnection, not including the control actions of a RAS.

[13] In most cases, inverter-based generating resources refer to Type 3 and Type 4 wind power plants, and solar photovoltaic (PV) resources. Battery energy storage is also considered an inverter-based resource. Many transmission-connected reactive devices such as STATCOMs and SVCs are also inverter-based. Similarly, HVDC circuits also interface with the AC network though converters.

[14] Interruption of resources caused by action of control systems on the resources in response to perturbations in voltage and/or frequency on the Interconnection, not including the control actions of a RAS

~~a. Unintended loss of load, generation (including inverter type resources), or dc tie to asynchronous resources of 2,000 MW or more.~~

b. System separation contrary to design, that results in an island of 5,000 MW ~~to 10,000 MW~~or more

~~b. Unintended system separation that results in an island of 5,000 MW to 10,000 MW~~

c. System separation (without load loss) contrary to design, that islands Florida from the Eastern Interconnection

~~c. Unintended system separation (without load loss) that islands Florida from the Eastern Interconnection~~

d. Loss of 2,000 MW or more provided by DC tie(s) ~~to~~connected to asynchronous resources ~~of 2,000 MW or more~~

e. Loss of generation (including inverter-based resources) of 2,000 MW or more. This excludes RAS action that performed as designed.

~~Category 4: An Event that Results in One or More of the Following:~~

~~a. Unintended loss of load, generation (including inverter type resources) from 5,001 MW to 9,999 MW Loss of firm load from 5,000 MW to 9,999 MW~~

~~Unintended sSystem separation that results in an island of more than 10,000 MW (with the exception of Florida, as described in Category 3c)~~

~~a. Loss of generation (including inverter-based resources) between 5,000 and 9,999 MW. This excludes RAS action that is performed as designed.~~

~~Category 5: An Event that Results in One or More of the Following:~~

~~. Unintended lLoss of load of 10,000 MW or more~~

~~Unintended lLoss of generation of 10,000 MW or more~~

Event Analysis Planning Meeting/Coordination Call (Step 2)

Following an event, the RE and/or NERC will determine if a planning or coordination meeting is required between the registered entity(ies) and the applicable RE. More than one planning meeting may be conducted based on the registered entity's experience level with the EAP, the scope of the event, or the number of registered entities involved.

The planning meeting (when held) should:

1. confirm the event category;
2. determine the level of analysis;[15]
3. identify the roles for the registered entity(ies), REs, and NERC;
4. establish milestones, coordination of target dates, and determine reporting entity(ies) for completing reports, lessons learned, and other necessary analysis for events requiring detailed analysis, or the analysis itself would take longer to complete than the target dates set in the appendices. Should additional time be needed beyond the target dates to complete the analysis, this can be granted by the RE on a case-by-case basis as necessary;
5. identify the need for a data retention hold; and

---

[15] Although the category of the event provides general guidance on the level of analysis needed, these guidelines may be adjusted by the EA team, based on the overall significance of the event and the potential for valuable lessons learned.

6. identify data and information confidentiality issues.

Registered entities should capture relevant data for the event analysis. REs will formally send a Data Retention Hold[16] Notice for events in Category 3~~ or higher~~, if deemed necessary by the RE(s) or NERC.

The Appendix B: Planning Meeting Scope Template can be used as an outline in the planning meeting.

Event Analysis Process Reports (Steps 3 and 4)

Timeframes for submitting the requisite reports are found in Appendix A: Target Timeframes for Completion of Brief Reports, EARs, and Lessons Learned.

The brief report is prepared by the impacted registered entities for all qualifying events and then sent to the applicable RE for review. The RE then forwards it to NERC. A brief report includes items identified in Appendix C: Brief Report Template. The brief report template may also be used for non-qualifying events that produce useful lessons learned for the industry.

An EAR is required for ~~more significant~~Category 3 events ~~(Category 3 and above)~~ and may be requested for lower-level events. An EAR is prepared by the impacted entity, a group of impacted entities, or relevant members of an event analysis team as defined in the planning meeting. It addresses in detail the sequence of events as they happened, the identified causal factors, and the appropriate corrective actions. Appendix D: Event Analysis Report Template can be used as a guideline. Once completed, the EAR is sent to the applicable REs for review. These documents are sent to NERC upon completion.

In the brief report or EAR, registered entities are encouraged to include one-line diagrams or other diagrams and representations of the facility(ies) involved in the event.

The final EAR should address corrective actions and recommendations related to the event's causal factors and any identified lessons learned. Positive outcomes identified during an event should be documented.

If any applicable governmental authorities (AGAs) initiate a formal review process in conjunction with NERC,[17] the decision on the composition of the event analysis team, the team lead, the information needed from affected registered entities, and the required scope of the analysis will be discussed and agreed upon by the AGAs and NERC executive staff.

Lessons Learned from Events (Step 5)

Lessons learned as a result of an event analysis should be shared with the industry in accordance with timing, as referenced in Appendix A. Proposed lessons learned should be drafted by a registered entity utilizing Appendix E: Lessons Learned Template, and should be submitted to the applicable RE. The lessons learned should be detailed enough to be of value to others, but should not contain data or information that is deemed confidential. When possible, one-line diagrams or other representations should be included to enhance the information provided in the lessons learned. Vendor-specific information should not be included unless it is discussed and coordinated with the vendor. If dissemination of vendor-specific information is beneficial, it may be pursued outside the EAP.

---

[16] BPS users, owners, and operators are required, upon request, to produce any requested data pursuant to Title 18 of the Code of Federal Regulations (CFR) Part 39.

[17] As specified in the ERO ROP, Section 807.f, the NERC president and chief executive officer ~~has~~ ~~have~~ has the authority to determine whether any event warrants analysis at the NERC level. A Regional Entity may request that NERC elevate an analysis of a major event to the NERC level.

Lessons learned will be reviewed by selected technical groups and NERC staff for completeness and appropriateness prior to posting.

~~Lessons Learned from Other Occurrences~~

~~Any occurrence on the BES may yield lessons of value to the industry. Lessons learned can include the adoption of unique operating procedures, the identification of generic equipment problems, or the need for enhanced personnel training. In such cases, an event analysis would not be required, but the ERO EAP encourages registered entities to share with their RE any potential lessons learned that could be useful to others in the industry.~~

Event Closure (Step 6)

Following the receipt of final reports, NERC and the RE will evaluate and close the event upon review and analysis of brief reports, EARs, and lessons learned. The RE will notify the registered entity(ies) involved that an event has been closed upon notification from NERC.

Lessons Learned from Other Occurrences

Any occurrence on the BES may yield lessons of value to the industry. Lessons learned can include the adoption of unique operating procedures, the identification of generic equipment problems, or the need for enhanced personnel training. In such cases, an event analysis would not be required, but the ERO EAP encourages registered entities to share with their RE any potential lessons learned that could be useful to others in the industry.

Confidentiality Considerations

Information and data designated as confidential by the entity supplying the data/information in the course of an event analysis shall be treated as confidential. In addition, all Critical Energy Infrastructure Information (CEII) shall be treated ~~accordingly, and~~accordingly and may be designated as CEII by the entity supplying the information or by NERC or its REs. By participating in the EAP, a United States entity acknowledges that any of its brief reports, EARs, or both may be disseminated to an AGA, upon request, in accordance with Section 1500 of the Rules of Procedure.

Appendices and Other Suggested References

Appendix A: Target Time Frames for Completion of Brief Reports, EARs, and Lessons Learned

Appendix B: Planning Meeting Scope Template

Appendix C: Brief Report Template

Appendix D: Event Analysis Report Template

Appendix E: Lessons Learned Template

Other References:

- Attributes of a Quality Event Analysis Report
- Attributes of a Quality Lessons Learned
- NERC Blackout and Disturbance Analysis Objectives, Analysis Approach, Schedule, and Status – Attachment D from Appendix 8 of NERC Rules of Procedure
- Cause Analysis Methods for NERC, Regional Entities and Registered Entities

For additional data submission information regarding particular event categories ~~See~~ see the ~~Addendums~~ supporting documents below on the EA Program page under reference materials~~for further data submission regarding particular events~~.

- ~~Addendum for Category 1h Events~~Addendum for Category 1h Events
- ~~Addendum for Category 1a Events~~Addendum for Category 1a Events
- ~~Addendum for Events with Failed Station Equipment~~Addendum for Events with Failed Station Equipment
- ~~NEI-NERC White Paper: Nuclear Power Plant Loss of Offsite Power Events - NERC Reporting Guidelines~~NEI-NERC White Paper: Nuclear Power Plant Loss of Offsite Power Events - NERC Reporting Guidelines
- ~~Addendum for Determining Event Category~~Addendum for Determining Event Category~~ (under development~~)

The EAP, appendices, and reference documents are posted on the EA Program page on the NERC website. To access the EA Program page on the NERC website, click on the Program Areas & Departments tab at the top of the NERC home page, then ~~Reliability Risk Management~~Event Analysis, Reliability Assessment, and Performance Analysis on the left side of the page, then EA Program under Event Analysis. The latest versions of the appendices are posted under the Current Event Analysis Process Documents tab.

Revision History

Rev.	Date	Reviewers	Revision Description
1	December 2011	Event Analysis Working Group (EAWG), NERC Management, Operating and Planning Committees.	Document endorsed by Operating and Planning Committees January 2012. Document endorsed by NERC Board of Trustees February 2012.
2	July 2013	Event Analysis Subcommittee (EAS), NERC Management, NERC Operating Committee.	Document endorsed by Operating Committees June 18, 2013.
3	September 2015	Event Analysis Subcommittee (EAS), NERC Management, NERC Operating Committee.	Document endorsed by Operating Committees September 16, 2015.
3.1	December 2016	Event Analysis Subcommittee (EAS), NERC Management, NERC Operating Committee.	Document endorsed by Operating Committees December 13, 2016.
4	December 2019	Event Analysis Subcommittee (EAS), NERC Management, NERC Operating Committee.	Document endorsed by Operating Committees December 10, 2019
5	September 2023	Event Analysis Subcommittee (EAS), Reliability & Security Technical Committee (RSTC)	

White Paper: Grid Forming Functional Specifications for BPS-Connected Battery Energy Storage Systems

Action

Approve

Background

The Inverter-Based Resource Performance Subcommittee (IRPS) has developed the White Paper: Grid Forming Functional Specifications for BPS-Connected Battery Energy Storage Systems. This white paper is intended to provide functional specifications to be used by Transmission Planners and Planning Coordinators to determine whether or not interconnecting battery energy storage systems can be considered a Grid Forming (GFM) resource based on its performance. This white paper also provides significant information regarding the implementation of GFM resources internationally and the benefits of GFM resources for BPS reliability. Additionally, a number of recommendations are made to industry regarding best practices for the implementation and study of GFM resources.

Summary

This guideline has been posted for comment from IRPS members and numerous technical revisions were made in response to the comments received during this comment period. IRPS is seeking RSTC approval for this white paper.

White Paper	Grid Forming Functional Specifications for BPS-Connected Battery Energy Storage Systems
Instructions	**Please use this form to submit comments on the draft White Paper. Comments must be submitted within the review period below to (Alex.Shattuck@nerc.net) with the words "Grid Forming Functional Specifications for BPS-Connected Battery Energy Storage Systems White Paper Comments" in the subject line. Only comments submitted in this Microsoft Excel format will be accepted. Both general and specific comments should be provided within this form. Red-line document changes, PDF versions of this document, or email comments will NOT be accepted.** Comments may be submitted by individuals or organizations. Please provide the requested information in Row 6. If comments are submitted on behalf of multiple organizations, list all organizations in Row 6. Please provide the Industry Segment and Region (if applicable) in Rows 7 and 8 and provide the requested contact information in Rows 9 and 10. If you have any questions regarding this process, please contact Levetra Pitts (Levetra.Pitts@nerc.net)
Review Period	June 21, 2023 – July 21, 2023

Name of Individual or Organization(s) (list multiple if submitted by a group):	
Industry Segment (if applicable)	
Region (if applicable)	
Contact Telephone	
Contact Email	

Organization(s)	Line / Paragraph	Comment	Proposed Change	NERC Response
PGSTech	844	The white paper should be vendor neutral	Replace PSCAD model by an offline EMT model	NERC Agrees. Software specific lanugage has been replaced with general EMT language
PGSTech	846	The white paper should be vendor neutral	Replace PSCAD model by the offline EMT model	NERC Agrees. Software specific lanugage has been replaced with general EMT language
PGSTech	in the legend	The white paper should be vendor neutral	Replace PSCAd by Offline EMT	NERC Agrees. Software specific lanugage has been replaced with general EMT language
PGSTech	849	The white paper should be vendor neutral	Replace PSCAd by Offline EMT	NERC Agrees. Software specific lanugage has been replaced with general EMT language
PGSTech	870	The white paper should be vendor neutral	Replace PSCAD model by the offline EMT model	NERC Agrees. Software specific lanugage has been replaced with general EMT language
Natural Resources Canada	85	Could be more specific in noting that the underlying issue is the absence of the services/characteristics typically provided by synchronous machine-based solutions, hence the need for GFM to provide certain characteristics rather than replicating synchronous machines in general.	"in the absence of grid stabilizing characteristics provided by supplemental synchronous machine-based solutions..."	Change made in document.
Natural Resources Canada	211	"relatively low incremental cost", are there any references putting a number on this, or is it based on discussions with OEMS? Even a range of x-y% could be useful if possible to substantiate the incremental cost more concretely.	If possible/available, include reference on incremental cost of GFM, useful for policymakers.	Multiple BESS manufacturers were involved in the drafting process and provided information on the general cost to enable GFM capabilities but no specific ranges were given. No change made.
Natural Resources Canada	270-275	Some TPs/PCs may see a potential risk that the general testing definition may not fully meet future quantitative response metrics or frequency domain characterizations, and therefore will just wait for one of those specifications prior to requiring GFM for new BESS. Can this be addresssed in general to further support the value of adopting these general testing definitions in the meantime?	Include sentence mentioning how this initial approach is in line with/compatible with future detailed specifications for GFM to mitigate risk aversion to adoption.	Change made in document.
Natural Resources Canada	278	Could be more explicit in relating increasing IBRs to decreasing stability characteristics provided by synchronous machines	"It is well understood that as the penetration of IBRs continues to rise and therefore the abundance of stabilizing characteristics provided by synchronous-machines falls, …"	Change made in document.
Natural Resources Canada	468-469	Assuming the comment on additional qualitative/quantitative criteria is in reference to some criteria which may require further detail e.g., should not osciillate excessively, any significant amount of time, etc. If possible, it could be valuable to include an example of fully flushed out criteria with additional generic qualitiative or quantitative criteria as a starting point for easier use by policymakers, but where TPs/PCs can still adjust based on their own systems.	Include a set of example test criteria with full baseline qualitative/quantitative details for an easier adoption starting point.	Thank you for your comment. The success criteria in this white paper are designed not to be overly prescriptive. Providing specific quantitative criteria is out of scope for this white paper.
Manitoba Hydro	108	editorial error in Footnote-3 "New interconnection studies is recommended ....".	"New interconnection studies are recommended ....".	Change made in document.

Manitoba Hydro	119	Spell out the full term whenever it is first mentioned (OEMs, GOPs)		Change made in document.
Manitoba Hydro	207	Do we always required to perform "large EMT studies" when integrating GFM technologies?!	we belive it is suficient to say "EMT studies…". TPs/PCs can determine the depth of the EMT studies and required study models	Change made in document.
Manitoba Hydro	546	Footnote 48 is missing		Change made in document.
Evergy		Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI).		Responses made to EEI comments.
Arizona Public Service Company		AZPS supports the following gneral comment that was submitted by EEI on behalf of its members: EEI appreciates the good work done in development of this white paper and supports NERC efforts to address performance issues related to the changing resource mix, however, many of the statements and recommendations contained in this white paper do not appear to be supported by work conducted within the North American BPS (BPS). We are also concerned by both the recommendations and GFM specifications contained in this white paper, which are portrayed as fully vetted for use on the BPS, while no support for either has been shown. We further note that this document reads more like a Reliability Guideline than a white paper, however, given the current state of testing and validation of this technology on the BPS, transforming this document into a Reliability Guideline at this time would be premature. While we understand the perceived urgency of resolving issues related to the changing resource mix, presumptuously pushing unproven technology onto the grid before it has been adequately tested within the environment it will be installed and without any known industry standards (e.g., IEEE, ANSI, etc.) that manufacturers can build to could create reliability issues. While we agree that the promise of GFM inverters is well worth the time and effort to pursue, such a pursuit needs to be done in a thoughtful manner employing good engineering processes, which has always been the hallmark of the North American grid since its inception. In this vein, NERC should partner with the UNIFI Consortium, EPRI and others. EEI additionally supports efforts to study and understand the impacts of GFM on the North American energy grid, and this white paper should be revised to focus on a call to action for industry engagement to study and understand the technology. The industry recognizes technology such as GFM is needed and represents the future, but good engineering practices employing testing, verifying, standardizing, while holding safety and the impacts on reliability and the general public paramount		See responses made to the EEI comments.

Arizona Public Service Company	Line 85 - 86	While EEI agrees that “grids dominated by IBRs, in the absence of supplemental synchronous machine-based solutions,” need supplemental support to maintain stable operation. Recommending such a broad reaching change without necessary pilots could negatively impact reliability noting the white paper provides no references to examples where this technology has been validated within the BPS.	Add references to tests validating the performance of the GFM on the BPS or add a disclaimer that the technology has not yet been validated on the BPS in any meaningful way.	See responses made to the EEI comments.
Arizona Public Service Company	Line 101 - 103	The paper suggests that “upwards of 30%” of IBRs will need to be deployed with GFM functionality enabled. This is apparently based on simulation testing conducted on a system planned for the Maui power system. While we support this work, such assumptions should not be made that this will be the case everywhere. Similar testing needs to be conducted throughout the BPS to validate that such assumptions can be transferred elsewhere.	Restate within the paper that tests conducted on the Maui power system indicate that upwards of 30% of the IBRs installed on that system will likely require GFM functionality enabled. Similar testing will be necessary throughout the BPS to assess the transferability of such findings.	See responses made to the EEI comments.
Arizona Public Service Company	Line 105 - 106	The paper states that “GFM technology is commercially available and can help improve stability and reliability in areas with high IBR penetration.” While this looks to be very promising technology and we agree that the technology is now commercially available, the performance still needs to be validated on the BPS before wide scale deployment, to do otherwise could significantly risk BPS reliability in unforeseen ways.	Restate as follows (proposed changes in boldface): GFM technology is commercially available but has not yet been standardized. While this technology looks very promising in its potential ability to help improve stability and reliability in areas with high IBR penetration, responsible entities should validate its performance on their system before widespread adoption.	See responses made to the EEI comments.
Arizona Public Service Company	Line 107 - 108	The paper states “BESS can potentially be retrofitted with GFM technology and new BESS can be equipped with GFM technology at a relatively low incremental project cost.	Add an addendum to explain anticipated costs for the owners of in-service IBRs. Also, if there is an expectation that existing BESS IBR owners will install GFM technology within their systems, there will need to be a recovery method for their costs. Otherwise, there will be no incentive for those entities to make this change. Additionally, such changes should not be made without the review and approval of the responsible Planning Coordinator, per FAC-001 & FAC-002. Such a change would be considered a “qualified change” that would require study prior to allowing the IBR controls change. While such studies will be needed, EEI questions whether responsible PCs have sufficient training and tools to assess the impacts of such a change at this time. This should be made clear in the white paper.	See responses made to the EEI comments.
Arizona Public Service Company	Line 116 - 120	EEI does not support this Key Takeaway – “GFM technology is commercially available and field-proven for BPS-connected applications, particularly for ESS (including standalone BESS4 in ac-coupled hybrid plants) as well as dc-coupled solar photovoltaic (PV)+BESS5 applications.” This broad endorsement appears to be based solely on a decision by a utility in Australia to build a large GFM battery system supporting their grid. While EEI supports such global efforts, decisions made supporting technology in Australia for their grid does not validate the use of this technology on the BPS. While EEI does not have direct knowledge of entity testing of this technology, we would support and welcome additions to this report that shared information on any current GFM pilots installed on either the BPS or even on distribution systems.	Add supporting references to installations done in support of the BPS should be added or the statement should be removed.	See responses made to the EEI comments.

Arizona Public Service Company	Lines 121-123	EEI does not support this Recommendation – "All newly interconnecting BPS-connected BESS should be designed, planned, and commissioned with GFM controls enabled to improve overall system stability across the BPS, particularly with increasing levels of IBRs." The wide scale deployment of new technology that is not yet standardized or fully tested on the BPS represents a substantial risk to grid reliability.	While it is clear there have been many successful tests and installations of GFM controls outside of the BPS, understanding and validating installations within the BPS is necessary and the recommendation should be removed. In its place, we recommend the following Recommendation: Owners and developers should begin assessing, testing and piloting GFM controls on BESS installations. Where possible, owners and developers should consider specifying IBR controls that have the capability of allowing IBRs to be controlled through both grid following controls and grid forming controls. This will allow the controlled testing of the technology under both owner and responsible utility oversight. This will also minimize and impacts that unforeseen control issues that could be uncovered have minimal impact on BPS reliability. It would also provide the industry with time to become better trained on this technology and resolve issues before they are widespread.	See responses made to the EEI comments.
Arizona Public Service Company	Lines 126 - 128	EEI does not support this Recommendation as currently written: "TOs in consultation with their TPs and PCs, should establish clear GFM functional specifications for BESS in their interconnection requirements (or provisions in power purchase agreements) using the materials contained in this guideline." EEI does not agree that TPs and PCs are sufficiently trained and prepared to guide TOs in the development of GFM functional specifications. This technology is in the very early stages of development and placing such a burden on TPs, PCs and TOs is inappropriate at this time.	TOs in consultation with their TPs and PCs, should begin the process of establishing clear GFM functional specifications for BESS within their interconnection requirements (or provisions in power purchase agreements) in anticipation of future BESS GFM IBR installations using considering the use of the materials contained in this guideline. However, approval to install a GFM BESS should be carefully studied and approved by the PC and monitored by the TO after installation to ensure correct performance. Additionally, before installing a GFM IBR TOs should require IBR owners install adequate fault recording and sequence of event recording equipment to ensure adequate assessment of the performance of the GFM controls during BPS disturbances.	See responses made to the EEI comments.
Arizona Public Service Company	Lines 129 - 130	EEI does not support this recommendation as written: "TPs and PCs should integrate GFM functional testing requirements in their interconnection study processes that ensure newly connecting GFM is able to meet the performance requirements for GFM." EEI does not agree that TPs and PCs are broadly prepared to develop GFM testing requirements at this time.	TPs and PCs should begin training their staff in conducting studies to assess the functional differences in GFM controls so that they can be properly prepared for the future integration of GFM IBRs and become fully competent to develop functional testing requirements in for their interconnection study processes that will be required to that ensure newly connecting GFM is are able to meet the performance requirements for GFM of their service areas.	See responses made to the EEI comments.
Arizona Public Service Company	Lines 131 - 134	EEI does not support this recommendation as written: "GFM technology can operate reliably and provide stabilizing characteristics in areas of high IBR penetrations and areas of low system strength. GFM BESS presents a unique opportunity to support system stability (e.g., transient, oscillatory, voltage) with a relatively low incremental cost to all resources and end-use consumers." There was not data contained in this white paper that validated that GFM controls on BESS can be operated reliably because there is no evidence contained in this white paper that the technology has been thoroughly tested on the BPS.	GFM technology can has been shown to operate reliably and provide stabilizing characteristics in areas of high IBR penetrations and areas of low system strength in other countries and outside of the North American BPS (BPS). Given these impressive demonstrations of GFM BESS performance on other grids, it is now time to consider limited and controlled testing and validation of these systems on the BPS. While we are encouraged by the results seen by others outside of the BPS, careful testing and validation of GFM performance is still needed before broad deployment of this technology. presents a To address the unique opportunities of GFM controls on BESS through their ability to support system stability (e.g., transient, oscillatory, voltage) with a relatively low incremental cost to all resources and end-use consumers IBR owners and Developers should be encouraged to procure BESS systems with dual control capability (Grid Following and Grid Forming Controls) to enable broader validation of its performance on the BPS.	See responses made to the EEI comments.

Arizona Public Service Company	Line 325 - 327	EEI does not support the following as currently written “This chapter defines the recommended functional specifications for GFM BESS. For effective and efficient adoption of GFM technology, TOs will need to establish functional specifications that define GFM functionality and. The GFM specification can then be provided to OEMs by developers and GOs to ensure procurement of GFM resources.”	This chapter defines the recommended provides a template for entities in their development of functional specifications for GFM BESS. While this template should be considered just a guide, , For effective and efficient adoption of GFM technology, TOs will need to establish the information provided should provide a useful guide in the development of a functional specifications that defines GFM functionality. The Additionally, once a TO decides to allow the installation of a GFM enabled IBR within their service area they are encouraged to work specification can then be provided to OEMs by with their perspective developers and GOs to ensure procurement of GFM resources align to the TO’s desired specifications. Moreover, considerable caution should be exercised in preparation for the deployment of this equipment through the installation of owner installed digital fault recording and sequence of event equipment in order to monitor and assess the performance of the GFM controls. For this reason, it is suggested that limited deployments be allowed until proper performance of the GFM controls can be validated. NOTE: The following specification should only be considered as a guide for those TOs looking to test and validate GFM performance within their service area.	See responses made to the EEI comments.
Arizona Public Service Company	Lines 348 - 361 and 388 - 391	EEI does not support language used in the section titled “Functional Specifications Defining Grid Forming BESS” because white papers are not intended to provide enforceable requirements. The use of “shall” throughout this section implies that entities are required to adopt the recommendations as written and contained in those sections where shall is used.	Remove shall and replace it with “should consider,” since this is a white paper and not a Reliability Guideline.	See responses made to the EEI comments.
Patrick Hart (Trina Energy Storage)	255-268	Options 2 and 4 seem like the same, whith slight variations, I would propose combining these. Also option 3 is very difficult to evaluate in a real world setting. While models can be stimulated to provide a valid result, demonstrating compliance with real hardware will be difficult and likely beyond the capability of most in the industry.	Combine Options 2 and 4. Remove Option 3.	The paper simply presents available options to specify GFM. No change made in document.
Patrick Hart (Trina Energy Storage)	Line 336-339	GFM BESS should not be expected to superimpose the GFM response with an additional Dynamic Reactive Power Support or Active Power Frequency Control service. I expect that this is inteded primarily for GFL equipment.	Specify that GFM assets are excluded from Dynamic Reactive Power Support or Active Power Frequency Control services when they are providing GFM Specific Voltage and Frequency Support.	Dynamic reactive power support and active power frequency controls ervices are longer timescale behaviors that take place after the subtransient to transient GFM response requirements. GFM are not excluded from providing ERS. No change made in document.
Patrick Hart (Trina Energy Storage)	388-391	GFM BESS cannot discharge further when the state of charge is at 0%, or charge further when the state of charge is at 100%. The phharagraph seems to ignore these conditions. There are also power limitations that may be imposed during periods of derating (due to heavy use, or near maximum or minimum state of charge)	Add language to allow exceptions to GFM behavior when there are physical limits to the design. Perhaps change to a form of: "shall not artificially limit the GFM operation unless continued operation would damage the equipment"	No change made in document. GFM is expected to perform within its energy and equipment capability limits.

Patrick Hart (Trina Energy Storage)	392-397	Blanket application of prior grid requirements will cause a lot of conflicting requirements. IEEE 2800 for example includes a lot of performance requirements that are not applicable for GFM technology. Exceptions being specified by the TO will immediately introduce variations of requirements across the regions, exactly what IEEE 2800 was designed to avoid.	Instead of using IEEE 2800 (or any other GFL standard) for compliance, a gap analysis should be peformed and an update to IEEE 2800 or an introduction of a new standard should be fast tracked	Thanks for your comment. This is out of scope of this white paper.
Patrick Hart (Trina Energy Storage)	463-464, 493-494	Comment is in reference to Test 3: BESS GFM Performance at Maximum Active Power. The test is performed with the Project BESS at a 0MW dispatch. The title of the test would seem to indicate that it should be at maximum active power. The test procedure as is currently written seems to make sense, but the title is confusing.	Rename the title of Test 3. If intending to test the Project BESS at maximum discharge, then I recommend removing the test, as the model wont match the behavior of real hardware when operating at a phsyical constraint.	In this test, the duplicate BESS was dispatched at its maximum active power. No change made.
ITC Holdings		General Comment: ITC supports EEI's comments.The white paper on this topic should be revised to focus on a call to action for industry engagement to study and understand the technology. Additionally, the call to action should also include encouraging developers and TOs to include GFM capability in interconnection agreements in the interim so that once these studies are completed and parameters determined, they can be readily implemented to existing facilities with these capabilities with minimal cost impact.		Please see NERC response to EEI comments.
American Transmission Co	All	This document provides necessary clarity on a significant emerging reliability challenge. The recommendation is supported, the proposed tests are feasible, and the solution proposed represents the likely most economical, feasible, and timely action to forestall significant grid upsets.	None	Thank you for your comment.
American Transmission Co	88-89	"proactively plan to ensure sufficient GFM IBRs are installed"	None - this language correctly sets the tone regarding the problem as well as the most beneficial and economic solution (i.e. the paper's recommendation)	Thank you for your comment.
American Transmission Co	89-91	"One of the most significant obstacles … is establishing clear interconnection requirements"	None - the paper correctly identifies that the lack of industry standards (i.e. not regulatory standards) for GFM design is hampering both deployment and requiring deployment of GFM IBR	Thank you for your comment.
American Transmission Co	104-105	"it is recommended to start requiring and enabling GFM in all future … BESS"	None - this recommendation is based on sound reasoning, as described in the document. Technical studies demonstrate the need and the benefit of GFM, and the timing is appropriate before significant amounts of BESS are installed. If anything, this recommendation may be too weak since many generator interconnection processes lock in projects at the then current interconnection requirements and planning criteria. As such, this recommendation may not be able to be applied to BESS requests already in the generation queues without further requirements from NERC or FERC.	Thank you for your comment.

American Transmission Co	105-106	"in areas with high IBR penetration"	This statement is accurate and does not need to change. However, it is important to note that GFM is also beneficial in areas that many would consider to be "low penetration" of IBRs. For example, there are areas of the existing system where only a single IBR plant is interconnected yet the system strength is substantially weakened by a single prior outage, resulting in IBR instability for the next contingency. GFM is useful in these "low penetration" scenarios as well and may be the most cost-effective, easily-achieved, lowest-societal impact solution.	Change made in document.
American Transmission Co	108	Insert new sentence or phrase following "low incremental project cost."	This correctly highlights the important role future BESS installations can have on stabilizing the electrical grid. There are also other technologies being deployed under various monikers, such as E-STATCOM, Ultra Caps, Super Caps, etc. It would be helpful to note that this technology is still developing and may also benefit from, or already be envisioned to use, GFM technology. This would draw the attention of the industry to other assets that can also play a role in stabilizing the grid. Here is a proposed sentence: "Though the focus in this paper is on near term BESS applications, GFM technology may need to be considered when developing new IBR transmission applications, such as E-STATCOM, Ultracapacitors, and Supercapacitors."	Change made in document.
American Transmission Co	108-109	"due to study limitations"	None - Still, it is important to note that this phrase understates the problem we are facing as an industry. We do not currently have a sufficient number of adequately trained engineers to run EMT analysis, the EMT models we receive contain inaccuracies (at times), EMT models do not always incorporate all the controls needed to predict performance, and there is both not enough time to run all the scenarios that might be needed (especially if the size of the model must be increased to capture more interactions) and there is an inability to run real-time EMT analysis in support of operations.	Thank you for your comment.
Amro Quedan	180	I suggest to define how GFM can provide this stability characteristics.	add a text stating that " the GFM can provide stabiltiy charactaristics based on it's active and reactive power responses after a disturbance, which different than the GFL responses"	The white paper describes how stability requirements are provided by GFM. No change made in document.
Amro Quedan	415	I suggest to define the model's domain	I suggest to define the model's domain, is it phasor, EMT,or both . Also, in case both models are provided a match between the two models' results should be provided.	The white paper focuses specifically on EMT models. No change made in document.

Amro Quedan	437	I suggest to define system strength (SCR, SCMVA) at the main bus or the GFM BESS terminal as a reference.		The test system is described in the following section. No change made in document.
Amro Quedan	438	I suggest to define the synchronous machine rating based on the GFM BESS rating.	Based on the current system it is three times the GFM BESS plant rating.	The test system is described in the following section. No change made in document.
Amro Quedan	440	I suggest to define the load rating based on the GFM BESS plant rating	Based on the current system it is same as the GFM BESS project rating	The test system is described in the following section. No change made in document.
Electric Reliability Council of Texas, Inc. (ERCOT)	126-128	The specifications should not be limited to TPs and PCs. This should be up at the RC/BA/TOP level to ensure that the grid forming functionality required of the BESS does not interfere with BES operations. In other words, the grid forming regulations should come from the local grid codes to ensure there are no adverse effects on the BES.	Revise lines 126-128 to indicate that the RC/BA/TOP should be included in the development of GFM functional specifications.	Change made in document.
Electric Reliability Council of Texas, Inc. (ERCOT)	129-130	Expand to TOP and BA/RC as well, since for ERCOT the ISO does its own interconnection studies, and the BESS need to comply with obligations to the RC/BA/ISO to ensure they deploy a reliable asset	Revise lines 129-130 to indicate that the RC/BA and TOP should also be involved in integrating GFM functional testing requirements in their interconnection study processes.	Change made in document.
Electric Reliability Council of Texas, Inc. (ERCOT)	373-381	BESS should not be considered eligible to provide blackstart services given its duration-limited capability. As such, any discussion about blackstart should be removed from the document. The concerns here are similar to concerns that have been expressed in relation to EOP-005. If the system takes longer to restore than planned, or if an island trips, the BESS is only available for a certain amount of restarts and then the battery power is exhausted. If that BESS is expected to be the blackstart resource for the island, there is no way for the island to start up again.	Remove the discussion of BESS as a blackstart resource from the document.	BESS with GFM capability can be part of blackstart system restoration plans provided that the limitations of BESS and GFM technology are considered. No change made in document.
Electric Reliability Council of Texas, Inc. (ERCOT)	402-405	The TOP or RC/BA should also be involved in the interconnection study process, as noted in the comments above. While the Resource Integration process may implicate the TP function, the TOP or RC/BA are also implicated and should be included as well.	Revise lines 402-405 to indicate that the TOP and RC/BA should be involved in the process of integrating functional performance verification tests into the interconnection study process.	Change made in document.

Electric Reliability Council of Texas, Inc. (ERCOT)	412-414	Similar to other comments, the TOP or RC/BA should also be included in setting model quality requirements and checks, or this should be done at the region level with grid code changes, rather than through a NERC Standard.	Revise lines 412-414 to indicate that the TOP and RC/BA should also be included in establishing model quality requirements and checks.	Change made in document.
AES Clean Energy	108	The project cost to implement GFM can vary significantly based on the functionality required and must be stated as such. For example, GFM used only while grid-connected has a lower cost than GFM used for utility blackstart purposes.	Change made in document.	Change made in document.
AES Clean Energy	113	As acknowledged in the Grid Forming Technology BPS Reliability White PAper published December 2021, there is a lack of a standard library model representing GFM, for which many TPs and PCs require for their studies. Consider mentioning this in the modeling section of this paper.	This paper specifically focuses on model based testing with EMT models to verify GFM functionality only, exploratory planning studies are out of scope for this document. No change made in document.	This paper specifically focuses on model based testing with EMT models to verify GFM functionality only, exploratory planning studies are out of scope for this document. No change made in document.
AES Clean Energy	159 - 160	Commercially available GFL inverters can pursue frequency and voltage regulation in the sub-transient timescale now. The language should reflect as such.	GFL cannot regulate sufficiently in the sub-transient timescale. No change made in document.	GFL cannot regulate sufficiently in the sub-transient timescale. No change made in document.
AES Clean Energy	173 - 176	There is a case to be made that GFL inverters responding with frequency and voltage regulation services in the sub-transient timescale can help with overall system stability as well (eg: Decreasing grid ROCOF and regulating frequency nadir).	GFL cannot regulate sufficiently in the sub-transient timescale. No change made in document.	GFL cannot regulate sufficiently in the sub-transient timescale. No change made in document.

AES Clean Energy	199 - 201	There are also systems capable of a hybrid GFL - GFM control, where a hot switch may be applied to change from GFL to GFM, and performed a planned islanding event. Additionally, a GFM only system interconnected to the BPS is capable of performing both planned and unplanned islanding events in the event of an upcoming (planned) grid outage, or an unplanned protection fault/grid outage.		Thank you for your comment.
AES Clean Energy	206 - 208	Detailed studies are also challenged by the fact that inverter manufacturers provide black box power simulation models (PSSE/PSCAD) that may not be tuned easily by the user.	Models should not be tuned without OEM support and verification. No change made in document.	Models should not be tuned without OEM support and verification. No change made in document.
AES Clean Energy	211 - 214	Similar to the first comment on this page: The project cost to implement GFM can vary significantly based on the functionality required and must be stated as such. For example, GFM used only while grid-connected has a lower cost than GFM used for utility blackstart purposes.	Change made in document.	Change made in document.
AES Clean Energy	255 - 258	How is this point relevant to specifying GFM? Frequency domain analysis (small signal stability) is a characterization/test of the functionalities of the GFM inverter's capabilities.	No change made in document.	No change made in document.
AES Clean Energy	342	What amount of negative sequence fault current contribution is expected from GFM IBR plants? Can this be clarified further?	The intent of the white paper is to describe criteria qualitatively to avoid being overly prescriptive. No change made in document.	The intent of the white paper is to describe criteria qualitatively to avoid being overly prescriptive. No change made in document.

AES Clean Energy	360 - 361	This is assuming that there are still synchronous machines present on the wider grid network, correct? Otherwise, this would mean an unplanned islanding event, where the nature and success of the transition of the GFM converter from a grid-connected to an islanded mode will depend on the type of fault leading to the event.	This is a hypothetical scenario which is later used as a basis for the testing procedures. No change made.	This is a hypothetical scenario which is later used as a basis for the testing procedures. No change made.
AES Clean Energy	375 - 378	How does the additional requirements for blackstart capability necessitate more stringent ride-through capability? A blackstart would only be initiated once the plant is in a shutdown state, and ride-through is irrelevant here.	During blackstart conditions, frequency and voltage conditions may be more extreme than normal operations and thus BESS may be required to remain online under severe conditions. No change made in document	During blackstart conditions, frequency and voltage conditions may be more extreme than normal operations and thus BESS may be required to remain online under severe conditions. No change made in document
AES Clean Energy	383	There are no considerations given to planned and unplanned islanding events that can be provided by GFM IBRs. Planned islanding can be performed by GFM IBRs during an upcoming planned grid outage. Unplanned islanding can be performed by GFM IBRs, where frequency and voltage regulation is provided (in addition to dispatch) prior to protection opening isolating sections of the grid; The GFM IBR maintains power to the connected loads in circuit.	Thanks for your comment. This is out of scope of this white paper. No change made in document.	Thanks for your comment. This is out of scope of this white paper. No change made in document.
AES Clean Energy	390 - 391	One of the challenges with GFM control is limiting over-current (due to the nature of voltage control). Some inverter manufacturers use techniques to switch between GFM to GFL during high SOC% conditions to help control the current and prevent the converter from tripping offline. Not sure if industry is at a place yet to consider absolutely no state of charge conditions where the BESS needs to operate in GFL mode.	Thank you for the comment. No change made in document.	Thank you for the comment. No change made in document.
AES Clean Energy	482	The tests described to verify GFM performance specifically tests the ability of the GFM plant to perform an unplanned seamless islanding (no interruption in power to the loads connected in circuit). In reality, the transition from a grid connected mode to an islanded mode of operation may depend on the type of fault leading to protection opening, system frequency, system voltage, and dispatch setpoint (distributed among online PCSs) at the time of protection opening.	The tests are specifically designed to verify the functional characteristics of GFM using minimum tests, not to recreate specific real-world scenarios. No change made in document.	The tests are specifically designed to verify the functional characteristics of GFM using minimum tests, not to recreate specific real-world scenarios. No change made in document.

AES Clean Energy	488	Similar to above comment	The tests are specifically designed to verify the functional characteristics of GFM using minimum tests, not to recreate specific real-world scenarios. No change made in document.	The tests are specifically designed to verify the functional characteristics of GFM using minimum tests, not to recreate specific real-world scenarios. No change made in document.
AES Clean Energy	601	What is forming the voltage of the island, after the synchronous generator is tripped offline if the two plants in the model are running in GFL?	The plants are opetating in voltage control mode. No change made in document.	The plants are opetating in voltage control mode. No change made in document.
AES Clean Energy	215	This section covers the cost of inaction well, but it is important to note the hurdles to action: Modeling studies that are not allowed without standard library models and the need to study GFM through the IC process, for which many projects could lose their queue position under current practices.		Thank you for your comment. No change made.
Beacon Power	519	After the synch gen trips, the load recovers quickly, but the frequency drops below and settles at 59.4 hz for the 20 second duration. With droop response, the load and frequency don't recover until tertiary response. The simulated load response is very (too) quick and frequency should also recover. These simulations are fatally flawed or a bad EMT model.	Simulation should be done correctly with realistic field verified EMT model. The analysis of the capabilities of the GFM should be redone to reflect the results of the simulations.	The example tests were conducted with field-tested, OEM-provided EMT models of their GFM BESS. The tests are specifically designed to verify GFM characteristics. They are not meant to replicate actual grid. When grid forming BESS are the only generation, their frequency and voltage droop settings determine the final steady state frequency and voltage. No change made.
Beacon Power	550	After the synch gen trips, the load recovers quickly, but the frequency drops below and then settles at 58.4 hz for the 20 second duration. This is a greater drop than the droop spec of 2%. With droop response, the load and frequency don't recover until tertiary response. The simulated load response is very (too) quick and frequency should also recover. These simulations are fatally flawed or a bad EMT model.	Simulation should be done correctly with realistic field verified EMT model. The analysis of the capabilities of the GFM should be redone to reflect the results of the simulations.	The example tests were conducted with field-tested, OEM-provided EMT models of their GFM BESS. The tests are specifically designed to verify GFM characteristics. They are not meant to replicate actual grid. When grid forming BESS are the only generation, their frequency and voltage droop settings determine the final steady state frequency and voltage. No change made.
Beacon Power	577	After the synch gen trips, the load recovers quickly, but the frequency drops below and then settles at 59.3 hz for the 20 second duration. On the grid, with droop response, the load and frequency don't recover until tertiary response minutes later. The simulated load response is very (too) quick and frequency should also recover. These simulations are fatally flawed or a bad EMT model.	Simulation should be done correctly with realistic field verified EMT model. The analysis of the capabilities of the GFM should be redone to reflect the results of the simulations. Field testing, perhaps at NREL, could verify or elucidate grid and GFM BESS performance.	The example tests were conducted with field-tested, OEM-provided EMT models of their GFM BESS. The tests are specifically designed to verify GFM characteristics. They are not meant to replicate actual grid. When grid forming BESS are the only generation, their frequency and voltage droop settings determine the final steady state frequency and voltage. No change made.

Beacon Power	552	The simulation shows the current from both GFM BESS's increased within a quarter-cycle. Battery response is generally reported at 40-100 milliseconds (2.5-6.3 cycles). The inverter can respond more quickly, but the energy comes from the battery.	Simulation should be done correctly with realistic field verified EMT model. The battery reponse should reflect actual performance, not only of the best BESS in new condition, but the worst or at least average performance of a range of BESS and ones of a range of ages out to 5 or more years old. The analysis of the capabilities of the GFM should be redone to reflect the results of the simulations.	The example tests were conducted with field-tested, OEM-provided EMT models of their GFM BESS. No change made.
Beacon Power	596	The GFL frequency chart makes no sense. With loss of the synch gen, the frequency would drop and the GFL BESS would follow. There's no reason that they should be able to increase the frequency above 60 hz. Another fatally flawed simulation or bad EMT model.	Simulation should be done correctly with realistic field verified EMT model. The analysis of the capabilities of the GFM should be redone to reflect the results of the simulations.	The example tests were conducted with field-tested, OEM-provided EMT models of their GFM BESS. No change made.
Beacon Power	113	With the flawed simulations, the summary that GFM can perform the specified functions for the grid are baseless. Part of the problem may be that the report is not transparent about what the simulation was based on, what GFM and with GFM models were used and the input parameters used with the models. Providing this information would allow more in-depth review and validation by users of the GFM equipment and models.	The simulations need to be redone with transparency of the simulations, models and model parameters before stating the summary of GFM capabilities on the grid. At that point the hardware should be tested in the field, perhaps at NREL where real generation could be disconnected and data collected on the resulting performance of the grid and the GFM connected BESS.	The example tests were conducted with field-tested, OEM-provided EMT models of their GFM BESS. Relevant model information and control settings such as frequency and voltage droop settings are provided so that the reader can verify against the results. No change made.
Edison Electric Institute	N/A	General Comments: EEI appreciates the good work done in development of this white paper and supports NERC efforts to address performance issues related to the changing resource mix, however, many of the statements and recommendations contained in this white paper do not appear to be supported by work conducted within the North American BPS (BPS). We note that this document reads more like a Reliability Guideline than a white paper, however, given the current state of testing and validation of this technology on the BPS, transforming this document into a Reliability Guideline at this time would be premature. While we understand the need to address issues related to the changing resource mix, installing technology onto the grid before it has been adequately tested within the environment it will be installed and without any known industry standards (e.g., IEEE, ANSI, etc.) that manufacturers can build to could create reliability issues. While we agree that the promise of GFM inverters is well worth the time and effort to pursue, such a pursuit needs to be done in a thoughtful manner employing good engineering processes, which has always been the hallmark of the North American grid since its inception. In this vein, NERC should partner with the UNIFI Consortium, EPRI and others. EEI additionally supports efforts to study and understand the impacts of GFM on the North American energy grid, and this white paper should be revised to focus on a call to action for industry engagement to study and understand the technology. The industry recognizes technology such as GFM is needed and represents the future, but good engineering practices employing testing, verifying, standardizing, while holding safety and the impacts on reliability and the general public paramount. We support efforts to find solutions to IBR performance and agree greater efforts in the pursuit of GFM controls is needed.	We ask that recommendations that are unsupported in this white paper be supported or removed. Add and cite GFM pilots conducted on the North American BPS. Develop NERC partnerships with organization working on developing standards for the North American grid such as the UNIFI Consortium, EPRI and other standards making organizations such as the IEEE. We also ask that consideration be given to removing statements that more closely align with a Reliability Guideline.	This white paper drafting teams includes SMEs from UNIFI, EPRI, and other standards organizations as well as numerous manufacturers. The recommendations in this paper are supported through numerous references throughout the document and additionally are supported by the participating SME who have extensive knowledge and experience in this field.

Edison Electric Institute	85 - 86	While EEI agrees that "grids dominated by IBRs, in the absence of supplemental synchronous machine-based solutions," need supplemental support to maintain stable operation. Recommending such a broad reaching change without necessary pilots could negatively impact reliability noting the white paper provides no references to examples where this technology has been validated within the BPS.	Add references to tests validating the performance of the GFM on the BPS or add a disclaimer that the technology has not yet been validated on the BPS in any meaningful way.	This white paper drafting teams includes SMEs from UNIFI, EPRI, and other standards organizations as well as numerous manufacturers. The recommendations in this paper are supported through numerous references throughout the document and additionally are supported by the participating SME who have extensive knowledge and experience in this field. This white paper also references numerous international studies and experiences.
Edison Electric Institute	101 - 103	The paper suggests that "upwards of 30%" of IBRs will need to be deployed with GFM functionality enabled. This is apparently based on simulation testing conducted on a system planned for the Maui power system. While we support this work, such assumptions should not be made that this will be the case everywhere. Similar testing needs to be conducted throughout the BPS to validate that such assumptions can be transferred elsewhere.	Restate within the paper that tests conducted on the Maui power system indicate that upwards of 30% of the IBRs installed on that system will likely require GFM functionality enabled. Similar testing will be necessary throughout the BPS to assess the transferability of such findings.	Change made in document.

Edison Electric Institute	105 - 106	The paper states that "GFM technology is commercially available and can help improve stability and reliability in areas with high IBR penetration." While this looks to be very promising technology and we agree that the technology is now commercially available, the performance still needs to be validated on the BPS before wide scale deployment, to do otherwise could significantly risk BPS reliability in unforeseen ways.	Restate as follows (proposed changes in boldface): GFM technology is commercially available **but has not yet been standardized. While this technology looks very promising in its potential ability to** help improve stability and reliability in areas with high IBR penetration, **responsible entities should validate its performance on their system before widespread adoption.**	Change made in document.
Edison Electric Institute	107 - 108	The paper states "BESS can potentially be retrofitted with GFM technology and new BESS can be equipped with GFM technology at a relatively low incremental project cost.	Add an addendum to explain anticipated costs for the owners of in-service IBRs. Also, if there is an expectation that existing BESS IBR owners will install GFM technology within their systems, there will need to be a recovery method for their costs. Otherwise, there will be no incentive for those entities to make this change. Additionally, such changes should not be made without the review and approval of the responsible Planning Coordinator, per FAC-001 & FAC-002. Such a change would be considered a "qualified change" that would require study prior to allowing the IBR controls change. While such studies will be needed, EEI questions whether responsible PCs have sufficient training and tools to assess the impacts of such a change at this time. This should be made clear in the white paper.	Change made in document.

Edison Electric Institute	116 - 120	EEI does not support this Key Takeaway – "GFM technology is commercially available and field-proven for BPS-connected applications, particularly for ESS (including standalone BESS4 in ac-coupled hybrid plants) as well as dc-coupled solar photovoltaic (PV)+BESS5 applications." This broad endorsement appears to be based solely on a decision by a utility in Australia to build a large GFM battery system supporting their grid. While EEI supports such global efforts, decisions made supporting technology in Australia for their grid does not validate the use of this technology on the BPS. While EEI does not have direct knowledge of entity testing of this technology, we would support and welcome additions to this report that shared information on any current GFM pilots installed on either the BPS or even on distribution systems.	Supporting references to installations done in support of the BPS should be added or consideration should be given to removing this statement until supporting evidence can be found.	Change made in document.
Edison Electric Institute	121 - 123	EEI does not support this Recommendation – "All newly interconnecting BPS-connected BESS should be designed, planned, and commissioned with GFM controls enabled to improve overall system stability across the BPS, particularly with increasing levels of IBRs." The wide scale deployment of new technology that is not yet been standardized or fully tested on the BPS represents a potential risk to grid reliability.	While it is clear there have been many successful tests and installations of GFM controls outside of the BPS, understanding and validating installations within the BPS is necessary and the recommendation should be validated through similar testing on the BPS before making this recommendation. In its place, we suggest the following Recommendation: **Owners and developers should begin assessing, testing and piloting GFM controls on BESS installations. Where possible, owners and developers should consider specifying IBR controls that have the capability of allowing IBRs to be controlled through both grid following controls and grid forming controls. This will allow the controlled testing of the technology under both owner and responsible utility oversight. This will also minimize and impacts that unforeseen control issues that could be uncovered have minimal impact on BPS reliability. It would also provide the industry with time to become better trained on this technology and resolve issues before they are widespread.**	Change made in document.

Edison Electric Institute	126 - 128	EEI does not support this Recommendation as currently written: “TOs in consultation with their TPs and PCs, should establish clear GFM functional specifications for BESS in their interconnection requirements (or provisions in power purchase agreements) using the materials contained in this guideline.” EEI does not agree that TPs and PCs are sufficiently trained and prepared to guide TOs in the development of GFM functional specifications. This technology is in the very early stages of development and placing such a burden on TPs, PCs and TOs is inappropriate at this time.	We suggest the following proposed changes (shown in boldface): TOs in consultation with their TPs and PCs, should **begin the process of** establish**ing** ~~**clear**~~ GFM functional specifications for BESS **with**in their interconnection requirements (or provisions in power purchase agreements) **in anticipation of future BESS GFM IBR installations** ~~**using**~~ **considering the use of** the materials contained in this guideline. **However, approval to install a GFM BESS should be carefully studied and approved by the PC and monitored by the TO after installation to ensure correct performance. Additionally, before installing a GFM IBR TOs should require IBR owners install adequate fault recording and sequence of event recording equipment to ensure adequate assessment of the performance of the GFM controls during BPS disturbances.**	Change made in document.
Edison Electric Institute	129 - 130	EEI does not support this recommendation as written: “TPs and PCs should integrate GFM functional testing requirements in their interconnection study processes that ensure newly connecting GFM is able to meet the performance requirements for GFM.” EEI does not agree that TPs and PCs are broadly viprepared to develop GFM testing requirements at this time.	EEI questions whether effective training can be developed for GFM controls as this time due to a lack of industry standards, however, we offer the following changes for consideration (in boldface): TPs and PCs should **begin training their staff in conducting studies to assess the functional differences in GFM controls so that they can be properly prepared for the future** integration of GFM **IBRs and become fully competent to develop** functional testing requirements in for their interconnection study processes **that will be required to** ~~**that**~~ ensure newly connecting GFM ~~**is**~~ are able to meet the performance requirements ~~**for GFM**~~ **of their service areas**.	The purpose of this white paper is to provide information to be used to educate and prepare the industry on GFM. Change made in document.

Edison Electric Institute	131 - 134	EEI does not support this recommendation as written: “GFM technology can operate reliably and provide stabilizing characteristics in areas of high IBR penetrations and areas of low system strength. GFM BESS presents a unique opportunity to support system stability (e.g., transient, oscillatory, voltage) with a relatively low incremental cost to all resources and end-use consumers.” There was not data contained in this white paper that validated that GFM controls on BESS can be operated reliably noting that there is no evidence contained in this white paper that the technology has been thoroughly tested on the BPS.	EEI offers the following changes (in boldface) for consideration: GFM technology ~~**can**~~ **has been shown to** operate reliably and provide stabilizing characteristics in areas of high IBR penetrations and areas of low system strength **in other countries and outside of the North American BPS (BPS). Given these impressive demonstrations of** GFM BESS **performance on other grids, it is now time to consider limited and controlled testing and validation of these systems on the BPS. While we are encouraged by the results seen by others outside of the BPS, careful testing and validation of GFM performance is still needed before broad deployment of this technology.** ~~**presents a**~~ **To** address the unique opportunities of GFM controls on BESS through their ability to support system stability (e.g., transient, oscillatory, voltage) ~~**with a relatively low incremental cost to all resources and end-use consumers**~~ **IBR owners and Developers should be encouraged to procure BESS systems with dual control capability (Grid Following and Grid Forming Controls) to enable broader validation of its performance on the BPS.**	Change made in document.
Edison Electric Institute	325 - 327	EEI does not support the following as currently written “This chapter defines the recommended functional specifications for GFM BESS. For effective and efficient adoption of GFM technology, TOs will need to establish functional specifications that define GFM functionality. The GFM specification can then be provided to OEMs by developers and GOs to ensure procurement of GFM resources.”	Proposed changes provided in boldface: This chapter ~~**defines the recommended**~~ **provides a template for entities in their development of** functional specifications for GFM BESS. **While this template should be considered just a guide,** ~~**, For effective and efficient adoption of GFM technology, TOs will need to establish**~~ **the information provided should provide a useful guide in the development of a** functional specifications that defines GFM functionality. ~~**The**~~ **Additionally, once a TO decides to allow the installation of a** GFM **enabled IBR within their service area** they are **encouraged to work** ~~**specification can then be provided to OEMs by**~~ **with their perspective** developers ~~**and GOs**~~ to ensure procurement of GFM resources **align to the TO’s desired specifications. Moreover, considerable caution should be exercised in preparation for the deployment of this equipment through the installation of owner installed digital fault recording and sequence of event equipment in order to monitor and assess the performance of the GFM controls. For this reason, it is suggested that limited deployments be allowed until proper performance of the GFM controls can be validated. NOTE: The following specification should only be considered as a guide for those TOs looking to test and validate GFM performance within their service area.**	Change made in document.

Edison Electric Institute	348 - 361, 388 -391	EEI does not support language used in the section titled “Functional Specifications Defining Grid Forming BESS” because white papers are not intended to provide enforceable requirements. The use of “shall” throughout this section implies that entities are required to adopt the recommendations as written and contained in those sections where shall is used.	Suggest removing “shall” and replace it with “should consider,” since this is a white paper and not a Reliability Guideline.	"Shall" is only used in the functional specification chapter and is necessary for a meaningful functional specification. All recommendations use "should" language. No change made.
David Jacobson		The primary intent of the White paper is to provide guidance to utilities who are considering adopting GFM in BESS as pilot projects. The recommendation "All newly interconnecting BPS-connected BESS should be designed, planned, and commissioned with GFM controls enabled..." is too strong a recommendation. IEEE 2800-2022, which is the latest IBR standard, noted the following, mainly in regards to GFM, "At the time of writing this standard, neither design details, test data, nor technical literature is available to confirm that emerging technologies and controls presently under research and development will be able to meet all specified requirements of this standard." In spite of that, the industry experts have done a great job collecting best available information to inform industry.	Please review/revise the recommendations to reflect the primary intent of the White paper. The recommendations should also summarize the key GFM functional specifications.	Change made in document.
David Jacobson		The Section on "Cost of Inaction" seems to be out of place in this White Paper and contains mixed messages. For example, I agree with the premise that entities should carry out studies to determine the benefits of using GFM technology in low grid strength areas and act quickly where opportunities arise to implement pilot projects. I'm also ok with the premise that all new BESS "should be considered" to at minimum have the capability of being upgraded with GFM controls if deemed necessary by studies. I don't agree with the final statement that it is strongly recommended that all newly interconnecting resources enable GFM controls to support enhanced BPS reliability. I believe it is too soon to make the leap from performing studies and installing pilot projects in weak areas to enabling GFM on all projects everywhere.	Please review the "Cost of Inaction" section to reflect the primary intent of the White Paper.	Change made in document.

David Jacobson		On page 2/12, the authors state "To the extent that existing requirements in IEEE 2800 may create any barriers to GFM applications, exceptions may need to be considered and specified by the TO." This creates a lot of doubt. The intent of IEEE 2800 is to be fully applicable to energy storage devices connected via inverters (GFL assumed).	Can the authors provide more guidance on which sections of IEEE 2800 may be in conflict with GFM technology, such as 7.2.2.3.4 Current injection during ride through mode?	The recommended requirements in this white paper are not intended to be overly prescriptive. This language is simply that all requirements are considered for conflicts before adoption. No change made.
David Jacobson		Several common specifications for GFM and GFL are noted but reference is only given to "applicable interconnection requirements."	Can the authors consider referencing IEEE 2800, for example, where applicable to reinforce use of this standard.	Requirements in IEEE 2800-2022 only become enforceable once they are adopted or referenced by transmission planners. No change made.
David Jacobson		Additional desirable characteristics of GFM technology such as passivity, negative sequence current and balanced internal voltage are noted as not being widely available but should be considered for future GFM technology. This creates some doubt as to the maturity of the technology.	Should a brief history of GFM technology evolution be presented? Where are we at in terms of GFM controls that are widely available. Is there a consequence if the controls don't provide the noted "desirable characteristics"? Here's a link to some history https://www.osti.gov/servlets/purl/1639991 ESIG notes in "Grid-Forming Technology in Energy Systems Integration" a few GFM control concepts are available such as virtual synchronous machine, droop, Virtual oscillator control. A brief description of the pros/cons of different techniques would be useful. Virtual synchronous machines may introduce artificial oscillation modes that other approaches wouldn't. Not all GFM is the same.	Thank you for the comment. No change made.
David Jacobson		Footnote 34 suggests that IEEE 2800.2 will be developing additional tests that will augment the list. While this is true, it should be noted that IEEE 2800 currently doesn't have special specifications for GFM technoology at present and any tests developed in 2800.2 won't be testing GFM features.	Please review and revise.	This footnote applied to model validation as a whole and not specifically GFM testing. No change made.
David Jacobson		For the GFL vs GFM tests, it is not clear what is assumed for the GFL and the system. How weak was the system? Was the GFL assumed to be modern and compliant with IEEE 2800 or was frequency/voltage control disabled?	Please review and revise.	Change made in document.
David Jacobson		2021 data noted 427 GW of BESS. If 2022 data is available it could be included to show the growth.	If data is available, please add to the White Paper.	
David Jacobson		I don't see mention of an active phase jump test being recommended in the white paper. Great Britain, for example, requires a 60 degree jump test to demonstrate the ability of the plant to provide active phase jump power. GFL inverters would be required to withstand the phase jump and not trip.	Please review and revise.	The tripping of the synchronous machine already subjects the GFL to a phase jump. No change made.

REV Renewables	105	NERC should clarify that any grid-forming requirements would only be for future projects and would not apply to existing projects or projects in development. Existing project retrofits would require product specific solutions that will be significantly more complex and costly than future project compliance. Hardware additions are expected (e.g., transient overvoltage protection) and will incur field retrofit costs and require plant outages to implement. In cases where a given product or manufacturer is no longer supported, full-scale replacement of plant inverters could be required at very high cost. Furthermore, significant specialized expertise will be needed to develop and evaluate the product specific GFM models. Investing this effort in bespoke and legacy product retro-fits will be many times more complex and time consuming than streamlined supplier and planner focus on future product compliance. In addition to the complexities and costs, a need to retrofit exisiting facilites has not been demostrated. The need for GFM on the US BPS has been assumed based on studies covering other systems and only show benefit at higher inverter based generation deployment than currently exists on the US BPS. If thorough analysis on the US BPS does show the need for GFM in the future, only a fraction of the total inverter based projects would even require GFM, making retrofits unnecessary.	The requirements should only be for future projects.	This paper's primary recommendation is to enable GFM in newly interconnected BESS installations. The inclusion of existing BESS is listed as a possible solution if retrofits are feasible and economic. No change made.
REV Renewables	101 - 103, 121	An initial major concern with mandating this functionality for new resources is the availability of validated GFM equipment models and timing of any new requirements / studies. The whitepaper proposes general GFM tests (simulations) to validate functionality. A key input to the test simulations are OEM-provided validated models and validation test reports against lab or field test, or hardware-in-the-loop tests. At present, only a small group of inverter suppliers have this capability. Any sudden mandated use of GFM could result in an inverter supply constraint for a period of time, which would drive up price or increase lead times for inverter equipment. This is of particular concern given existing supply chain challenges causing project delays. Current procurement and construction timelines require selection of inverter equipment many years in advance of a project's initial operation. Any new requirements should not be required for projects with initial delivery dates within 3 years of finalization of GFM requirements.	Any requirement for future BESS projects should phase in gradually over time (e.g. 3-5 years). Consider an initial voluntary period including incentives for early GFM adoption.	This paper provides recommendations with "should" language and thus implementation by industry can be decided by industry. No change made.

REV Renewables	373	REV agrees with distinction between grid-forming and black start requirements. Black start entails additional project capabilities to GFM that will increase cost of compliance. For example, the storage reserve capacity requirements are typically much larger (adding significant cost) for black start due to the required duration of response. In addition, inverters will require back up power supply or extended UPS supply to black-start which further increases cost.		Thank you for your comment. No change made.
REV Renewables	385-391 577	REV agrees that GFM requirements should apply "when the BESS is within its limits of the energy source behind the inverter and the equipment ratings of the inverter"; however, the following concerns are noted: (1) the example in Test 3 shows BESS 2 temporarily exceeding its stated power limit. There is a footnote that "BESS 2 has extra power capability at the inverter level, allowing it to momentarily exceed site power limit"; however, this example introduces confusion as to what is the expected performance at maximum active power. (2) The paper states "GFM BESS shall continue providing GFM operational characteristics even at its highest and lowest allowable state of charge". That's not possible for active power without reserve capacity. Very short duration response requirements (a few seconds) do not require costly reserve capacity (may not be more than a few kWh), but anything longer than a few seconds may add significant cost depending on the required response duration.	Agree that GFM should only apply "when the BESS is within its limits of the energy source behind the inverter and the equipment ratings of the inverter"; however, the expected response metrics for active power, reactive power, rise time and duration should be better charactarized for stakeholder review.	Thank you for your comment. The success criteria in this white paper are designed not to be overly prescriptive. Providing specific quantitative criteria is out of scope for this white paper.

REV Renewables	277-321	Studies on the US BPS need to be performed to determine the need for GFM. Studies used in the white paper mostly consist of island systems with much higher IBR capacity than is present on the US BPS. The studies should also assume that frequency and voltage stability are provided by GFL IBRs, since this is already a requirement for many LGIAs. The data and studies used in this white paper are insufficient to determine a timeline for when GFM is needed in the US BPS. Given the differences in the referenced systems compared to the US BPS, it is assumed that the need date is in the future, but criteria to determine conditions necessitating GFM should be confirmed based on studies of the US BPS.	Studies of the US BPS need to be performed to inform the criteria underwhich and timeline of when GFM is needed.	The scope of the paper is primarily to provide functional specifications and model testing methods. No change made.
Bonneville Power Administration	N/A	BPA's observation is that the basic concepts of this document would likely apply to any resource, not just battery systems. We are going to need grid-forming capabilities on wind and solar as installations, as well.		Thank you for your comment.
Morgan King	188	Isn't it Hawaiian Islands, not Hawaii Islands	Hawaiian Islands	Change made in document.
MISO (Iknoor Singh)	N/A - Global comment	As EMT modeling is new, few entities are performing their own, in-house EMT modeling. Instead, entities are relying on vendors to conduct these studies. As there is a general lack of industry experience in running EMT studies, it would be helpful to know whether it is possible to run the GFM functionality verification tests using positive sequence tools that a majority of entities in industry are already familiar with (e.g., PSSE, PSLF and TSAT).	Add a section to discuss whether it is possible to run GFM functionality verification tests using positive sequence tools that a majority of entities in industry are familiar with; such as PSSE, PSLF, TSAT, etc., and if not, describe why not.	This paper states "using detailed and accurate EMT models... is necessary". No change made

MISO (Iknoor Singh)	N/A - Global comment	This white paper, Grid Forming Functional Specifications for BPS-Connected Battery Energy Storage Systems (BESS), is a good start.	MISO would like to see the whitepaper expanded to address all Inverter-Based Resources (IBRs) and not just BESSs.	Thank you for your comment. This paper has a specific scope for BESS. No change made.
MISO (Iknoor Singh)	2	The underlined text in the following two sentences appears to be contradictory: “This uniquely differs from conventional grid following (GFL) IBR controls in that the primary GFL control objective in the sub-transient time frame is to maintain a constant output current phasor magnitude and angle. The current phasor begins changing within the sub-transient time frame to control the active and reactive power being injected into the network.” Similarly, the next sentence seems to contradict the earlier statement of maintaining constant current phasor: “conventional GFL inverter’s control objective is to maintain a desired active power and reactive power.”	The underlined text in the following two sentences appears to be contradictory. Please clarify. “This uniquely differs from conventional grid following (GFL) IBR controls in that the primary GFL control objective in the sub-transient time frame is to maintain a constant output current phasor magnitude and angle. The current phasor begins changing within the sub-transient time frame to control the active and reactive power being injected into the network.” Similarly, the next sentence seems to contradict the earlier statement of maintaining constant current phasor: “conventional GFL inverter’s control objective is to maintain a desired active power and reactive power.”	Change made in document.
MISO (Iknoor Singh)		In the pre-trip condition, the synchronous generator is supplying both the connected load and the batteries. Therefore, should the success criteria under Pre-Trip be modified? From: “Synchronous generator active power output matches the rest of the load” To: “Synchronous generator active power output matches the load and the BESS charging load”	In the pre-trip condition, the synchronous generator is supplying both the connected load and the batteries. Therefore, should the success criteria under Pre-Trip be modified? Please clarify. From: “Synchronous generator active power output matches the rest of the load” To: “Synchronous generator active power output matches the load and the BESS charging load”	Change made in document.

MISO (Iknoor Singh)		Relabel the three figures as Figure B.1 to Figure B.3.	Relabel the three figures as Figure B.1 to Figure B.3.	Change made in document.
MISO (Iknoor Singh)	N/A - Global comment	Grid following versus grid forming; i.e. a capacitor can regulate voltage but not produce it.	Ensure the grid following versus grid forming concept is clear thoughout the whitepaper.	Thank you for your comment.
MISO (Iknoor Singh)	Table 2.1 Table 2.2 Table 2.3 Table 2.5 Table 2.6 Table 2.7 Table 2.8	Description of GFM Functional Tests and Success Criteria The current Post-Trip Success Criteria is too subjective. For example: - "Immediately following the trip, BESS output should be well controlled. System frequency and voltage should not oscillate excessively or deviate from steady state levels for any significant amount of time." The Post-Trip Success Criteria should be more explicit, similar to what was done with Pre-Trip Success Criteria on page 5. For example: - Frequency should be 1 pu. - Voltage at Bus 1 should be within 5% of nominal.	Better define Post-Trip Success Criteria to measurable quantities such as those in the Pre-Trip Success Criteria or those in Table 2.4 (page 9)	Thank you for your comment. The success criteria in this white paper are designed not to be overly prescriptive. Providing specific quantitative criteria is out of scope for this white paper.

MISO (Iknoor Singh)	Global comment	For EMT studies, there is a need to scale up the granularity of EMT modeling	For EMT studies, there is a need to scale up the granularity of EMT modeling	Thank you for your comment.
Advanced Energy United, Mike Gabriel submitter		Advanced Energy United is a national association of businesses that are making the energy we use secure, clean and affordable. Advanced Energy United is the only industry association in the United States that represents the full range of advanced energy technologies and services, both grid-scale and distributed. Advanced energy includes energy efficiency, demand response, energy storage, wind, solar, hydro, nuclear, electric vehicles, and more. The comments expressed in this filing represent the position of Advanced Energy United but may not represent the views of any particular member.		Thank you for your comment.
Advanced Energy United, Mike Gabriel submitter	107/108	"Low incremental project cost" is subjective. The paper needs to be modified to include some representation of the additional cost that would be incurred by the owner to implement GFM capability. Survey the available OEMs/vendors and obtain an understanding of the percentage increase in cost per inverter that is outfitted with GFM. It is understandable that the OEMs/vendors would want to protect their pricing, so this data should be anonymized, and only provided as a range of percentages of cost increase, and not a specific price.	Provide an average percent increase in cost per inverter that is provisioned with GFM, such that potential owners as well as market operators and regulators understand the incremental cost increases.	Multiple BESS manufacturers were involved in the drafting process and provided information on the general cost to enable GFM capabilities but no specific ranges were given. No change made.
Advanced Energy United, Mike Gabriel submitter	118	"GFM requirements, policies, and/or market incentives should be developed for BESS…" The market incentives must be a pre-requisite, not an afterthought that may or may not be implemented. Adding (undefined as of yet) costs to projects can have a chilling effect on getting the necessary financing to conduct the project.	Make a firm recommendation about incentives and compensation for the additional cost of GFM technology.	Incentives and market based solutions are out of scope of this white paper. No change made.

Advanced Energy United, Mike Gabriel submitter	124	"may be able to be retrofitted at relatively low incremental costs". Define the costs as in line 14 above.	See line 14 above.	Multiple BESS manufacturers were involved in the drafting process and provided information on the general cost to enable GFM capabilities but no specific ranges were given. No change made.
Advanced Energy United, Mike Gabriel submitter	214	Incentivizing the adoption of GFM should not be optional. See lines 678, 705, 706.	change "may" to "must"	Incentives and market based solutions are out of scope of this white paper. No change made.
Advanced Energy United, Mike Gabriel submitter	221	Incentivizing the adoption of GFM should not be optional. See lines 678, 705, 706.	strike "or requirements"	Incentives and market based solutions are out of scope of this white paper. No change made.
Advanced Energy United, Mike Gabriel submitter	233	Adding future GFM capability will add costs to a project. The paper needs to be modified to include some representation of the additional cost that would be incurred by the owner to implement future GFM capability. Survey the available OEMs/vendors and obtain an understanding of the percentage increase in cost per inverter that is outfitted with future GFM capability. It is understandable that the OEMs/vendors would want to protect their pricing, so this data should be anonymized, and only provided as a range of percentages of cost increase, and not a specific price.	Provide an average percent increase in cost per inverter that is provisioned with future GFM capability, such that potential owners as well as market operators and regulators understand the incremental cost increases.	Multiple BESS manufacturers were involved in the drafting process and provided information on the general cost to enable GFM capabilities but no specific ranges were given. No change made.

Submitted on behalf of Energy Systems Integration Group - Jason MacDowell	All	To date, the continental US is behind other countries in Europe (e.g. Great Britain, Germany) and Australia regarding grid forming specifications and testing guidelines. This critical whitepaper sets the stage for specification and testing of GFM BESS in North America, which may in turn, evolve to all GFM resources. This paper uniquely outlines various test scenarios and methodologies of the important attribues of GFM BESS that can resolve grid reliability gaps with high penetration of IBR. The contents are technically and procedurally solid and the references to other work help to create requirements, codes and standards necessary to maintain reliability. Without these specifications and testing procedures in place, there will be severe limits to taking full advantage of cost-effective GFM capabilities, which may also pose reliability risks to the system if GFM is not deployed as part of the solution. It will also be used as a foundational reference for ESIG's reliability working group and the Global Power System Transformation Consortium's Grid Forming Implementation Council. Congratulations and job well done to IRPS and the authors for publishing such a critically important docuemnt.	No changes.	Thank you for your comment.
Southern Co. SCS Trans-Inc.		Southern believes that the reasoning behind this whitepaper is that the issue of establishing clear GFM fuctional specifications for BESS is really hard to quantify in studies as it is not known how much is needed, why it's needed , along with the location of these resources. We believe that this whitepaper should be more concise and state the minimum specifications, while also stating that these specifications should not be supplemented by anything other than what the TP/PC has identified through its detailed studes or known system conditions. For a wide scope adoption of GFM capability in all BESS inverters, there may be potential interaction with nearby existing synchronous generators, other GFL an+E13d GFM resources itself. There is no measure in this document to help understand how instability may arise due to such control interactions. In addition, the integration of GFM should require compliance with industry standards. It is not clear if standard like IEEE 2800-2022 applies or need to be revised to be fully compatible with the unique characteristics and capabilities of GFM inverters. Furthermore, the adoption of GFM capability in BESS (as an IA or PPA requirement) without proper industry standard and testing platform may involve significant upfront costs. Balancing the costs and benefits of GFM inverters to ensure their economic viability and sustainability of a system can be a challenge at the moment.	1) TOs in consultation with their TPs and PCs, should establish clear GFM functional specifications for BESS in their interconnection requirements (or provisions in power purchase agreements) using the materials contained in this guideline. (TOs, TPs, PCs)	Thank you for your comment.
Southern Co. SCS Trans-Inc.		Southern believes that the lack of testing of GFM capabilities especially at a large scale, may not be well-established or harmonized yet and the effectiveness of GFM will not exist in the current TP/PC models, because most of them are not an area of concern. It seems more prudent to require the minimum specifications and require the GO to provide a model for the TP/PC to utilize in future simulations when the GFM is activated. In addition, the TO should establish a validation process prior to depending or implementing the technology.	2)TPs and PCs should integrate GFM functional testing requirements in their interconnection study processes that ensure newly connecting GFM is able to meet the performance requirements for GFM. (TPs, PCs)	Thank you for your comment.
Southern Company	103	Footnote is a claim that is not substantiated by any documentation.	Remove foot note or provide actual referance documentation	Footnone 1 provides a link to an IEEE paper supporting the information in the white paper. No change made.

Southern Company	104-105	The recommendation to require GFM with all BESS projects based on the "near zero" percentage of GFM, is some what miss leading since most if not all bidirectional inverters used in BESS have some form of grid forming mode.	Better requiment is to ensure that all bidirectional inverters used in BESSs meet cirtain requierments, test performance and are standerized. There are several well researched and tested ways to address to address the instability caused by the introduction of IBR and the shutting down of large rotating machines	The "near zero" refers to BESS facilities without GFM modes enabled. GFM modes may be available but not enabled. The paper recommends that all newly interconnecting BPS-connected BESS should be designed, planned, and commissioned with GFM controls enabled. No change made.
Southern Company	107	"retrofitted with GFM technology and new BESS can be equipped with GFM technology at a relatively low incremental project cost" Is dependent on the stage of the project is at and what atributes the GFM inverter is to meet, although metion in the foot note the cost of new interconnection study in both time and money is not trifle.	Provide a more realistic justification	Multiple BESS manufacturers were involved in the drafting process and provided information on the general cost to enable GFM capabilities but no specific ranges were given. No change made.
Southern Company	116	"GFM technology is commercially available and field-proven for BPS-connected applications, " Such a statement requires documentation and references on its own is extreamly missleading.	Justify or rewrite	Change made in document.
Southern Company	122-123	There is little to no studies that have been performed on large grid scale to make these claims	Justify or remove	Large scale modeling challenges are highlighted and grid stabilization benefits are demonstrated internationally. No change made.
Southern Company	123	"ensure requirements… are in contractual language with OEM"	What requirements and how do we recommend their language be written? One limited example is some what provided by foot note.	This paper provides functional specifications that can be used to inform requirements. Providing specific quantitative performance requirements is out of scope for this white paper.Thank you for your comment.
Southern Company	124	"Existing BESS may be able to be retrofitted at relatively low cost" is not true in general and I may say in most if not all cases	Justify or remove	Multiple BESS manufacturers were involved in the drafting process and provided information on the general cost to enable GFM capabilities but no specific ranges were given. No change made.
Southern Company	126-128	While the statement is correct we do not provide suffient guidelines/recommendation to perform this task.	Correct the deficiency	This paper provides functional specifications that can be used to inform requirements. Providing specific quantitative performance requirements is out of scope for this white paper.Thank you for your comment.
Southern Company	131	"GFM technology can operate reliably and provide stabilizing characteristics in areas of high IBR penetrations and areas of low system strength." This is an unproven statement when pertaining to large grids and high penatration of IBRs	Provide documentation and or referance	Relevant references are provided throughout the white paper. Thank you for your comment.
Southern Company	135-139	This paragraph does not belong under the Key Takeaways and Reecommendations; minimally as a listed item	Remove it from the listed items and place on its own.	Thank you for your comment.
Southern Company	282-285	Given the very few actual studies and research with large interconnected power grid and the complex nature of GFM's sub cycle interaction and required controls it is imprudent to claim any industry recommendations on this topic.	Do not claim as industry recommendation or clearly state that that they are guidance extrapolated from small islanded system interacting with localized grids.	Large scale modeling challenges are highlighted and grid stabilization benefits are demonstrated internationally. Relevant references are provided throughout the white paper. Thank you for your comment. No change made.

0	Lines 340-341: Disturbance Ride-Through Performance27: Capability of the facility to ride through normal grid disturbances 340 within a defined set of parameters or expectations including but not limited to faults	The North American Electric Reliability Corporation (NERC) has released a document titled "Grid Forming Functional Specifications for BPS Connected Battery Energy Storage Systems" in June 2023 and has requested comments on this document. We appreciate the opportunity to comment on these functional specifications. The Bulk Power System (BPS) is of strategic importance to the United States; it is important that whatever is done preserves or enhances existing reliability, availability, and resilience of this strategic resource. On page 2 of the document, Lines 385-387, NERC states the following: All the functional specifications listed above are applicable when the Battery Energy Storage Systems (BESS) is within its limits of the energy source behind the inverter and the equipment ratings of the inverter. These functional specifications do not impose any requirements for fault current capability beyond equipment ratings. A footnote to this paragraph states: Transient conditions can cause Grid Forming Mode (GFM) BESS to reach current limits, resulting in transient behavior that differs from the GFM performance characteristics described above. The footnote does not specify any excess capacity above "the equipment ratings of the inverter", so the original stated requirement (capacity only up to equipment ratings of the inverter) seems to imply no excess capacity requirement for the inverter. This standard of behavior does not appear to align with the standards of behavior of rotating-machine generation systems. IEC 60034-1 states that an alternator must be capable of withstanding occasional excess current equal to 1.5 times the rated current for not less than 30 seconds, for rated outputs not exceeding 1200MVA.[1] If inverter-based BESS are to successfully supplement or supplant rotating machines in the BPS, it appears that their overload capacity should be equivalent to the rotating machines they replace. It is not clear that the proposed standard functional specifications meet that requirement. We believe the NERC functional specifications should state this requirement explicitly. The Specifications also do not explicitly deal with the fact that peak load periods are frequently caused by weather extremes accompanied by wind and cloud conditions that make inverter-based GFM resources unavailable. We believe it should be explicitly stated that wind and solar resources cannot always be used to meet, or partially meet, expected peak load conditions, and that battery-based systems can only be accredited for the amount of time they can be expected to deliver their full rated capacity. MITRE thanks NERC for this opportunity to comment. [1] https://www.stamford-avk.com/sites/stamfordavk/files/AGN013_C.pdf		Equipment ratings includes any available overload capability. No change made in document

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

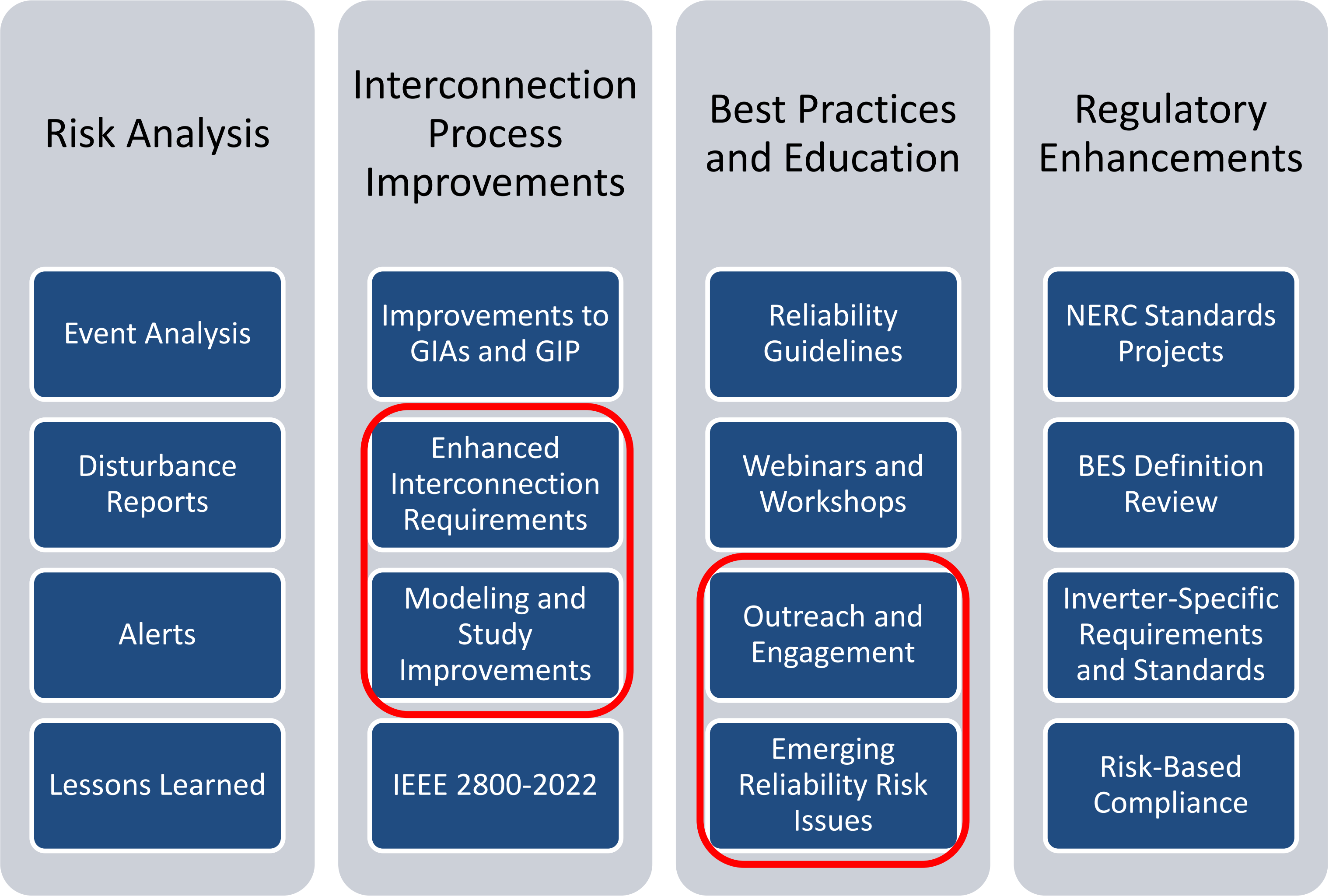
Development of

White Paper: Grid Forming Functional Specifications for BPS-Connected Battery Energy Storage Systems

Julia Matevosyan IRPS Chair | Jody Green, Sponsor
RSTC Meeting
September 20, 2023

RELIABILITY | RESILIENCE | SECURITY

NERC IBR Strategy



Risk Analysis

- Event Analysis
- Disturbance Reports
- Alerts
- Lessons Learned

Interconnection Process Improvements

- Improvements to GIAs and GIP
- Enhanced Interconnection Requirements
- Modeling and Study Improvements
- IEEE 2800-2022

Best Practices and Education

- Reliability Guidelines
- Webinars and Workshops
- Outreach and Engagement
- Emerging Reliability Risk Issues

Regulatory Enhancements

- NERC Standards Projects
- BES Definition Review
- Inverter-Specific Requirements and Standards
- Risk-Based Compliance

White Paper Background

- White Paper: Grid Forming Functional (GFM) Specifications for BPS-Connected Battery Energy Storage Systems
  - Provides functional specifications for Transmission Owners (TOs), Transmission Planners (TPs), and Planning Coordinators (PCs) to reference when establishing interconnection requirements
  - Provides information on currently in-service GFM resources and examples of GFM specifications, requirements, and grid codes currently in-use internationally
  - Includes recommendations to be utilized by TP and PC to implement GFM testing and to promote the interconnection of GFM resources
  - This white paper has undergone IRPS comment and an additional industry comment period
    - Numerous revisions were made to the address comments received
    - Changes made in the redline document are technical in nature and this white paper is currently undergoing non-substantive, editorial review through NERC Publications.

Additional Industry Comment Period

- 130 Comments provided by 20 entities
  - Predominantly from registered entities
  - Very positive comments on the paper from manufacturers and registered entities
- IRPS drafting subgroup met numerous times to address the comments
- General themes of the comments:
  - Clarification was needed for various aspects regarding the GFM functional tests and their implementation
  - Additional references or analysis were needed, particularly for North American bulk power system (BPS)
  - Confusion over the use of “should” and “shall”
- IRPS drafting subgroup made numerous revisions to address these comments
  - Details regarding the comments received and NERC’s response are located in the comment matrix provided with this meeting's materials

Use of “Should” and “Shall”

- “Shall” is critically necessary when providing functional specifications
- “Shall” is used exclusively in the *Functional Specifications Defining Grid Forming BESS* section
- No recommendations use “shall”
- **“Should” is used for all industry recommendations regarding the potential implementation of GFM technology**

Developments During Review Period

- Fingrid (Finland) has published GFM IBR requirements
  - Defined Specific Study Requirements for BESS where the use of GFM controls is seen necessary
- AEMO (Australia) has published Voluntary Specifications for Grid-forming Inverters
  - Provides guidance to stakeholders while the regulatory environment develops
  - AEMO's definition of GFM IBR is similar to NERC's definition in this paper
- ERCOT released a "Preliminary Assessment of GFM IBR Energy Storage Resources in the ERCOT Grid"
  - Shows GFM could be a viable option to improve BPS stability
  - ERCOT will continue work on GFM requirements
- IRPS is seeking RSTC approval for this white paper

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Grid Forming Functional Specifications for BPS-Connected Battery Energy Storage Systems

June 2023

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

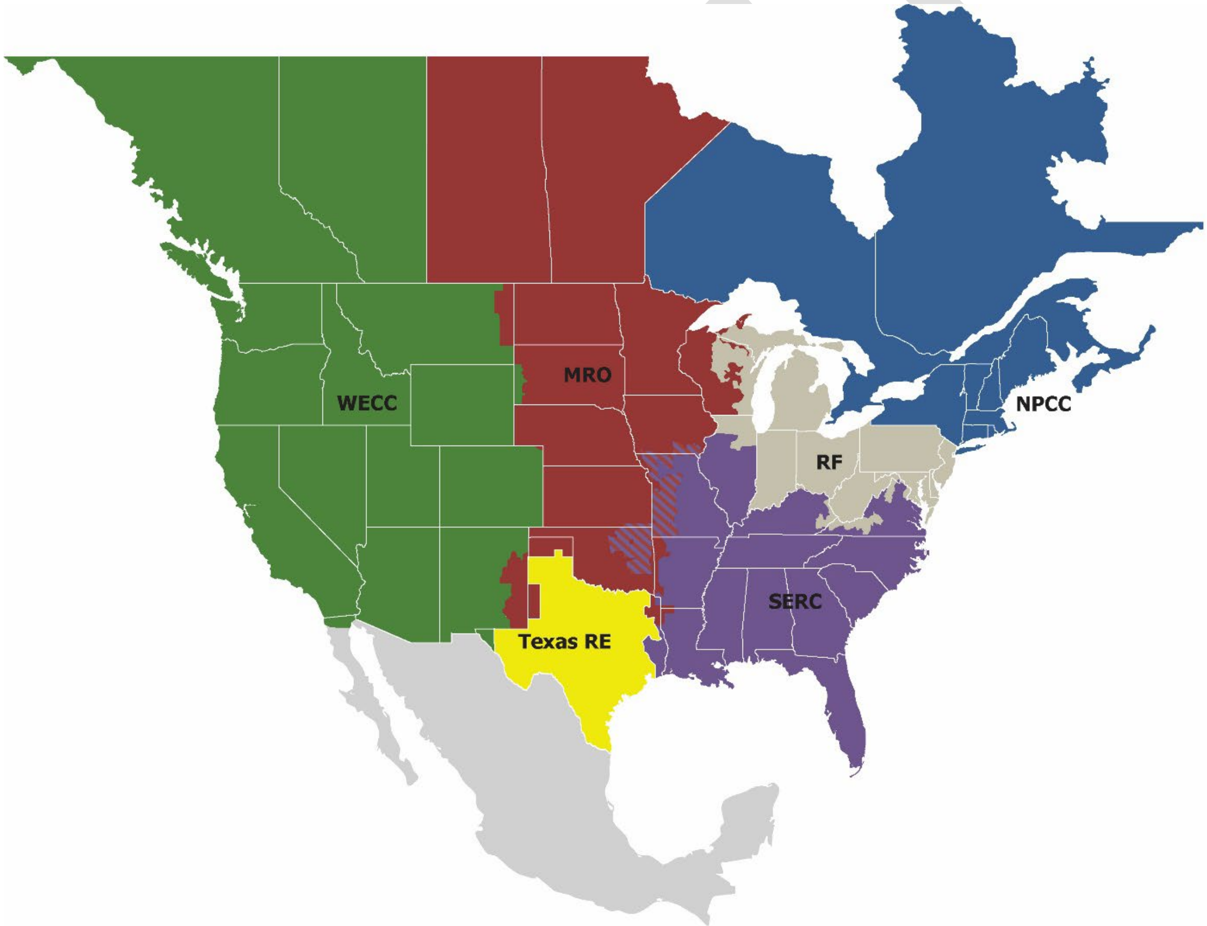
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of NERC and the six Regional Entities, is a highly reliable, resilient, and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six Regional Entities as shown on the map and in the corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Executive Summary

Studies have shown that grids dominated by inverter-based resources (IBR), in the absence of supplemental synchronous machine-based solutions, need grid forming (GFM) IBRs to maintain stable operation. While some smaller islanded systems are already facing these challenges today, it is expected that the need for GFM technology will accelerate with the rapid growth of IBRs across North America and the world. Industry needs to proactively plan to ensure sufficient GFM IBRs are installed on the system under these future operating conditions. One of the most significant obstacles of deploying GFM on the bulk power system (BPS) is establishing clear interconnection requirements regarding the expected performance, testing, and validation of the technology. This paper addresses how Transmission Owners (TOs), Transmission Planners (TPs), and Planning Coordinators (PCs) can establish these requirements and test interconnecting resources to ensure they meet the GFM specifications. Generator Owners (GOs) will also have clear performance expectations for GFM resource interconnections and can work with their respective equipment manufacturers prior to interconnection studies being conducted to help streamline the interconnection queue process, where possible. TPs and PCs will need to test new project models to ensure they meet the GFM specifications. The recommended set of GFM tests are provided in this paper, designed to verify the unique characteristics of GFM. The paper also addresses GFM model quality and accuracy as a prerequisite to any studies being conducted.

A common question posed by industry stakeholders is "how many future IBRs should be deployed with GFM functionality enabled?" The answer is system-specific and requires detailed reliability studies to determine, and studies conducted thus far indicate these numbers may be upwards of 30%.[1,2,3] Since the current percentage of GFM resources is near zero in nearly all large interconnected power systems, it is recommended to start requiring and enabling GFM in all future Battery Energy Storage System (BESS) projects for multiple reasons. GFM technology is commercially available but has not yet been widely deployed. While this technology has great potential in its ability to help improve stability and reliability in areas with high IBR penetration or low system strength areas, responsible entities should evaluate GFM IBR benefits and performance on their system before following-up with wide-scale implementation[4]. New BESS can be equipped with GFM technology at a relatively low incremental controller and hardware cost[5] [6]. Implementing GFM controls at existing GFL BESS projects may only requires controls changes. However, these changes to an existing plant, as a material modification, will require additional studies to determine any impacts to BPS reliability. Due to the potential costs, time delays and complexities of this retroactive process, it is recommended that all new BESS projects are commissioned with the ability to perform GFM control, with GFM controls being enabled after being sufficiently studied. Enabling GFM in all future BESS projects is a relatively low-cost solution that helps ensure system-wide stability that is difficult to quantify today due to study limitations. Industry should begin specifying, requiring, and implementing GFM for all new BPS-connected BESS quickly to mitigate any potential BPS reliability risks that could be posed under high IBR penetration levels expected in the near future. Though the focus in this paper is on near-term BESS applications, GFM technology may need to be considered when developing new inverter-based transmission applications, such as STATCOMs or HVDC converter stations.

Key Takeaways and Recommendations

The following key takeaways and recommendations should be considered and implemented by the associated entities for adoption of GFM to improve overall BPS reliability under conditions of increasing penetrations of IBRs:

---

[1] https://ieeexplore.ieee.org/document/9875186

[2] Using the full capabilities of modern inverters may enable lowering this threshold somewhat.

[3] This percentage results from a studies performed outside of the North American BPS and is intended to be informational. In order to determine an appropriate percentage for a specific area, similar studies should be performed using large area EMT models.

[4] For example, ERCOT presented the results of ERCOT Assessment of GFM Energy Storage Resources at the Inverter-Based Resource Working Group meeting on 8/11/2023. As the next step, ERCOT will work on the requirements for GFM Energy Storage Resources including but not limited to performance, models, studies, and verification. See Appendix B of this paper for more details.

[5] New interconnection studies are recommended for the existing GFL project updated to GFM.

[6] Cost to implement GFM technology varies due to variations in the hardware on-site and the performance intended to be enabled.

- GFM technology is commercially available and field-proven for transmission-connected applications, particularly for BESS (including standalone BESS[7] in ac-coupled hybrid plants) as well as dc-coupled solar photovoltaic (PV)+BESS[8] applications. GFM requirements, policies, and/or market incentives should be developed for BESS or hybrid plants including BESS, as mentioned above. (Original Equipment Manufacturers (*OEM), developers, GOs, Generator Operators (GOP), TPs, PCs, Transmission Operators (TOPs), Reliability Coordinators (RCs), regulatory entities, policymakers)*

- All newly interconnecting BPS-connected BESS should be designed, carefully studied by responsible entities, and commissioned with GFM controls[9] enabled to improve overall system stability across the BPS, particularly with increasing levels of IBRs. Developers and GOs can ensure requirements[10] are in contractual language with OEMs. Existing BESS may be able to be retrofitted at relatively low incremental controller and hardware costs; however, they will need to be restudied by the TP, PC, TOP, RC, or BA and potentially retuned, as determined by the study results. In cases where the responsible entities conclude that barriers to deploying GFM BESS exist at this time, responsible entities should consider specifying IBRs that can be configured for both GFL controls and GFM controls; this will allow the controlled testing of the technology under both owner and responsible utility oversight. *(GOs, TPs, PCs, RCs, TOP, BA developers, OEMs)*

- TOs in consultation with their TPs and PCs, should leverage the information in this white paper to begin the process of establishing GFM functional specifications for BESS in their interconnection requirements (or provisions in power purchase agreements) in anticipation of future GFM BESS installations. As with any other resource, GFM BESS should be studied to assess its impact on the BPS before interconnection. Additionally, it is recommended to require adequate fault recording and sequence of event recording equipment before installing a GFM IBR to ensure adequate assessment of the performance of the GFM controls during BPS disturbances.

- TPs and PCs should begin training their staff in conducting studies to assess the functional differences in GFM controls so that they can be properly prepared to integrate GFM functional testing requirements in their interconnection study processes ensuring that newly connecting GFM is able to meet the performance requirements for GFM. *(TPs, PCs)*

- GFM technology has been shown to operate reliably and provide stabilizing characteristics in transmission systems outside of the BPS in areas of high IBR penetrations and areas of low system strength. GFM BESS presents a unique opportunity to support system stability (e.g., transient, oscillatory, voltage) with a relatively low incremental cost to all resources and end-use consumers *(Developers, OEMs, GOs, GOPs, TPs, PCs, TOPs, RCs)*. While the results seen by others outside of the North American BPS are very encouraging, careful testing and validation of GFM performance by responsible entities is still needed before broad deployment of this technology in their system.

- GFM technology will continue to develop and improve beyond where it is today. Future research efforts can help aid in accelerated development and adoption, particularly focusing on GFL-to-GFM conversion possibilities, equipment standardization, GFM in blackstart applications, technical specifications for GFM blackstart, and GFM controls in other IBR technologies such as wind and solar PV. *(US Department of Energy, national laboratories, research institutes, academic institutions)*

---

[7] World's largest 'grid-forming' battery to begin construction in Australia – pv magazine International (pv-magazine.com)

[8] Hybrid Solar and Storage in Hawaii | T&D World (tdworld.com)

[9] As functionally specified in this paper

[10] See, for example: Appendix J-1 Oahu RDG PSA (hawaiianelectric.com)

Introduction

Background

NERC *White Paper: Grid Forming Technology*[11] defined GFM controls for IBRs as:

> **Grid Forming Control for BPS-Connected Inverter-Based Resources** are controls with the primary objective of maintaining an internal voltage phasor that is constant or nearly constant in the sub-transient to transient time frame. This allows the IBR to immediately respond to changes in the external system and maintain IBR control stability during challenging network conditions. The voltage phasor must be controlled to maintain synchronism with other devices in the grid and must also regulate active and reactive power appropriately to support the grid.

This uniquely differs from conventional grid following (GFL) IBR controls in that the primary GFL control objective in the sub-transient time frame is to maintain a constant output *current* phasor magnitude and angle, with adjustments to control the desired active and reactive power being injected into the network. Hence, GFL does not maintain fixed voltage magnitude or phase angle on those timescales. On longer timescales (seconds), it can also pursue other control objectives such as maximum power point tracking, frequency response, and voltage regulation.

A GFM inverter's control objective, on the other hand, in the shortest [sub-transient] time frames (e.g., 0-5 cycles after a disturbance), is to maintain *voltage* phasor magnitude and angle internally, and prioritize the support of terminal voltage. Therefore, it does not maintain fixed active or reactive power on those time frames. On longer time frames, a GFM inverter must also synchronize with other sources and may also pursue other objectives including tracking of active power and reactive power set point. In all cases, the inverter controls could be restricted by the inverter and primary energy source capability limits (e.g., available energy, current limits, voltages).

Benefits of Enabling GFM Controls in BPS-Connected BESS

It is estimated that there was 427 GW of BESS capacity (including both standalone BESS capacity and BESS capacity as a part of hybrid plants) in the interconnection queues around the US as of the end of 2021.[12] By the end of 2022 this number increased to 680 GW[13]. In the absence of any requirements or incentives for GFM capability, all of these resources are being planned with GFL controls. Many of these BESS will be deployed in IBR-dominated areas of the BPS with existing stability constraints. Installing these resources as GFL will likely further reduce stability margins and may result in new stability constraints. This will lead to further reduction of low-cost generation from existing IBRs in these areas (i.e., curtailment of IBRs during real-time operation) due to stability constraints that could be addressed by GFM, thus increasing overall energy costs. To relieve these constraints without considering GFM in BESS, additional transmission assets such as synchronous condensers[14] , GFM STATCOM[15] with energy storage, or new transmission lines[16] will be needed which will drive transmission costs higher.

GFM controls can provide grid stabilizing characteristics that support reliable operation of the BPS under increasing penetration of IBRs. Enabling GFM in BPS-connected BESS allows for system-wide enhancement of stability margins as these resources are interconnected. Therefore, system stability enhancements can be achieved at much lower cost than through the addition of transmission assets.[17] As discussed above, GFM controls can be implemented on any type of IBR including new solar photovoltaic and wind plants with some limitations; however, GFM controls in BESS

---

[11] https://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_Grid_Forming_Technology.pdf

[12] https://emp.lbl.gov/sites/default/files/queued_up_2021_04-13-2022.pdf

[13] https://emp.lbl.gov/sites/default/files/queued_up_2022_04-06-2023.pdf

[14] https://aemo.com.au/-/media/files/electricity/nem/security_and_reliability/congestion-information/sa-transition-to-fewer-synch-gen-grid-reference.pdf?la=en

[15] STATCOM Technology Evolution for Tomorrow's Grid (nxtbook.com)

[16] Adding new transmission lines will decrease the transfer impedance (make it a stiffer/stronger system)

[17] Transmission assets still serve critical roles for overall BPS reliability in addition to the considerations for GFM BESS presented in this paper.

are particularly low hanging fruit for assuring BPS reliability since they already have the needed energy buffer on the dc side which makes the enhancement purely software-based (minimizing much more costly hardware-based improvements and/or the moderate level of curtailment that may be needed for other IBR technologies).

While some areas like the Hawaiian islands already need to enable GFM BESS to maintain grid stability and prevent large-scale outages, many areas of the US are reaching relatively high penetrations of IBRs now or in the future and will face similar challenges. Industry is faced with a unique window of opportunity to procure, test, and gain experience with GFM technology now before significant adverse reliability issues are faced with insufficient GFM controls installed in the future.

Testing and Demonstration of Services Ahead of Requirements

Existing GFL technology can provide a number of essential reliability services to the BPS. Demonstration projects[18] have illustrated these capabilities for many years, and modern IBR facilities can provide regulation services, primary and fast frequency response, dynamic voltage support, etc. GFM control do not preclude a resource from providing any of these critical features to the BPS. Rather, GFM controls enable additional features from BESS beyond what can be provided from GFL today. Examples include operating in low system strength conditions, improving overall system stability, helping stabilize the system following large generator loss events (supporting arresting frequency changes), and potentially enabling blackstart capability from IBRs.

Multiple GFM projects around the world have been deployed, with more GFM projects under procurement See **Table I.1** and more details in **Appendix A**. However, widespread adoption has been relatively slow due to limited pilot projects (particularly of large numbers of GFM resources in one area) and difficulties establishing GFM performance specifications and testing procedures. Furthermore, detailed studies of GFM technology require electromagnetic transient (EMT) modeling, which is challenging for large areas due to lack of expertise and computational limitations today.

Table I.1: GFM BESS Projects Deployed or under Construction

Project Name	Location	Size (MW)	Time
Project #1	Kauai, USA	13	2018
Kauai PMRF	Kauai, USA	14	2022
Kapolei Energy Storage	Hawaii, USA	185	2023
Hornsdale Power Reserve	Australia	150	2022
Wallgrove	Australia	50	2022
Broken Hill BESS	Australia	50	2023
Riverina and Darlington Point	Australia	150	2023
New England BESS	Australia	50	2023
Dalrymple	Australia	30	2018
Blackhillock[19]	Great Britain	300	2024
Bordesholm[20]	Germany	15	2019

While GFM capability in batteries can be delivered at relatively low incremental cost, there may still be some costs associated with project and product development simply due to the newness of the technology. Widespread adoption of GFM IBRs will ensure an adequate level of BPS reliability moving forward. In addition, market operators may establish market-based mechanisms that can drive GFM adoption at a rapid pace, where appropriate.

---

[18] Demonstration of Essential Reliability Services by a 300-MW Solar Photovoltaic Power Plant (nrel.gov)

[19] Zenobē breaks ground on pioneering 300MW battery in Blackhillock - Zenobē (zenobe.com)

[20] The Bordesholm stand-alone grid ensures power supply even in the event of a grid failure - Sunny. SMA Corporate Blog (sma-sunny.com)

The Cost of Inaction

This is a unique moment in the industry when a need is becoming fully understood and an effective, relatively low-cost GFM solution has emerged. GFM capability in BESS is a viable and effective solution to address declining stability margins system-wide and to manage decreasing system strength and the issues that arise under these conditions (e.g., wind and solar PV curtailments). The industry is at the cusp of a rapid growth of BESS capacity on the system in the next few years. Without GFM functional specifications and test procedures established by TOs, TPs, and PCs, and the appropriate incentives or requirements in place, much or all of the newly installed BESS capacity will likely not have GFM capability enabled (either precluding the possibility of GFM or requiring significantly more costly retrofits or network upgrades). If GFM capability is not adopted very soon, the outcome will be reduced transfer limits for existing IBRs and consequently growing levels of solar PV and wind curtailment, and additional costs of supplemental stabilizing equipment (e.g., synchronous condensers) in the future.

ISOs/RTOs/utilities should work with stakeholders to carry out studies of the implementation of GFM technology in low grid strength areas[21] and act quickly to implement pilot projects (similar to how the provision of ancillary services from GFL IBRs has been tested in the past). Experience from GFM BESS project installations around the world, particularly Great Britain and Australia (see **Appendix A**), can be used as a guide.

Presently, the recommendation is that all new BESS connecting to the BPS should have the capability for GFM operation or future capability to be upgraded with GFM controls (if necessary). TOs should establish this requirement in their interconnection requirements or power purchase agreements (PPAs). Developers and GOs can also ensure that these requirements are in contractual language with the equipment manufacturers. To support enhanced BPS reliability, it is strongly recommended that newly interconnecting BESS enable GFM capability, or have the capability for GFM controls. Additionally, GFM controls should be enabled only after being studied by responsible entity as with any new resource or qualified change.

Functionally Defining GFM Performance

Although the concept of GFM technology has been around for many years, mainly in small islanded systems or microgrids, the term has presented confusion in recent years when the concept is applied to the BPS. Various documents have proposed definitions to try and reduce confusion (see Appendix A for reference). Most definitions agree that at a minimum GFM controls tend to hold their voltage magnitude and angle at the device terminals constant in the period immediately following a system event. This tends to provide a resistance to change in the external system and thereby grants certain stabilizing properties. Although there is general consensus on what GFM is as a concept, opinions differ on the degree and extent the concept should be used when qualifying an interconnecting device as GFM, as well as how to test the capability. Specifying GFM may be done in a number of ways, including the following:

1. Control topology: The theoretical behavior of a device may be defined based on specific types of control topologies such as virtual synchronous machine or droop-based topologies. It is not recommended to define GFM behavior based on control topology, to leave the room for innovation.
2. *Quantitative response metrics:* The precise behavior of a device in response to external system events can be defined, with no regard to the internal control topology. Quantities like active and reactive power rise time in response to a network event can be used to test whether the controls provide the stabilizing influence expected from GFM.
3. *Frequency domain characterization:* GFM controls tend to have signature responses to stimuli with varying frequencies. It is likely possible to provide an accurate determination of the GFM capabilities of a device by

---

[21] Due to loss of last synchronous machine, an extremely low system strength scenario manifests in the tests described in this document

measuring its response to external perturbations across a range of frequencies[22]. Significant promising research work is underway in this field.[23] [24]

4. *General testing definition (***Recommended***):* It is possible to determine whether a device functionally meets the definition for GFM control by observing whether the device is capable of performing well during certain well-defined simulation tests. For example, GFM IBRs can be subjected to severe external events that are generally difficult or impossible for conventional GFL devices to stably operate through. For example, a GFM device, like a synchronous generator, is able to operate and serve load with no other synchronous machines in service. It is generally able to operate in synchronism with other synchronous machines, continue stable operation when those machines are disconnected, and continue stable operation when those machines are re-connected. GFL IBRs are generally not able to do all of these things. Even if a GFM plant will not be subjected to these events in real-time operation, the tests indicate that the controls can provide the stability benefits needed.

To avoid confusion and conflicts in understanding, the fourth approach is proposed and further described in Chapter 2, until sufficient research and field experience is available to fairly and effectively use other methods. This method provides confidence that GFM controls will provide the necessary stabilizing characteristics even if the specific test scenarios never occur during real-time operations. The general testing definitions in this white paper are not intended to be overly prescriptive and should be used to inform the development of future qualitative GFM performance requirements. The method is simple to implement and agnostic to GFM control topologies, and similar approaches have been successfully implemented in BESS procurements around the world[25] [26].

Minimum Necessary Capacity of GFM Inverters for Future High IBR Grids

It is well understood that as the penetration of IBRs continues to rise and the stabilizing effects provided by synchronous machines decrease, the grid will need some amount of GFM-enabled resources to ensure system stability[27]. This logically raises the question of a necessary or recommended capacity (presumably a % value) of GFM-enabled IBRs relative to the total capacity of IBRs and/or machines on the BPS. While industry does not currently have a rule-of-thumb to prescribe the minimum necessary capacity of GFM IBRs needed to stabilize a given system, recent research provides a few points of reference. This section outlines current industry recommendations on this topic.

Relatively few studies have been performed, particularly for large interconnected power systems. However, smaller islanded systems have explored this issue in much more detail. For example, power hardware in the loop (PHIL) tests of the HECO Maui system illustrated the percentage of GFM inverters needed for stability at various system inertia levels.[28] This work found that as system inertia dropped towards zero (an entirely inverter-based system), the amount of GFM inverters necessary to maintain system stability increased relatively linearly. When the system has zero mechanical rotating inertia system inertia, the percentage of GFM inverters relative to total system capacity (consisting of only GFM and GFL inverters) was around 30% (see **Figure I.1**). The GFL IBRs in this system consisted primarily of IBRs with no voltage or frequency support capability, with only a few grid-supportive GFL IBRs providing voltage support or fast frequency response. HECO also highlighted needing some reliability margin, therefore recommending that this ratio be increased to account for unexpected issues like legacy distributed energy resource momentary cessation issues or unexpected inverter tripping issues. This study also highlighted that the necessary

---

[22] Small-signal frequency-domain methods can be used as screening methods which are typically followed up by time-domain verification that consider both large and small-signal stability.

[23] Sequence Impedance Measurement of Utility-Scale Wind Turbines and Inverters - Reference Frame, Frequency Coupling, and MIMO/SISO Forms (nrel.gov)

[24] https://www.nrel.gov/docs/fy23osti/84604.pdf

[25] https://www.nationalgrideso.com/document/250216/download

[26] https://www.youtube.com/watch?v=2e5ET0L1j5g

[27] Note that, alternatively, adequately sized and placed synchronous condensers can also be used to ensure system stability with high IBR. However, with GFM capability provided by IBRs themselves, installation of these additional grid assets can be avoided.

[28] https://ieeexplore.ieee.org/abstract/document/9875186

capacity of GFM IBRs does not necessarily depend on the total percentage of generation from IBRs (which was above 95% in all cases studied). Instead, low total online synchronous machine capacity (as quantified via system inertia constant, for example) was a much better predictor of the need for GFM.

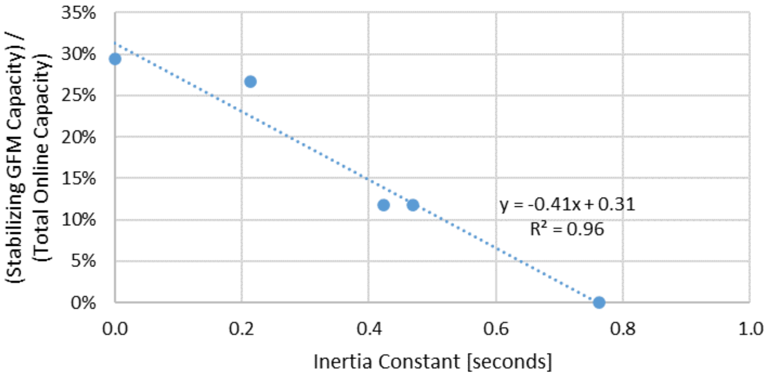


Figure I.1: HECO Study of GFM Needed for Stability at Various Inertia Levels

Similarly, a recent paper[29] from the European Union-funded project, MIGRATE, studied the composition of GFM and GFL inverters in various systems and identified a need for at least a 37% ratio of GFM IBRs to total IBRs in the system. There were sensitivities based on numerous factors that modified that number slightly.

It is important to note that the actual GFM capacity needed for system stability will vary from system to system and can also depend on the type of contingency being studied. Issues could be system-wide (e.g., need for stable fast frequency response) or could be more localized (e.g., need for operation in low short circuit strength networks). This could drive the need for stabilizing services from additional resources, or from existing installed resources. The needed capacity of GFM is also impacted by the dynamic characteristics of other sources in the network such as GFL inverters and load. With the approval of FERC Orders 842 and 827 and IEEE 2800-2022, the response of GFL resources may be more advanced than that of legacy IBRs, which could impact the necessary capacity of GFM to maintain grid stability.

As an example, a study on an island power network[30] identified that the minimum percentage of GFM required to maintain frequency and voltage stability was 11% if frequency and voltage support were provided by other IBR resources per IEEE 2800-2022. However, if GFL IBRs had no frequency and voltage response capability, the study identified that a minimum of 23.5% GFM IBR was necessary to maintain stability. Therefore, it is important that TOs, TPs, and PCs ensure adequate levels of GFM resources moving forward to maintain system stability, with suitable margin to avoid any adverse reliability impacts from unexpected performance issues.

---

[29] https://www.h2020-migrate.eu/_Resources/Persistent/5d0f8339650bcf53cd24a3006556daa1da66cb42/D3.4%20-%20New%20Options%20in%20System%20Operations.pdf

[30] "Services from IBR for future systems", 2022 ESIG Reliability Working Group Meeting, October 2022.

Chapter 1: Functional Specifications for GFM BESS

This chapter defines the recommended functional specifications for GFM BESS that applicable entities can use to inform inclusion of GFM specifications in their requirements. For effective and efficient adoption of GFM technology, TOs will need to establish functional specifications that define GFM functionality. The GFM specification can then be provided to OEMs by developers and GOs to ensure procurement of GFM resources.

Functional Specifications for GFM and GFL Battery Energy Storage

All BPS-connected generating resources are required to meet applicable interconnection requirements and performance-based standards. Requirements often establish specifications related to, but not limited to, the following:

- **Dispatchability:** Capability of the facility to be dispatched (or curtailed) to a specific active power set point
- **Steady-State Voltage Control:** Capability of the facility to control steady-state voltage at the point of interconnection to a specific voltage schedule (set point and operating band)
- **Dynamic Reactive Power Support:** Capability of the facility to provide dynamic reactive support in response to normal and emergency grid conditions within the expected ride-through performance range
- **Active-Power Frequency Control:** Capability of the facility to respond to changes in system frequency by changing active power output when the resource has available headroom/tailroom
- **Disturbance Ride-Through Performance[31]:** Capability of the facility to ride through normal grid disturbances within a defined set of parameters or expectations including but not limited to faults, and phase jumps
- **Fault Current and Negative Sequence Current Contribution:** Capability of the facility to provide fault current, including negative sequence current to mitigate unbalanced voltage conditions and facilitate relay operation[32]
- **Security:** Capability of the facility to ensure cyber and physical controls are in place to ensure resilience to potential threats.

Functional Specifications Defining Grid Forming BESS

Additionally, the functional specifications need to be clearly defined for the GFM-specific functions. The following are performance characteristics specific to GFM BESS: These characteristics shall be provided within GFM BESS equipment rating limits:

- **GFM-Specific Voltage and Frequency Support:** GFM shall provide autonomous, near-instantaneous frequency and voltage support by maintaining a nearly-constant internal voltage phasor in the sub-transient time frame, including:
    - **Phase Jump Performance:** GFM shall resist near-instantaneous voltage magnitude and phase angle changes by providing appropriate[33] levels of active and reactive power output in the sub-transient time frame.
    - **System Strength Support:** GFM shall help reduce the sensitivity of voltage change for a given change in current in the sub-transient time scale.

---

[31] GFM BESS FRT capability and performance during and after the fault is critical to grid stability and should be tested just as it would be for a GFL facility

[32] This can be achieved, for example, by maintaining balanced GFM resource internal voltage during asymmetrical faults.

[33] As an example, if the phase difference between the inverter terminal and the grid increases, the resource should increase (or make less negative) its active power injection in the sub-transient time scale. If the phase difference reduces, it should result in a reduction of its active power injection in the sub-transient time scale.

- **Ability to Stably Operate with Loss of Last Synchronous Machine:** GFM shall be able to stably operate through and following the disconnection of the last synchronous machine in its portion of the power grid[34].

There are additional desirable characteristics for GFM performance; however, present technology may not be able to widely meet this performance specification today. Therefore, they are listed here for consideration in specification for future GFM technology. They include the following:

- **Passivity:** GFM should present a non-negative resistance and present a passive characteristic to the grid within a wide frequency range (0–300 Hz) to prevent adverse interactions.
- **Negative Sequence Current during Continuous Operating Region:** GFM Plant should provide negative sequence current.
- **Balanced GFM Internal Voltage:** The GFM resource should also ensure its internally generated voltage remains balanced during all near-nominal operating conditions (e.g., 0.9–1.1. pu voltage range).

Blackstart Considerations

GFM and blackstart-capable are not synonymous terms; however, GFM functionality is a prerequisite for an inverter-based resource (IBR) to be eligible for blackstart capability. The TO, TOP, or RC may establish additional requirements for blackstart capability[35] beyond the general specifications for GFM, which may necessitate extended capability for the short-term overcurrent, more stringent ride-through capability, longer energy duration needs or additional hardware to supply sufficient and reliable start-up power to restore the electricity system from a blackout. These unique local requirements may preclude certain GFM resources from participating in blackstart services. It should be noted that a GFM IBR does not necessarily have to provide blackstart services, and blackstart capability requirement should be specified separately.

Additional Considerations

The following are additional considerations for the functional specification of GFM in BESS:

- All the functional specifications listed above are applicable when the BESS is within its limits of the energy source behind the inverter and the equipment ratings of the inverter[36]. These functional specifications do not impose any requirements for fault current capability beyond equipment ratings.
- GFM BESS shall continue providing GFM operational characteristics even at its highest and lowest allowable state of charge. If the BESS remains connected to the network, it shall remain in GFM mode as defined in the Introduction of this document. There should be no state of charge condition where the BESS should need to operate in GFL mode.
- Performance requirements for BPS-connected inverter-based resources such as, for example, IEEE 2800 may also apply to GFM resources unless explicitly stated by the local interconnection requirements. To the extent that existing requirements in IEEE 2800 may create any barriers to GFM applications, exceptions may need to be considered and specified by the TO, TOP, RC, or BA. Simultaneously, industry can contribute towards improvements of the relevant standards to accommodate the requirements for GFM.

---

[34] While generation capacity in the system can still meet the load.

[35] https://www.hawaiianelectric.com/documents/clean_energy_hawaii/selling_power_to_the_utility/competitive_bidding/20220531_exh_5.pdf

[36] Transient conditions can cause GFM BESS to reach current limits, resulting in transient behavior that differs from the GFM performance characteristics described above.

Chapter 2: Verifying GFM Functionality

This chapter describes the functional performance verification tests that determine whether an interconnecting BESS can be classified as GFM. TPs and PCs should integrate these tests as part of the interconnection study process in coordination with TOs, PCs, BAs, or TOPs establishing GFM requirements for newly interconnecting BESS. GOs, developers, OEMs can ensure that planned facilities meet these functional specifications prior to interconnection studies, which will help expedite the process. Verifying GFM functionality with test simulations[37] (referred to herein as "GFM functional tests") using accurate and detailed electromagnetic transient (EMT) models provided and certified directly from the OEM is necessary, in addition to attestations and detailed descriptions of the control modes from the OEMs.

Model Quality Fundamentals

The most important prerequisite to model-based performance verification is establishing confidence in the model quality. Ensuring an accurate and verified model is a fundamental pre-requisite to conducting any reliability studies using the models, and clear model quality requirements and checks should be established by TPs and PCs in all instances. As with all model representations of actual facilities, the following fundamental aspects of modeling and verification are needed before GFM-specific testing is conducted:

- OEM-provided validated models and validation test reports against lab or field test, or hardware-in-the-loop test of the product to be used in this project. This model validation test may include a generic representation of the overall facility but must include the actual control and converter level protection of the product that will be installed in the project. The following validation tests are recommended at a minimum:[38]
  - Balanced and unbalanced faults
  - Grid voltage disturbance – step change in magnitude and phase
  - Grid frequency disturbance – step change in frequency and frequency ramp at slow and fast ROCOF
  - Active and reactive power dispatch command step change
  - Loss of the last synchronous generator[39]
  - Load rejection
- Attestation from the inverter OEM(s) that the model provided matches the expected as-built configuration and settings to the degree known at the time of model submission.[40]
- Attestation from the plant-level controller(s) OEM(s) that the model provided matches the expected as-built configuration and settings to the degree known at the time of model submission.
- Model quality checks conducted by the TP/PC to ensure appropriate representation and parameterization of the model provided by the GO/developer.
- Model documentation is provided that describes the functionality and operation of the resource being deployed and model used.
- The model meets the quality criteria outlined in the NERC EMT Reliability Guideline[41]

---

[37] One of the best mechanisms to gain confidence in simulation models is to compare them against real event data. Currently availability of this type of data is limited for GFM installations, but as more are obtained in the coming years it will be beneficial to review this performance and integrate the learning into future GFM guides.

[38] Refer to IEEE 2800.2 once published for additional benchmarking test that could supplement or augment those listed.

[39] For model validation using hardware testing, OEMs may choose to leverage tests similar to those outlined in "Verification Test for GFM Functionality" section.

[40] The final tuning parameters/setting of the project should be accompanied with the provided model parameters/settings update to GO/TO.

[41] https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Reliability_Guideline-EMT_Modeling_and_Simulations.pdf

Description of GFM Functional Test System

The GFM functional test system (see **Figure 2.1**) consists of the following components connected to a single bus without any impedance:

- A synchronous generator with a simple excitation system model (e.g., SCRX) and turbine-governor model (e.g., TGOV1), with circuit breaker[42]
- A load[43] with both active and reactive power (inductive) components, with a maximum power factor of 0.9
- The GFM BESS plant model under test
- A duplicate of the GFM BESS plant model, rated at or near half (MVA and MW) of the model under test [44]

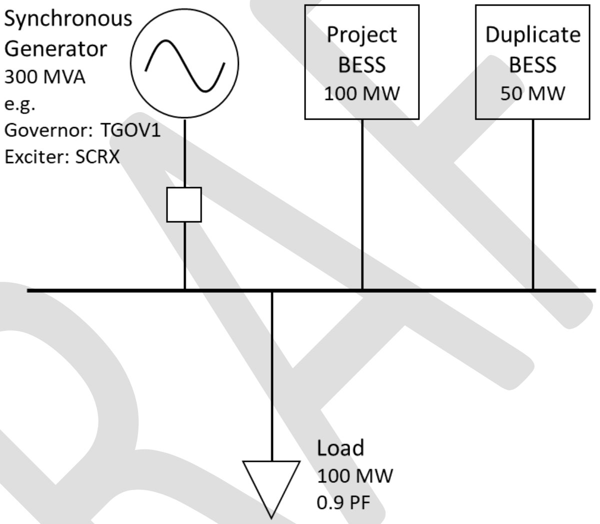


Figure 2.1: GFM Functional Test System[45]

The combined MVA rating of the BESS models must be sufficient to fully supply the load upon disconnection of the synchronous generator. The synchronous generator MVA rating must be sufficient to simultaneously serve the load and charge both BESS at their rated maximum charge power. Both BESS models should be in voltage control mode with the same voltage and frequency droop settings and set points. All protection settings in the BESS should reflect the equipment planned to be installed in the field; however, settings should be set as wide as possible within the equipment ratings and capabilities (as recommended in NERC reliability guidelines)[46] since the tests are intended to subject the GFM BESS to extreme frequency, voltage, and phase jump events.

Description of GFM Functional Tests and Success Criteria

Using simulated disturbances that only a GFM BESS meeting the functional specifications could survive, the following suite of GFM functional tests are designed to ensure that each proposed project meets the GFM BESS functional specifications as described in this document.[47] [48]

---

[42] For simulating the loss of the synchronous generator

[43] Constant impedance load model is used in the example tests described later in this chapter

[44] The purpose of adding the duplicate BESS is to consider control interaction between multiple GFM devices, including droop response and to provide flexibility in post event power balancing.

[45] BESS ratings and synchronous generator ratings are for example only.

[46] https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Reliability_Guideline-EMT_Modeling_and_Simulations.pdf

[47] TP/PC may require additional tests such as load rejection, faults, etc.

48 For example: Hawaiian Electric Facility Technical Model Requirements and Review Process, August 2022: https://www.hawaiianelectric.com/documents/clean_energy_hawaii/selling_power_to_the_utility/competitive_bidding/20210901_cbre_rfp/20210825_redline_lanai_appxb_att3.pdf

- **Test 1 – BESSs Initially Discharging and Ends at Higher Level of Discharging:** This test assesses the GFM BESS performance following the generator trip when operating within its limits and in discharging state.
- **Test 2 – BESS Initially Charging and Ends Discharging:** This test assesses the GFM BESS performance when operating within its limits and transitioning from charging state to discharging state after the generator trips.
- **Test 3 – BESS GFM Performance at Maximum Active Power:** This test assesses the GFM BESS performance following the generator trip when operating at or near its limits.

Each test is conducted using different initial operating conditions, as outlined in Table 2.1–Table 2.3. Once the system is stable at the given power flow conditions (without oscillations), the synchronous generator is disconnected. Each test then includes a set of pass/fail success criteria that *all* must be met. TPs/PCs should add additional qualitative or quantitative criteria specific to their own systems, as applicable. GFM BESS under test must pass all three tests to qualify as GFM. [49]

Although the tests require the BESS to be operated in the absence of any synchronous generation, many GFM BESS will never be operated that way. Regardless, the ability to survive such tests indicates that the controls have the necessary properties from GFM in grid-connected conditions. Conversely, if the resource is unable to meet the performance requirements in these tests, the controls will not have the desired characteristics for future BPS operating conditions.

These tests do not guarantee that the facility will be stable for a specific location on the grid. Interconnection studies are critical for ensuring reliable operation of the BPS for each specific interconnecting resource.[50] If settings change during interconnection studies, the model with the new settings should still pass these tests.

Test 1: BESSs Initially Discharging and Ends at Higher Level of Discharging

Table 2.1: Test 1 – Setup and Success Criteria	
Initial Dispatch	
• The project BESS is dispatched at 20% of its maximum discharge power limit. • The duplicate BESS is dispatched at 20% of its maximum discharge power limit	
Test Sequence:	
1. Run until the system is stable at the given power flow conditions, without oscillations. 2. Trip the synchronous generator.	
Success Criteria	
Pre-Trip:	**Pass/Fail**
a. BESSs active power outputs match dispatched levels.	
b. Synchronous generator active power output matches the rest of the load.	
c. Frequency should be 1 pu.	
d. Voltage at Bus 1 should be within 5% of nominal.	
e. Phase voltage and current waveform should not be distorted.	
f. There should not be oscillations in the RMS quantities.	

---

[49] GFL BESS can potentially form an island with load under very specific power flow and resonance conditions. Hence, it's important to subject the project model to all three tests.

[50] Other tests such as ride-through capability, voltage control, etc. are necessary to be conducted for all resources, including GFM and GFL.

Table 2.1: Test 1 – Setup and Success Criteria	
g. Reactive power output from all devices should be within limits.	
Post-Trip:	**Pass/Fail**
a. Immediately following the trip, BESS output should be well controlled. System frequency and voltage should not oscillate excessively or deviate from steady state levels for any significant amount of time.	
b. Voltage settles to a stable and acceptable operating point.	
c. The final voltage is as expected based on the droop and deadband settings.	
d. Frequency settles to a stable operating point.	
e. The final frequency is as expected based on the droop and deadband settings.	
f. Any oscillation shall be settled.	
g. Any distortion observed in phase quantities should dissipate over time.	
h. Active power from each BESS should move immediately to meet the load requirement and settle according to its frequency droop setting.	
i. Reactive power from each BESS should move immediately and settle according to its voltage droop setting.	

Test 2: BESS initially charging and ends up discharging

Table 2.2: Test 2 – Setup and Success Criteria	
Initial Dispatch	
- The project BESS is dispatched at half of its maximum charge power limit. - The duplicate BESS is dispatched at half of its maximum charge power limit.	
Test Sequence:	
1. Run until the system is stable at the given power flow conditions, without oscillations. 2. Trip the synchronous generator.	
Success Criteria	
Pre-Trip:	**Pass/Fail**
a. BESSs active power outputs match dispatched levels.	
b. Synchronous generator active power output matches the load and BESS charging.	
c. Frequency should be 1 pu.	
d. Voltage at Bus 1 should be within 5% of nominal.	
e. Phase voltage and current waveform should not be distorted.	
f. There should not be oscillations in the RMS quantities.	
g. Reactive power output from all devices should be within limits.	
Post-Trip:	**Pass/Fail**
a. Immediately following the trip, BESS output should be well controlled. System frequency and voltage should not oscillate excessively or deviate from steady state levels for any significant amount of time.	
b. Voltage settles to a stable operating point	
c. The final voltage is as expected based on the droop and deadband settings.	
d. Frequency settles to a stable operating point	
e. The final frequency is as expected based on the droop and deadband settings.	
f. Any oscillation shall be settled.	
g. Any distortion observed in phase quantities should dissipate over time.	
h. Active power from each BESS should move immediately to meet the load requirement and settle according to its frequency droop setting.	
i. Reactive power from each BESS should move immediately and settle according to its voltage droop setting.	

Test 3: BESS GFM Performance at Maximum Active Power

Table 2.3: Test 3 – Setup and Success Criteria	
Initial Dispatch	
• The project BESS is dispatched at 0 MW. • The duplicate BESS is dispatched at its steady state maximum discharge power limit.	
Test Sequence:	
1. Run until the system is stable at the given power flow conditions, without oscillations. 2. Trip the synchronous generator (no fault).	
Success Criteria	
Pre-Trip:	**Pass/Fail**
a. BESSs active power outputs match dispatched levels.	
b. Synchronous generator active power output matches the rest of the load.	
c. Frequency should be 1 pu.	
d. Voltage at Bus 1 should be within 5% of nominal.	
e. Phase voltage and current waveform should not be distorted.	
f. There should not be oscillations in the RMS quantities.	
g. Reactive power output from all devices should be within limits.	
Post-Trip:	**Pass/Fail**
a. Immediately following the trip, BESS output should be well controlled. System frequency and voltage should not oscillate excessively or deviate from steady state levels for any significant amount of time.	
b. Voltage settles to a stable operating point	
c. The final voltage is as expected based on the droop and deadband settings.	
d. Frequency settles to a stable operating point	
e. The final frequency is as expected based on the droop and deadband settings.	
f. Any oscillation shall be settled.	
g. Any distortion observed in phase quantities should dissipate over time.	
h. Active power from BESS 1 should move immediately to meet the load requirement and settle according to its frequency droop setting. Active power from BESS 2 should not exceed its max discharge power limit at steady state.[51]	
i. Reactive power from each BESS should move immediately and settle according to its voltage droop setting.	

Example Conducting GFM Functional Tests

To illustrate conducting the GFM functional tests, an OEM-provided GFM model, including a power plant controller model, was subjected to each test outlined above. **Appendix B** provides additional examples of the GFM functional

---

[51] BESS 2 output may exceed momentarily depending on the active power availability at the inverters.

tests applied to a GFM model supplied by a different OEM. **Table 2.4** shows the BESS voltage and frequency droop settings used for these tests.

Table 2.4: BESS Voltage and Frequency Droop Settings for Example Tests

Parameter	Value
Voltage Droop	2% (on Qmax)
Frequency Droop	2% (on Pmax)
Frequency Deadband	0.03 Hz

Test 1: BESSs Initially Discharging and Ends at Higher Level of Discharging

The test system is initialized with power flow conditions shown in **Figure 2.2**. BESSs are discharging at a quarter of their maximum discharge site limit, with the synchronous generator servicing the rest of the load.

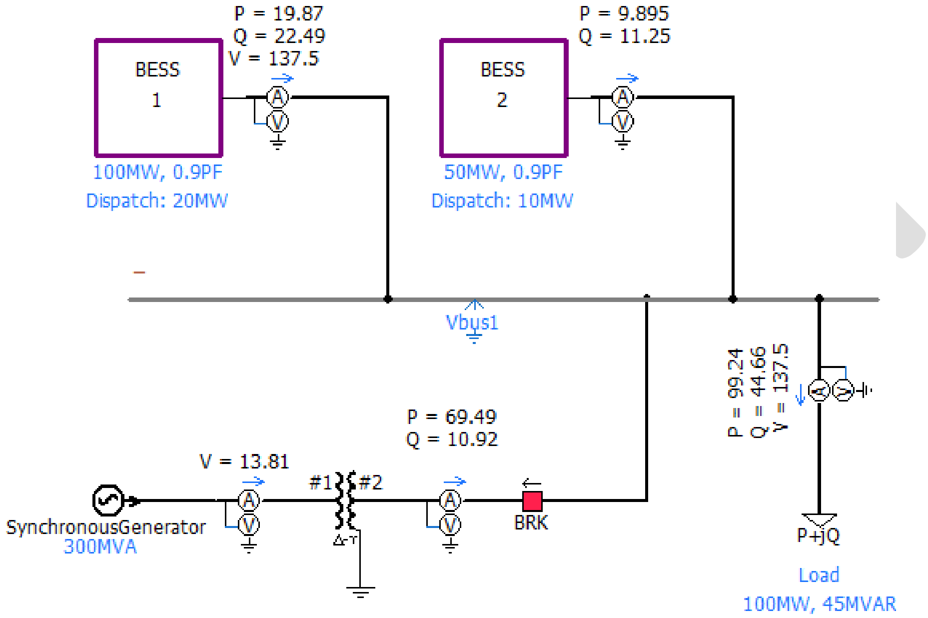


Figure 2.2: Example Test 1 – Initial Power Flow

Figure 2.3 shows the RMS quantities of the Test 1 simulation results including bus voltage (Vbus1_rms), frequency, active power (synchronous generator power (P_SyncGen), load power (P_Load), project BESS (BESS 1) power (P_BESS_1) and duplicate BESS (BESS 2) power (P_BESS_2)), reactive power, and current. The following observations are made:

- Near-instantaneous jump in active and reactive power from both BESS (see Point 1), followed by dynamics driven by specific GFM control topology and parameters.
- Minimal deviation in voltage thus resulting in small change in voltage-dependent load power (see Point 2)
- Final steady-state quantities (see Point 3 for values indicated by O-marker at *t = 40 sec* in **Figure 2.3**) can be verified against the droop parameters in **Table 2.4**.

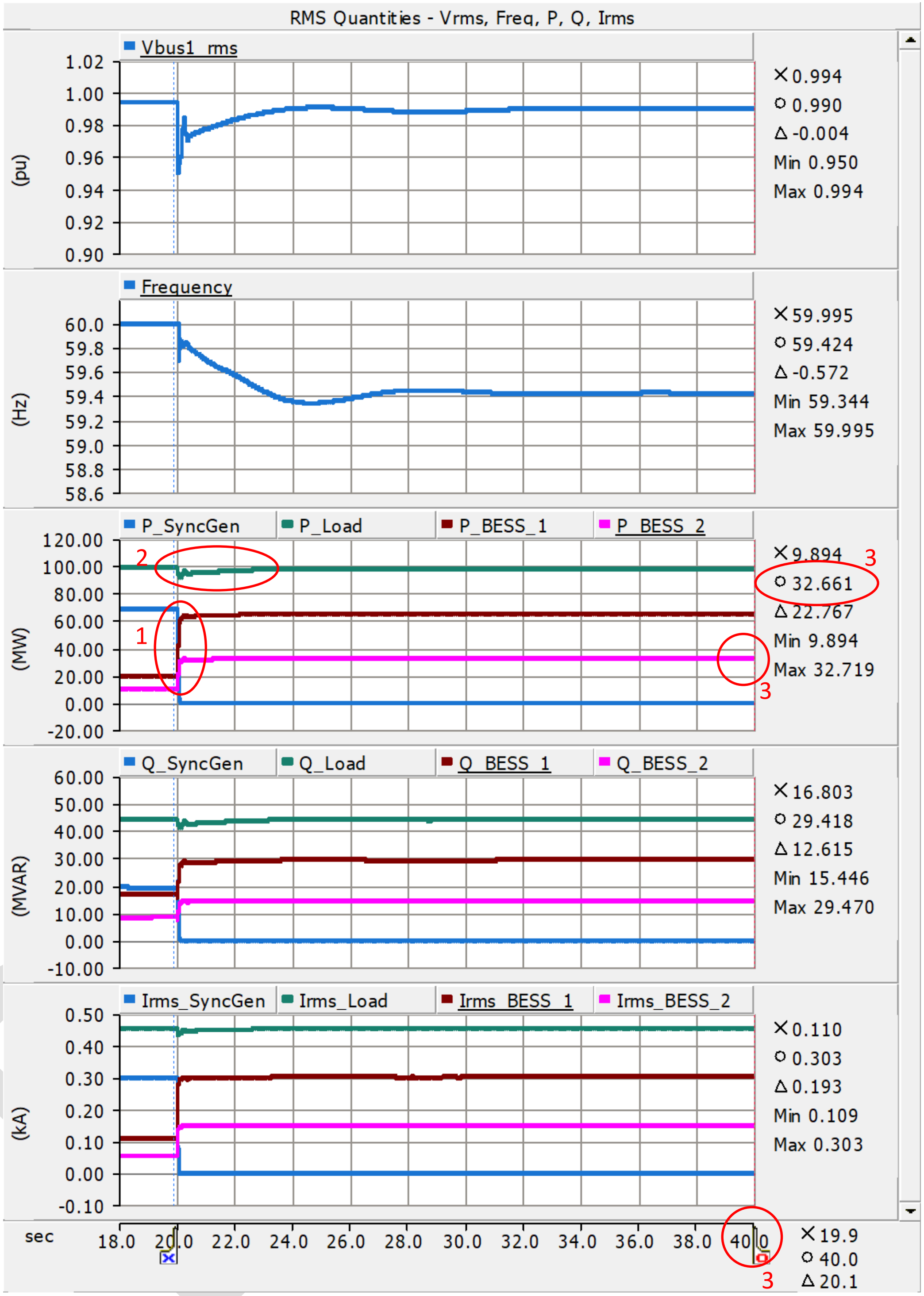


Figure 2.3: Test 1 Results – RMS Quantities

Figure 2.4 shows the instantaneous quantities of the Test 1 simulation results including bus voltage (Vbus1), synchronous generator current (I_SyncGen), load current (I_Load), BESS 1 current (I_BESS_1) and BESS 2 current (I_BESS_2), with the following observations made:

- Phase angle shift in bus voltage (see Point 1)
- Sub-cycle increase in BESS currents (see Point 2)
- Sub-cycle change in BESS current phase angle; this is more observable in the Test 2 results

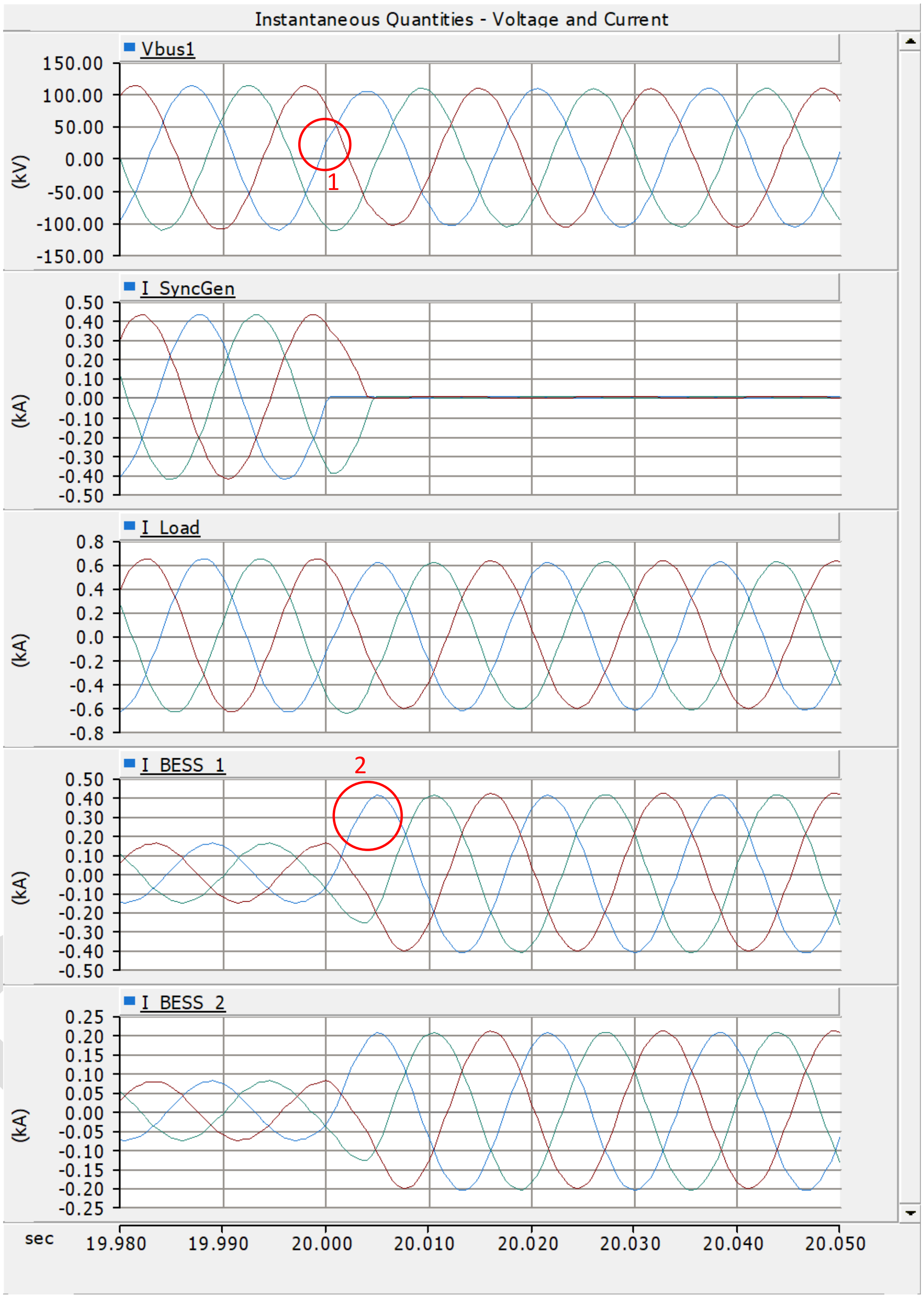


Figure 2.4: Test 1 Results – Instantaneous Quantities

As summarized in **Table 2.5**, the model passed Test 1.

Table 2.5: Evaluation of Test 1 Results

Pre-Trip:	**Pass/Fail**
a. BESSs active power outputs match dispatched levels.	Pass
b. Synchronous generator active power output matches the rest of the load.	Pass
c. Frequency should be 1 pu.	Pass
d. Voltage at Bus 1 should be within 5% of nominal.	Pass
e. Phase voltage and current waveform should not be distorted.	Pass
f. There should not be oscillations in the RMS quantities.	Pass
g. Reactive power output from all devices should be within limits.	Pass
Post-Trip:	**Pass/Fail**
a. Immediately following the trip, BESS output should be well controlled. System frequency and voltage should not oscillate excessively or deviate from steady state levels for any significant amount of time.	Pass
b. Voltage settles to a stable operating point	Pass
c. The final voltage is as expected based on the droop and deadband settings.	Pass
d. Frequency settles to a stable operating point	Pass
c. The final frequency is as expected based on the droop and deadband settings.	Pass
f. Any oscillation shall be settled.	Pass
g. Any distortion observed in phase quantities should dissipate over time.	Pass
h. Active power from each BESS should immediately move to meet the load requirement and settle according to its frequency droop setting	Pass
i. Reactive power from each BESS should move according to its voltage droop setting.	Pass

Test 2: BESS Initially Charging and Ends Discharging

The test system is initialized with power flow conditions shown in **Figure 2.5**. BESS are initially charging at half of their maximum charge rating, with the synchronous generator supplying power to the load and both BESS.

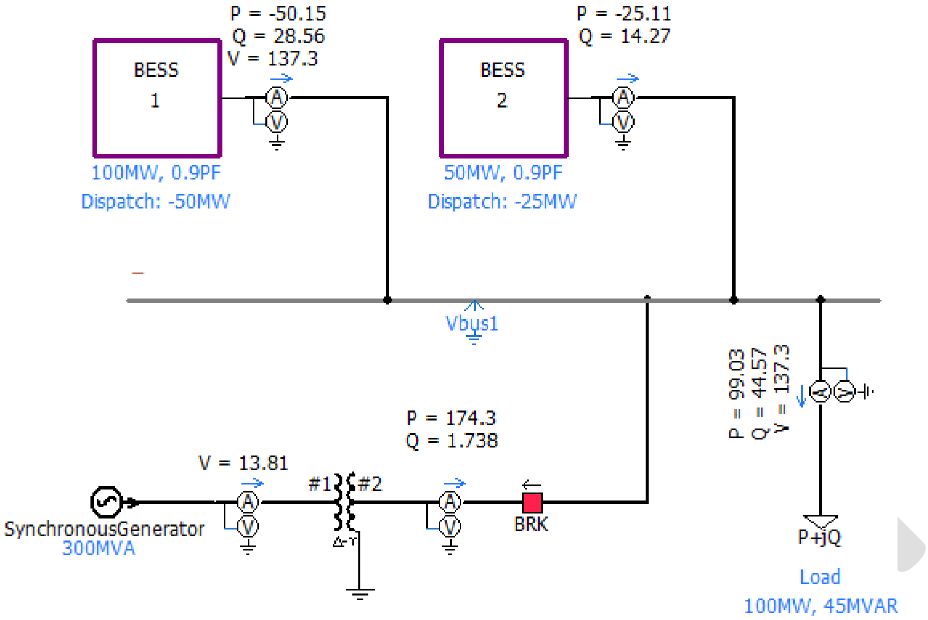


Figure 2.5: Example Test 2 – Initial Power Flow

In addition to similar observations as those from Test 1, the following can be noted in **Figure 2.6** which shows the RMS quantities of the Test 2 simulation results.

- Due to the larger differences between initial output power level and final settled output power level, driven by load, the frequency settled to a greater deviation according to the frequency droop setting[52].
- Frequency spike (see Point 1) is an artifact of frequency measurement algorithm in response to the shift in voltage phase angle (see Point 1 in **Figure 2.7**).

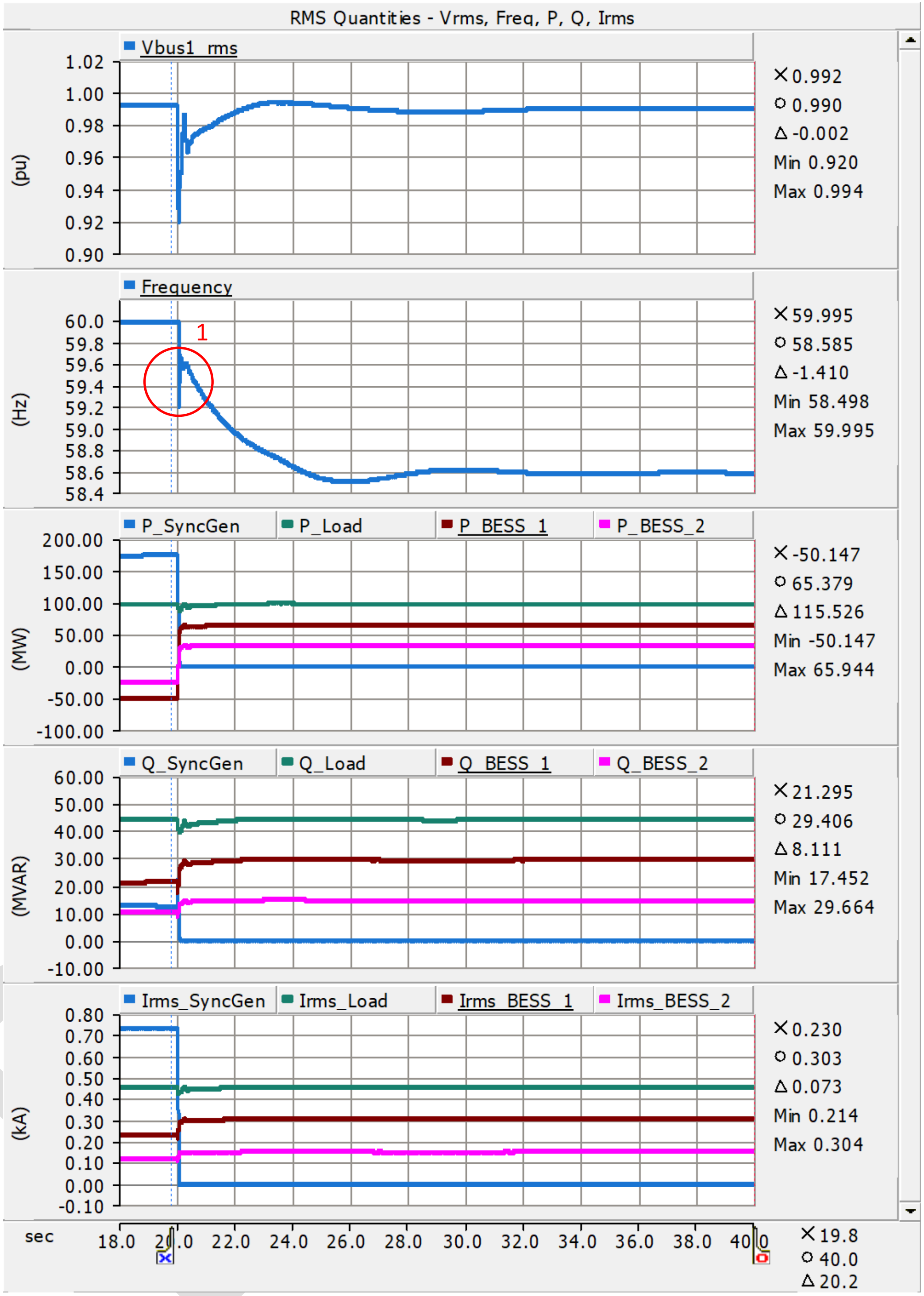


Figure 2.6: Test 2 Results – RMS Quantities

Figure 2.7 shows the instantaneous quantities of the Test 2 simulation results, with the following observations made:

- Current from both GFM BESS's increased within a quarter-cycle to make up for the loss of synchronous generator current (see Point 2)
- Change in BESS current phase angle as BESS's transition from charging to discharging within a quarter-cycle to serve the load (see Point 3)

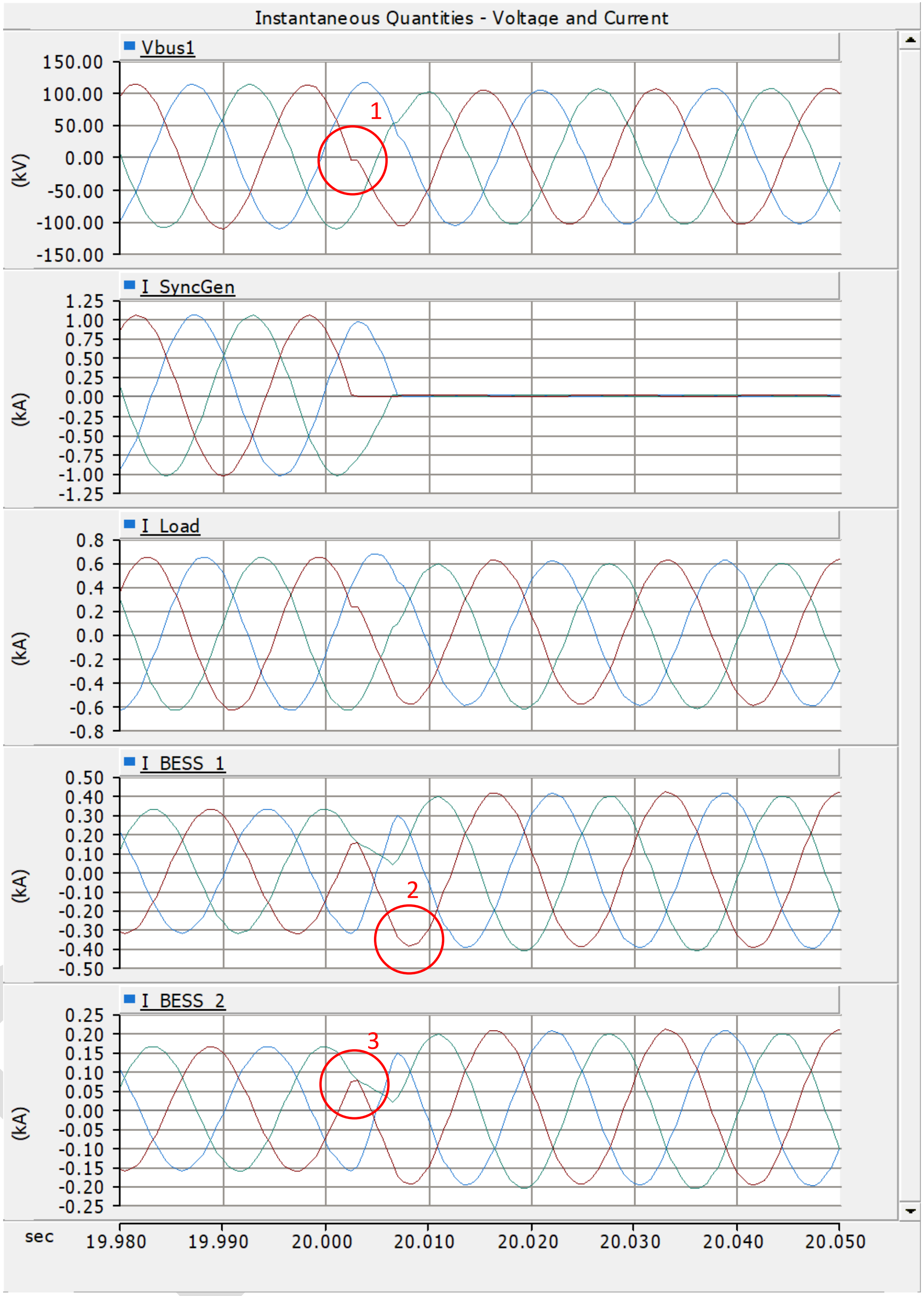


Figure 2.7: Test 2 Results – Instantaneous Quantities

As summarized below in **Table 2.6**, the model also passed Test 2.

Table 2.6: Evaluation of Test 2 Results

Pre-Trip:	**Pass/Fail**
a. BESSs active power outputs match dispatched levels.	Pass
b. Synchronous generator active power output matches the rest of the load.	Pass
c. Frequency should be 1 pu.	Pass
d. Voltage at Bus 1 should be within 5% of nominal.	Pass
e. Phase voltage and current waveform should not be distorted.	Pass
f. There should not be oscillations in the RMS quantities.	Pass
g. Reactive power output from all devices should be within limits.	Pass
Post-Trip:	**Pass/Fail**
a. Immediately following the trip, BESS output should be well controlled. System frequency and voltage should not oscillate excessively or deviate from steady state levels for any significant amount of time.	Pass
b. Voltage settles to a stable operating point.	Pass
c. The final voltage is as expected based on the droop and deadband settings.	Pass
d. Frequency settles to a stable operating point.	Pass
e. The final frequency is as expected based on the droop and deadband settings.	Pass
f. Any oscillation shall be settled.	Pass
g. Any distortion observed in phase quantities should dissipate over time.	Pass
h. Active power from each BESS should move immediately to meet the load requirement and settle according to its frequency droop setting.	Pass
i. Reactive power from each BESS should move immediately and settle according to its voltage droop setting.	Pass

Test 3: BESS GFM Performance at Maximum Active Power

The test system is initialized with power flow conditions shown in **Figure 2.8**. BESS 1 is dispatched to zero active power and BESS 2 is dispatched to its steady state maximum discharge site active power limit. The synchronous generator serves the remainder of the load.

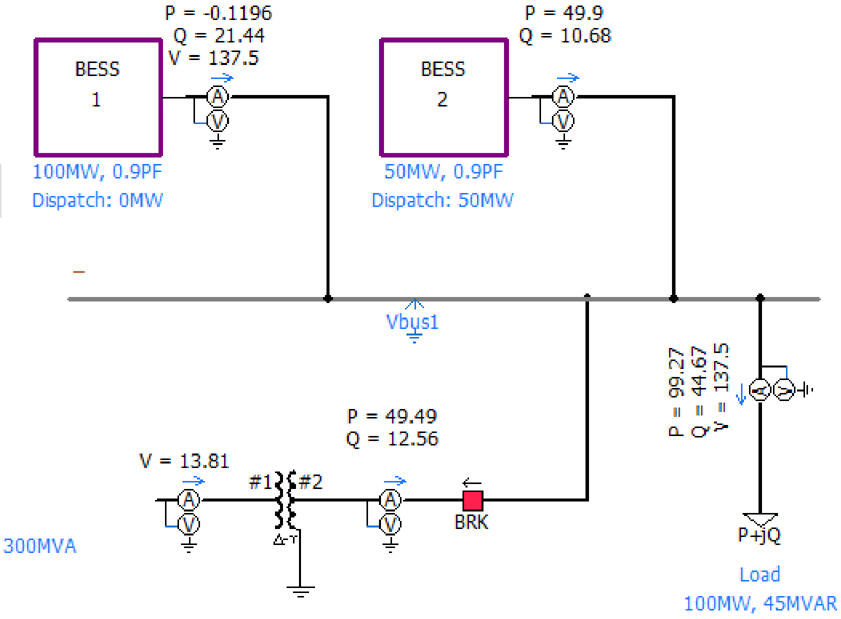


Figure 2.8: Example Test 3 - Initial Power Flow

Figure 2.9 shows the Test 3 simulation results with the following observations made that are unique to this test:

- BESS 2 (discharging at maximum active power) will not follow the droop curve past its maximum discharge power limit (see Point 1). BESS 1 makes up the active power difference to meet load demand, reaching the final frequency based on droop and deadband settings.[53]

---

[53] BESS 2 has extra power capability at the inverter level, allowing it to momentarily exceed site power limit.

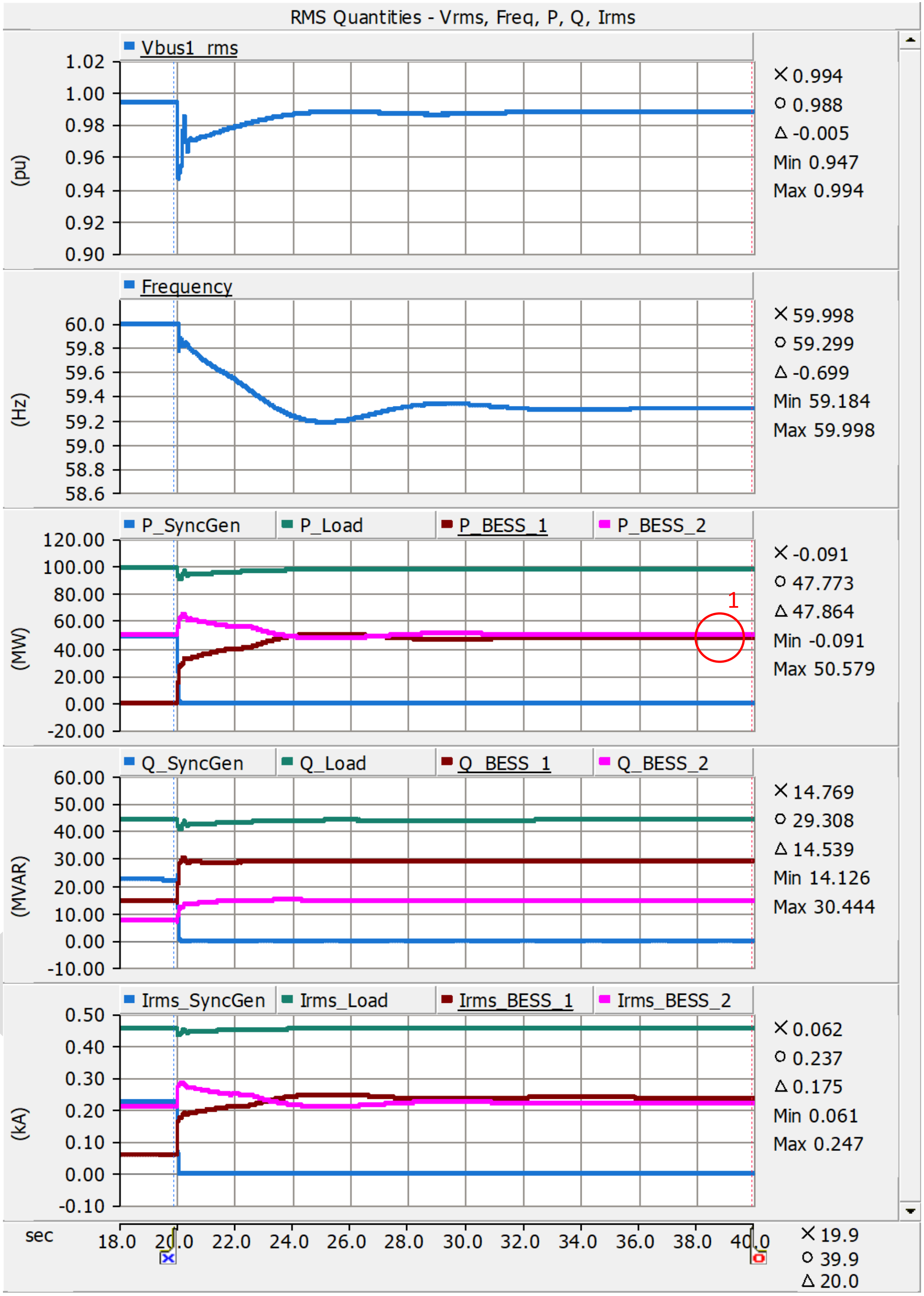


Figure 2.9: Test 3 Results – RMS Quantities

Figure 2.10 shows the instantaneous quantities of the Test 3 simulation results. Similar to the previous tests, it shows GFM BESS currents changed within a quarter cycle to match the load current (see Point 1).

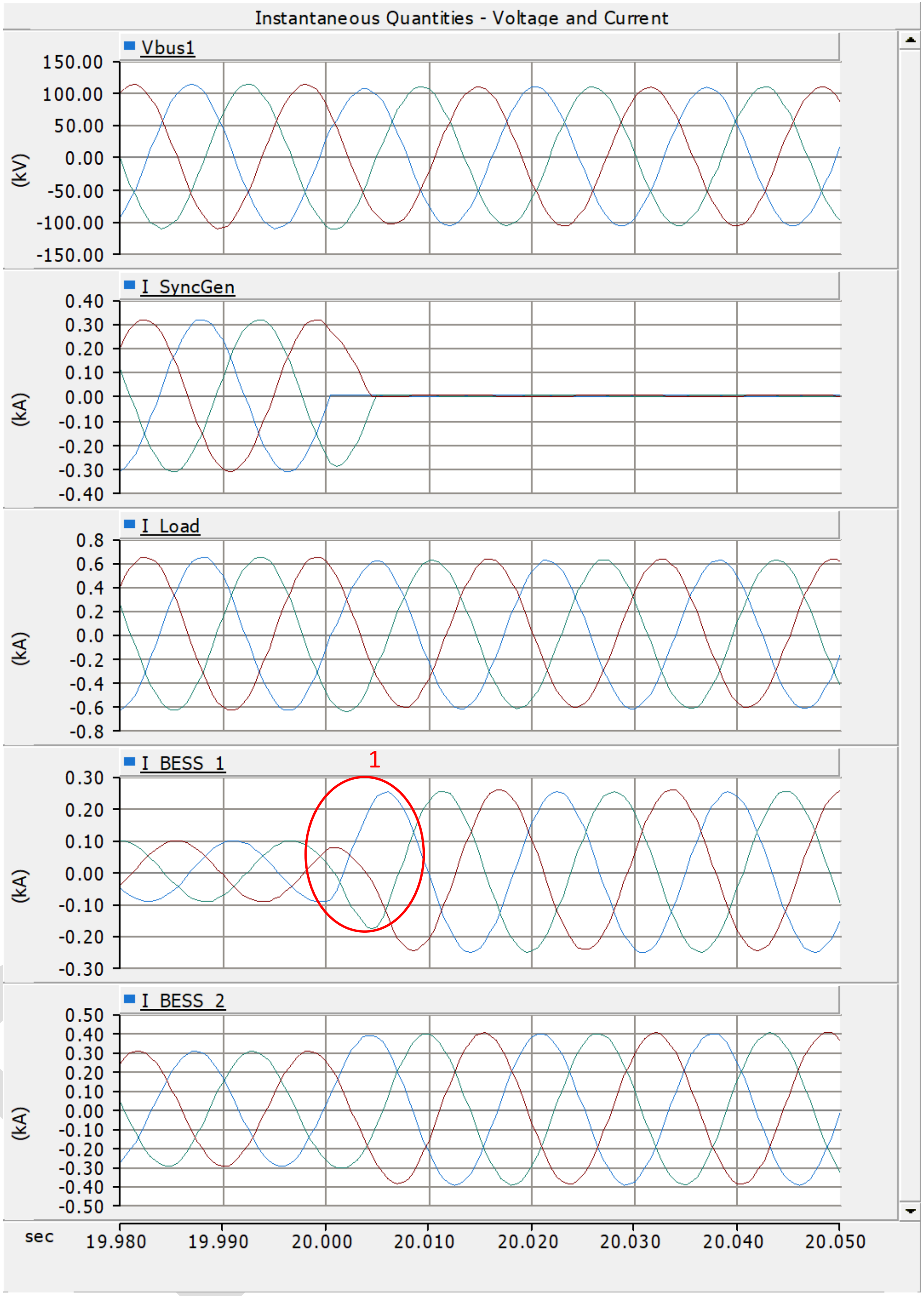


Figure 2.10: Test 3 Results – Instantaneous Quantities

As summarized below in **Table 2.7**, the model also passed Test 3.

Table 2.7: Evaluation of Test 3 Results

Pre-Trip:	**Pass/Fail**
a. BESSs active power outputs match dispatched levels.	Pass
b. Synchronous generator active power output matches the rest of the load.	Pass
c. Frequency should be 1 pu.	Pass
d. Voltage at Bus 1 should be within 5% of nominal.	Pass
e. Phase voltage and current waveform should not be distorted.	Pass
f. There should not be oscillations in the RMS quantities.	Pass
g. Reactive power output from all devices should be within limits.	Pass
Post-Trip:	**Pass/Fail**
a. Immediately following the trip, BESS output should be well controlled. System frequency and voltage should not oscillate excessively or deviate from steady state levels for any significant amount of time.	Pass
b. Voltage settles to a stable operating point.	Pass
c. The final voltage is as expected based on the droop and deadband settings.	Pass
d. Frequency settles to a stable operating point.	Pass
e. The final frequency is as expected based on the droop and deadband settings.	Pass
f. Any oscillation shall be settled.	Pass
g. Any distortion observed in phase quantities should dissipate over time.	Pass
h. Active power from BESS 1 should move immediately to meet the load requirement and settle according to its frequency droop setting. Active power from BESS 2 should not exceed its max discharge active power limit in steady state.	Pass
i. Reactive power from each BESS should move immediately and settle according to its voltage droop setting.	Pass

Illustration of GFM versus GFL Performance in Functional Tests

To illustrate the response of a grid following BESS for comparison with GFM, the same EMT model is put through Test 1 on the same test system *without* GFM functionality enabled. Note that frequency and voltage trip settings were widened to demonstrate the unstable behavior. **Figure 2.11** shows GFL failing Test 1 criteria and resulting in instability.

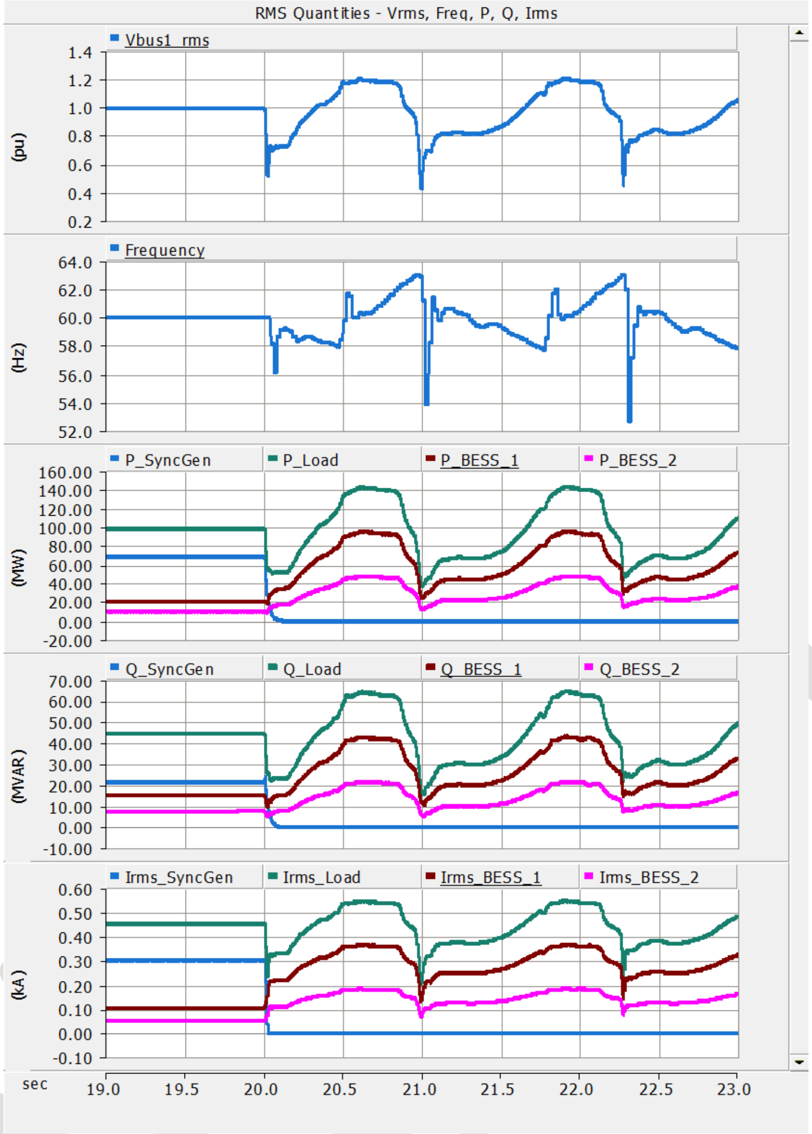


Figure 2.11: Test 1 Results with GFL

As summarized in **Table 2.8**, the BESS in GFL mode failed to settle to a steady state operating point, although the distortion in voltage and current waveforms are reasonable.

Table 2.8: Evaluation of GFL for Test 1	
Pre-Trip:	**Pass/Fail**
a. BESSs active power outputs match dispatched levels.	Pass
b. Synchronous generator active power output matches the rest of the load.	Pass
c. Frequency should be 1 pu.	Pass
d. Voltage at Bus 1 should be within 5% of nominal.	Pass
e. Phase voltage and current waveform should not be distorted.	Pass
f. There should not be oscillations in the RMS quantities.	Pass
g. Reactive power output from all devices should be within limits.	Pass
Post-Trip:	**Pass/Fail**

Table 2.8: Evaluation of GFL for Test 1

a. Immediately following the trip, BESS output should be well controlled. System frequency and voltage should not oscillate excessively or deviate from steady state levels for any significant amount of time.	Fail
b. Voltage settles to a stable operating point	Fail
c. The final voltage is as expected based on the droop and deadband settings.	Fail
d. Frequency settles to a stable operating point	Fail
c. The final voltage is as expected based on the droop and deadband settings.	Fail
f. Any oscillation shall be settled.	Fail
g. Any distortion observed in phase quantities should dissipate over time.	Pass
h. Active power from each BESS should move immediately to meet the load requirement and settle according to its frequency droop setting.	Fail
i. Reactive power from each BESS should move immediately and settle according to its voltage droop setting.	Fail

Figure 2.12 and **Figure 2.13** are zoomed in versions of **Figure 2.11**to compare the GFL response (left) to GFM response (right). Notable differences include:

- Sub-cycle response in GFM current that GFL does not provide (see Point 1 in **Figure 2.12**)
- Fast active and reactive power response from GFM that GFL does not provide (see Point 2 in **Figure 2.13**)

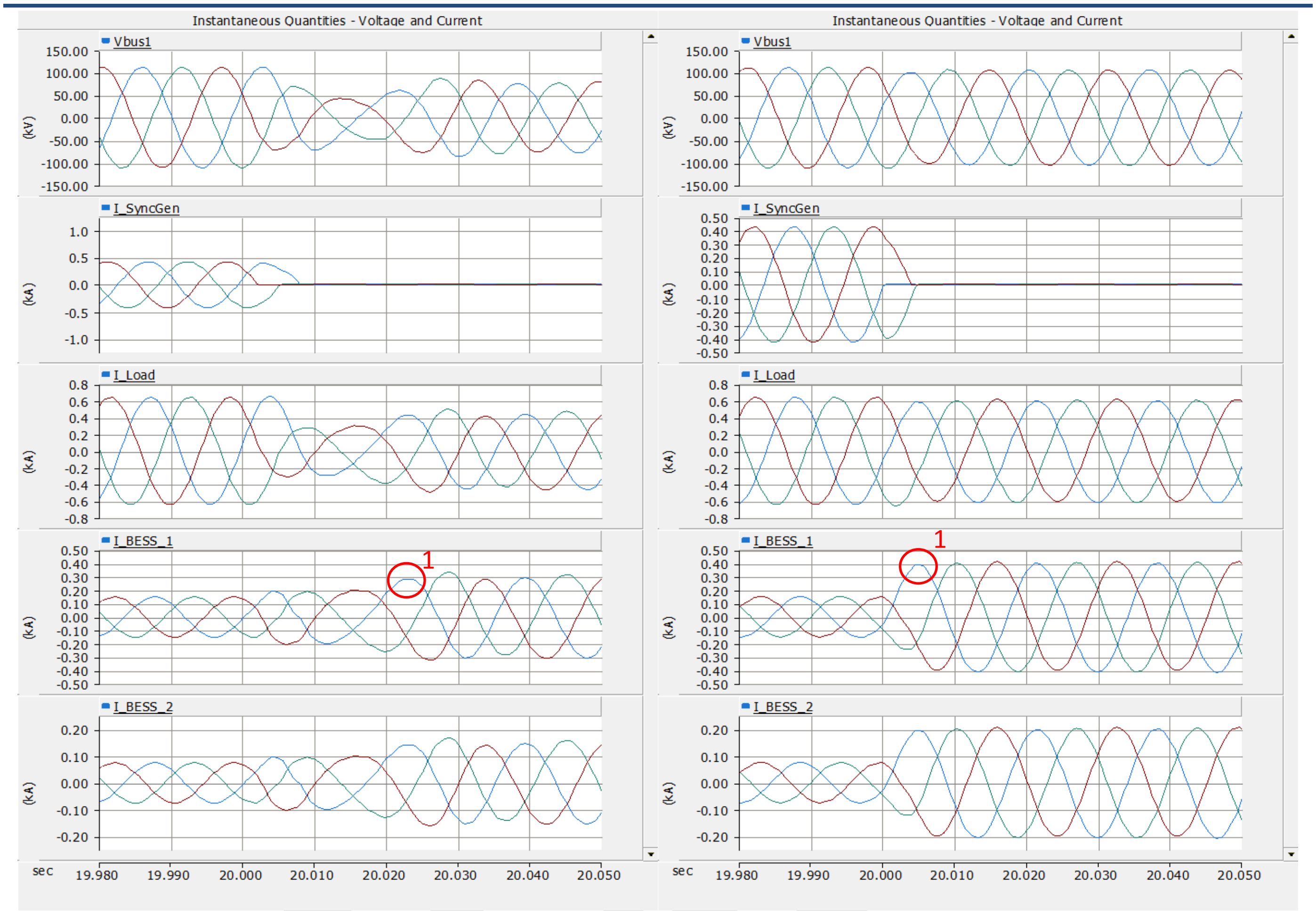


Figure 2.12: Comparison between GFL (Left) and GFM (Right) Responses – Instantaneous Quantities

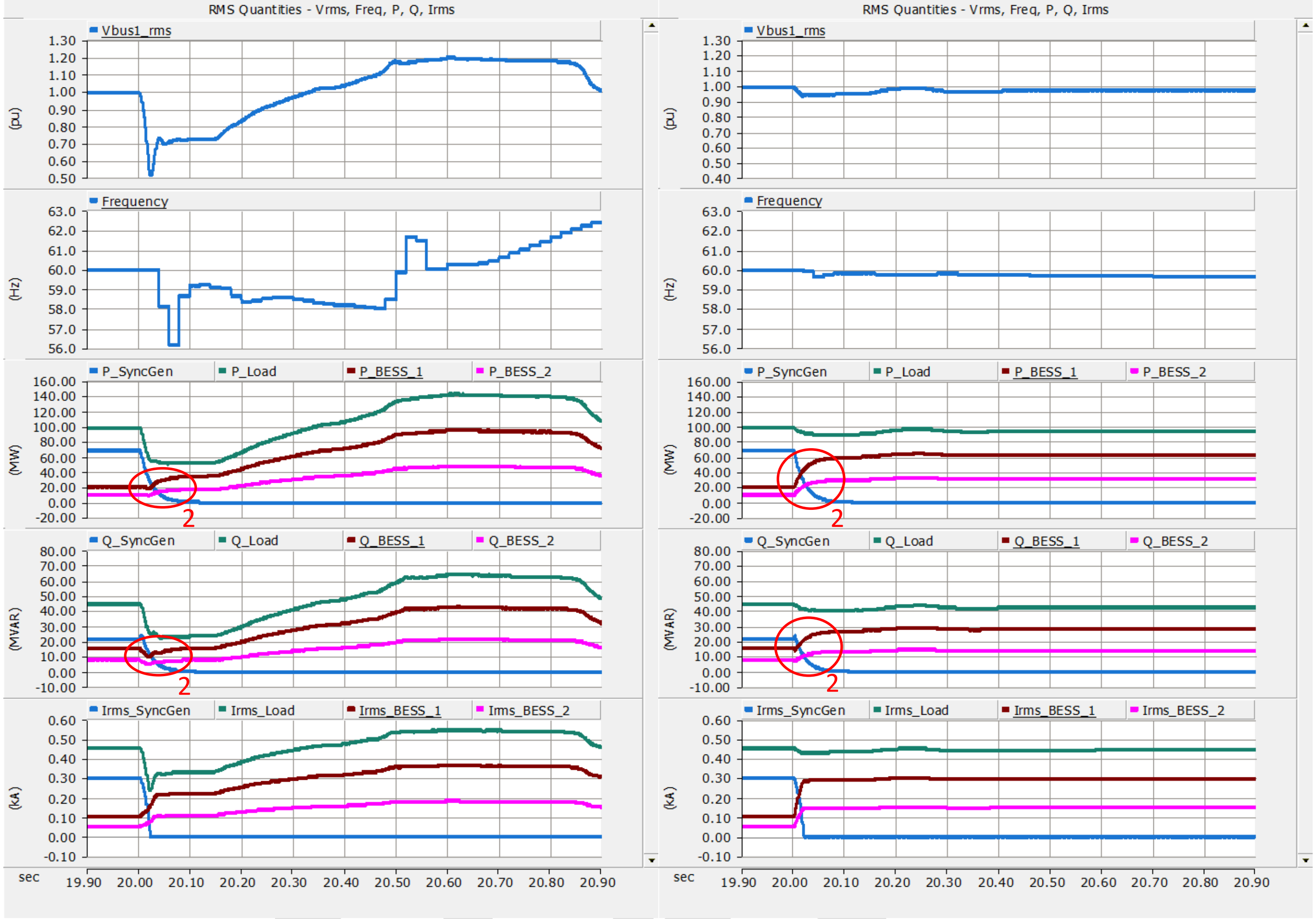


Figure 2.13: Comparison between GFL (Left) and GFM (Right) Responses – RMS Quantities

Appendix A: Industry Experience with GFM Integration

This appendix shares industry experience with integrating and operating GFM BESS technology on the BPS around the world.

Forum Network Technology/Network Operation (FNN) Guideline

The German FNN institute has published a guideline[54] on GFM behavior of HVDC systems and dc-connected power plant modules in 2020. The guideline is a supplement to VDE-AR-N-4131.[55,56] The FNN guideline describes the dynamic active power–frequency behavior and dynamic voltage control without reactive current specification. It consists of a conformity verification procedure for GFM resources, which includes methods for specifying the reference behavior, test description (networks and scenarios) as well as validation criteria. GFM resources are characterized with an immediate response and "network-stabilizing behavior" expected to counteract system events. This guideline includes tests that cover:

- Phase angle steps of 10 and 30 degrees
- Linear frequency change with 2 Hz/s ROCOF during 0.5 seconds
- Voltage magnitude step of 5% and 10% within normal operational ranges
- Grid distortion including the presence of negative sequence (2% unbalance in one phase), harmonics (including ranks 2, 5, 7, 19 and 31), and low frequency subharmonics (at 5, 10 and 15.9 Hz)
- Changes in the network impedance leading to short circuit ratio reductions from 20 to 5, from 5 to 2, and from 2 to 1
- Islanding in an active network, with only load or including another GFM converter

Conformity verification is based on time varying reference "envelopes" that can be applied to instantaneous value signals giving special attention to the initial behavior up to the first peak. These signals can be obtained from field measurements, electromagnetic transient (EMT) simulations, or hardware in the loop (HIL) simulations. Verification can include recalculated quantities to be determined over a certain time period such as active and reactive power. Conformity proof includes delivery of a technical verification report and a digital model with the installation manual and benchmark report.

Massive Integration of Power Electronic Devices (MIGRATE)

The European Union-funded MIGRATE project provides requirements for upcoming IBR-dominated power systems to maximize IBR penetration levels while maintaining stability and reliability.[57] In 2019, MIGRATE proposed high-level definition of GFM functions including:

- Behave as a voltage source
- Be synchronized with other grid forming sources
- Operate in standalone after seamless islanding
- Limit output current magnitude (preserving voltage source behavior and preferably avoiding control switches during voltage dips, for instance)
- Be compatible with all devices connected on the system, especially synchronous machines and GFL IBRs

---

[54] VDE/FNN Guideline: Grid forming behavior of HVDC systems and DC-connected Power Plant Modules, August 2020: https://shop.vde.com/en/fnn-guideline-hvdc-systems-2

[55] VDE is the Europe's largest technical scientific associations Verband der Elektrotechnik

[56] Technical Connection Rule for the connection of HVDC systems and generation plants connected via HVDC systems

[57] PowerPoint-Präsentation (h2020-migrate.eu)

Additionally, within this project a number of studies were carried out demonstrating compatibility of GFM IBRs with various control types operating in parallel in a fully IBR system.

European Network of Transmission System Operators for Electricity (ENTSO-E) Report

ENTSO-E published *High Penetration of Power Electronic Interfaced Power Sources and the Potential Contribution of Grid Forming Converters*[58] defining seven properties of a GFM inverter:

- Creates system voltage (does not rely on being provided with firm clean voltage)
- Contributes to fault level (positive and negative sequence within first cycle)
- Contributes to total system inertia (limited by energy storage capacity)
- Supports system survival to allow effective operation of low frequency demand disconnection (LFDD) for rare system separations
- Controls act to prevent adverse control system interactions
- Acts as a sink to counter harmonics and inter-harmonics in system voltage
- Acts as a sink to counter unbalance in system voltage

While the MIGRATE definition focuses on capabilities regarding standalone operation and synchronization, the ENTSO-E paper adds a response deployment dimension.

Great Britain Grid Code GC0137

Grid Code GC0137 *Minimum Specification Required for Great Britain GFM Capability*[59] was approved and published in February 2022. This grid code was applied by National Grid Electricity System Operator (NGESO) to address grid stability issues arising from increasing penetration of IBRs. Although the requirements are non-mandatory, the provider of GFM IBRs will declare how much capability is available so that these GFM IBRs could be selected and remunerated for those capabilities.[60] Successful implementation of this grid code would provide additional grid stability services by these GFM resources. To help relevant IBR stakeholders understand the GFM requirements, NGESO released the *GBGF Best Practice Guide*[61] in April 2023. GFM IBRs are expected to provide the same type of performance as synchronous generator to:

- Limit the rate of change of system frequency
- Inject instantaneous active power and instantaneous fast fault current into the grid
- Contribute to damping power
- Limit vector shift
- Contribute to synchronizing torque
- Contribute to voltage performance during a fault

GC0137 specifies the following minimum technical, design, and operational capability for GFM IBRs:

- Withstand 2 Hz/sec ROCOF over a rolling 500 ms period

---

[58] https://euagenda.eu/upload/publications/untitled-292051-ea.pdf

[59] GC0137 Authority Decision (ofgem.gov.uk)

[60] https://www.nationalgrideso.com/industry-information/codes/grid-code/code-documents

[61] https://www.nationalgrideso.com/document/278491/download

- Operate at a minimum short circuit level of zero MVA at the grid interconnection point
- Fast short circuit current injection on both magnitude (typical 1 pu or 1.5 pu at zero voltage) and response speed (start in 5 ms and full in 30 ms)
- Active power responds to changes in the grid at bandwidths below 5 Hz to avoid ac system resonance problems
- Provide damping factor between 0.2 and 5.0

UK Stability Pathfinder

While a market for GFM capability is under development, NGESO needs some of the stability services such as improved system strength and inertia in certain locations today. Currently those are being procured through a series of tenders called Stability Pathfinder.[62] Phase 1 was only open to synchronous solutions and awarded to a number of synchronous condensers. Phase 2 was open to new technologies and five GFM BESS projects[63] were awarded in April 2022 with in-service dates between March 2024 and April 2026. These projects must comply with the requirements set forth in GC0137. Stability Pathfinder tenders are an exploratory temporary solution for broader procurement of stability services from a variety of capable technologies. NGESO is currently in the process of designing a market for new stability services, which will allow to them to procure additional stability services through a market mechanism.

Optimal System Mix of Flexibility Solutions for European Electricity (OSMOSE)

EU-funded project OSMOSE Deliverable 3.3 *Analysis of Synchronization Capabilities of BESS Power Converters*[64] was released in March 2022, defining GFM minimum technical capabilities, technical requirements to formulate these capabilities, and recommendations to add these requirements into European-level and national grid codes. According to this specification, GFM units shall within its rated power and current be capable of self-synchronization, standalone operation, and provide synchronization services. The GFM capabilities shall include:

- Standalone operation
- Synchronizing active power (in response to phase-jump)
- Inertial response (immediate active power output following a frequency change)
- System strength (immediate reactive power output in response to grid voltage variation)
- Fault current (immediate current output within installation capabilities following voltage dips, active/reactive current sharing during the first instances of the fault dependent on system impedance (not control action), during asymmetrical voltage dips prioritization between positive and negative sequence current can be defined by a system operator.)

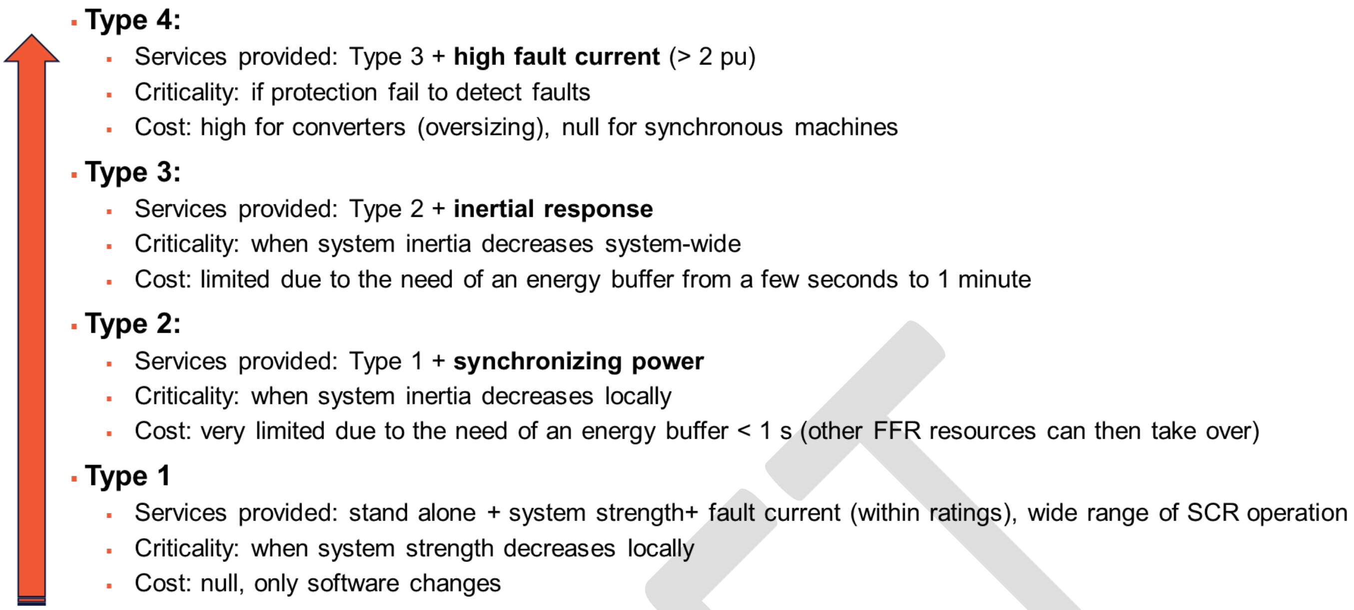
The report proposed separating GFM resources into four types based on the capabilities shown in **Figure A.1**.

---

[62] https://www.nationalgrideso.com/future-energy/projects/pathfinders/stability

[63] Stability Phase 2 Master Results Final with Tech Type.xlsx (live.com)

[64] https://www.osmose-h2020.eu/wp-content/uploads/2022/04/D3.3-Analysis-of-the-synchronisation-capabilities-of-BESS-power-converters.pdf



- **Type 4:**
  - Services provided: Type 3 + **high fault current** (> 2 pu)
  - Criticality: if protection fail to detect faults
  - Cost: high for converters (oversizing), null for synchronous machines
- **Type 3:**
  - Services provided: Type 2 + **inertial response**
  - Criticality: when system inertia decreases system-wide
  - Cost: limited due to the need of an energy buffer from a few seconds to 1 minute
- **Type 2:**
  - Services provided: Type 1 + **synchronizing power**
  - Criticality: when system inertia decreases locally
  - Cost: very limited due to the need of an energy buffer < 1 s (other FFR resources can then take over)
- **Type 1**
  - Services provided: stand alone + system strength+ fault current (within ratings), wide range of SCR operation
  - Criticality: when system strength decreases locally
  - Cost: null, only software changes

Figure A.1: Type of Grid Forming Resources as proposed by OSMOSE project[65]

A delineation is made in the report between capabilities that can only be provided by GFM resources versus capabilities that can also be provided by GFL resources (e.g., power oscillation damping, provision of negative sequence current, phase jump withstand capability, harmonics mitigation). The paper defined synchronization services and concluded that due to criticality and geographic dependence, some of these services need to be required at the time of interconnection from all new large transmission-connected IBRs and some additional services should be required from new transmission-connected BESS. It was recognized that synchronous machines may be needed in the interim to provide additional short circuit current or, alternatively, higher overcurrent capability of IBRs can be incentivized.

UNIFI Consortium

The Universal Interoperability for Grid-Forming Inverters (UNIFI) Consortium is a US Department of Energy-funded effort to advance GFM technology. The consortium developed the first version of a set of specifications that outline plant- and unit-level performance requirements for GFM technologies.[66] These specifications are intended to facilitate the integration and seamless operation of GFM resources, particularly unifying their operation smoothly with synchronous generators. The purpose of the UNIFI specifications for GFM IBRs is to provide uniform technical requirements for the interconnection, integration, and interoperability of GFM IBRs of any size in electric power systems of any scale. These specifications establish functional requirements and performance criteria for integrating GFM IBRs in power systems at any scale which includes GFM devices used as the local load, in microgrid, distribution, and transmission system. These specifications cover all GFM technologies including, but not limited to: battery storage, solar PV, wind turbines, HVDC, STATCOM, UPS, supercapacitors, fuel cells, or other yet to be invented technologies. While each GFM resource have different DC side and energy limitations, the specifications focus on the ac side performance requirements.

This UNIFI specifications cover both normal and contingency operation conditions. Under normal operation conditions, performance requirements for GFM include (but are not limited to) autonomous voltage and frequency support of the grid, active and reactive power sharing, robust operation in low system strength grid, and unbalancing

---

[65] Adapted from Carmen Cardozo's OSMOSE project presentation at 2022 ESIG GFM Workshop: https://www.esig.energy/event/2022-special-topic-workshop-grid-forming-ibrs/

[66] B. Kroposki, et. al, "UNIFI Specifications for Grid-forming Inverter-based Resources – Version 1," UNIFI Consortium, UNIFI-2022-2-1, December 2022 [Available at: https://sites.google.com/view/unifi-consortium/publications]

grid operation support of. In contingency operation conditions, performance requirements for GFM include (but are not limited to) fault ride-through behavior, response to asymmetrical faults, response to phase jumps, and intentional islanding event. The requirements are considered to be the minimum capability from GFM resources; additional capabilities such as blackstart capability and short-term over current capability are also covered in the specifications.

ESIG Grid Forming White Paper and Workshop

The Energy Systems Integration Group (ESIG) published a technical report on GFM technology in March 2022.[67] The report covered the following topics

- GFM versus GFL inverter basic principles and an overview of types of GFM controls
- How BPS needs are changing with increasing penetrations of IBRs and the trade-offs between system needs and resource needs
- System services provided by GFM and technical requirements around the world, specifically around breaking the "chicken-and-egg" problem regarding deployment of GFM and requirements/incentives
- Advanced characterization and testing of GFM resources, including field tests
- Simulation tools needs (stability, analytics, economics, etc.) and the need for compatibility
- Recommendations for GFM technology moving forward

ESIG also held a technical workshop dedicated to GFM technology in June 2022, structured around steps needed to solve the "chicken-and-egg" issue around GFM technology deployment.[68] Topics addressed system operator experience with high shares of IBRs, OEMs with commercial GFM products, research and development in this space, and the low-hanging fruit of enabling GFM in BESS to provide core GFM capabilities (excluding high overcurrent and blackstart capability). Key points highlighted that commercial offerings for GFM BESS are already available today from multiple OEMs; however, the absence of clear GFM requirements is leading to customized site-specific applications that drive higher implementation costs. It was also recommended to distinguish between equipment specification/minimum capability requirements and system needs/services.

Finland Specific Study Requirements for Grid Energy Storage System

A large number of BESS are planned to connect to the transmission grid in Finland. Studies have shown that GFL IBR are not able to operate in stable manner when the share of the IBRs is increasing in the future. The solution is to use GFM IBRs to compensate for the reduction of synchronous generation and improve external system strength required by present GFL inverters to function properly. The need for GFM control has been identified already in weak grid regions, where connection of more GFL IBRs is not possible without further grid strengthening. As a result, Fingrid defined Specific Study Requirements for BESS (30 MW, ≥110 kV) connected to the specific locations where use of GFM controls is seen as necessary. The document describes functional requirements, modeling requirements, simulation studies and field tests for GFM BESS.

According to Fingrid requirements, GFM IBR shall be able to self-synchronize, operate in stand-alone mode and provide synchronization services: synchronizing power, system strength, fault current and virtual inertial response (within current inverter rating). The requirements are in addition to existing grid code specifications for energy storage systems, in case of conflict, GFM requirements prevail.
Switching to GFL mode from GFM mode at the current limit is not permitted, when the GFM BESS is reaching the current limit, stability and grid support must still be maintained. GFM BESS shall continue providing GFM operational characteristics even at its highest and lowest allowable state of charge.

---

[67] https://www.esig.energy/grid-forming-technology-in-energy-systems-integration/

[68] https://www.esig.energy/event/2022-special-topic-workshop-grid-forming-ibrs/

GFM shall provide autonomous, near-instantaneous frequency and voltage support by maintaining a nearly constant internal voltage phasor in the sub-transient time frame, including:

- Phase jump performance: resist near-instantaneous voltage phase angle change in sub-transient time frame
- System strength: resisting the change in voltage magnitude in the sub-transient time frame
- Seamless transition between islanded operation and grid-connected operation
- Positive damping: GFM shall present a positive resistance to the grid within frequency ranges 0–47 Hz and 53-250 Hz to prevent adverse interactions.

GFM BESS shall provide a closed loop path for unbalanced current to flow, i.e. GFM shall present negative sequence current to ensure that its internally generated voltage remains balanced during normal operation and disturbances.

The specification includes additional clarifications on how existing active power/frequency control and reactive power/voltage control requirements for BESS should be interpreted for GFM BESS.

Similarly to HECO requirements, the document provides a table with the list of disturbances to be tested & acceptance criteria, simulation software and BESS operating scenarios (prescribed values of SOC, P and Q). The list also includes loss of last synchronous generator in test network model, identical to the one recommended in this document, Test 3 in Chapter 2.

In addition to software simulations, hardware type test reports are required. The document also provides the list of site tests such as for phase jump, island operation (upstream 110 kV breaker is opened), measurement of power quality, accompanied with high level acceptance criteria.

Fingrid finalized and sent the requirements to their customers in June 2023. Their requirements will be posted on Fingrid's website after summer holidays in beginning of August 2023[69].

Currently the plan is to require GFM capabilities from BESS that interconnected to the grid with high penetration of IBRs. Fingrid plans to gather more experience from the current GFM projects and aims to make it a general requirement for all BESS projects next year.

AEMO GFM Voluntary Specification

AEMO published Voluntary Specification for Grid-forming Inverters in May 2023[70]. The document provides guidance to stakeholders while the regulatory environment around GFM technology develops. The definition of GFM IBR provided by AEMO is similar to that from NERC.

Similarly to UNIFI, it specifies the 'core' GFM capabilities, which require only a small energy buffer and can be delivered through control changes and 'additional' GFM technical capabilities that require a large energy buffer through hardware or operational practices change as well as over current capably. It is recognized that not all GFM inverters need to provide 'additional' capabilities, but these capabilities are valuable for secure operation of a power system with high share of IBRs.

The core requirements include:

- Nearly-instantaneous (< 5 ms) reactive response to an external voltage magnitude step, to oppose the change in grid voltage.
- Nearly-instantaneous active power response to a voltage phase angle step, by injecting or absorbing power to oppose the change in phase angle.

---

[69] https://www.fingrid.fi/en/grid/grid-connection-agreement-phases/grid-code-specifications/grid-energy-storage-systems/

[70] https://aemo.com.au/-/media/files/initiatives/primary-frequency-response/2023/gfm-voluntary-spec.pdf?la=en&hash=F8D999025BBC565E86F3B0E19E40A08E

- Inertial response from GFM inverters should be inherent (no calculation of frequency), providing a near-instantaneous active power response to a grid disturbance (e.g. load or generation trip). If the inertia is configurable, it needs to be tuned based on network conditions and requirements (high inertia constant may increase risk of power oscillations, particularly in strong systems).
- The response when the inverter is at a limit, and in transition to and from a limit condition, must be smooth and stable.
- The behavior at a limit should not be detrimental to stability and to harmonic performance (for example, clipping of current waveforms).
- Surviving Loss of Last Synchronous Machine (SM): operate stably in a grid without any other GFM inverters or SMs; remain stable for a transition from a grid with SMs to one without (and back); provide frequency and reactive support, unaffected by these transitions. All of that, provided that the resultant state of the system is within the operating envelope of the GFM inverter.
- Operate stably under a very low short circuit ratio, as defined by the system operator; provide system strength support to nearby GFL inverters during and after disturbances.
- Provide positive damping for oscillations: following a disturbance GFM inverter output should be adequately damped; add damping to the system for the oscillatory phenomena listed in the document.

‘Additional’ capabilities include higher current capability above the continuous rating, larger headroom and energy buffer and power quality improvements.

AEMO is currently working on the development of a test plan and metrics for each of the qualitative capabilities to quantify requirements and to demonstrate that a device meets the specifications, to be published in 2024. The next step will be development of methodology to account for contributions from GFM devices in planning studies (as some contributions are dependent on the operating point).

ERCOT Assessment of GFM Energy Storage Resources

Recent notable events in ERCOT (Odessa 1 in 2021 and Odessa 2 in 2022) have shown the need to strengthen the system and resilience necessary to mitigate the reliability risk. ERCOT continues to focus on improving IBRs’ capability and performance combined with improvements on the transmission system, recognizing that both are needed to maintain the reliable operations of the ERCOT grid. Therefore, alongside the adoption of NERC reliability guidelines, IEEE 2800 ride-through requirements and recent recommendation for six new synchronous condensers to strengthen West Texas grid, additional improvements will be needed to support the continued growth of IBRs in the ERCOT grid.

Increasing industry interest in GFM controls for improvement of IBR performance and system support have prompted ERCOT to evaluate the potential application of GFM Energy Storage Resources (ESR)[71] in ERCOT grid. The results were presented at the ERCOT Inverter-Based Resource Working Group[72] on 8/11/2023.
ERCOT preliminary GFM ESR evaluation focused on three scenarios:

- Scenario 1: a weak grid condition, a simple test case that mimics known stability challenges in ERCOT (in phasor domain)
- Scenario 2: West Texas grid based on 2022 Q4 Quarterly Stability Assessment case (in phasor domain):
  - West Texas IBRs were dispatched at 55%,

---

[71] Energy Storage Resource (ESR) is a defined term in ERCOT

[72] https://www.ercot.com/calendar/08112023-IBRWG-Meeting-_-Webex (see presentation slides under Key Documents)

    - Include 22 ESRs (existing and planned) with ~2000 MVA capacity behind West Texas Export transmission constraint, all batteries were modelled as GFL first and then as GFM
    - Include potential new condensers in six locations in West Texas.
  - Scenario 3: an actual ERCOT local area (138 kV) with identified stability constraints (tested in both phasor domain and EMT models).

Two GFM IBR dynamic models used in these tests were developed by Pacific Northwest National Laboratory (PNNL) and Electric Power Research Institute (EPRI)[73]. Both phasor domain models and EMT models from these two entities showed similar performance in the study. ERCOT's assessment results from all three scenarios indicate that GFM ESRs could be a viable option to improve system dynamic responses, but require headroom or energy buffer to provide adequate GFM support, proper control setting tuning and coordination. As the next step ERCOT will work on the GFM ESR requirements including but not limited to performance, models, studies, and verification. ERCOT expects GFM ESR to be capable of meeting IEEE 2800 and existing ERCOT requirements along with additional performance requirements specific to GFM.

GFM BESS Projects around the World

BPS-connected GFM BESS are commercially available from different OEMs and projects are quickly growing around the whole world.[74] Some of the major GFM BESS projects are summarized here.

Kauai Experience

Kauai Island Utility Cooperative (KIUC) has had the BESS portion of a 13 MW ac-coupled solar PV+BESS plant operating in GFM mode since 2018, which is a significant portion of the 70 MW system peak load. Field experience has shown the plant to operate stably during grid disturbances while providing instantaneous response to frequency and voltage events, avoiding load shedding and possible system outages.

Since April 2022, portions of a second solar PV+BESS plant on Kauai were converted to GFM mode. The second plant is a 14-MW dc-coupled solar PV+BESS plant that uses a different GFM control technique than the first plant. As of August 2022, the second plant now has all inverters in GFM mode. No adverse interactions between the two GFM plants have been observed in the field to-date.[75]

Both GFM plants have been shown to operate stably at all hours of the day, including times when the system is dominated by synchronous generation and times when it is dominated by inverter-based generation (including one other 30 MW GFL solar PV+BESS plant, three other large (6–12 MW) solar PV plants and about 45 MW of aggregate behind-the-meter solar PV). System inertia constant ranges from about 0.5 MW-s/MVA to 2.7 MW-s/MVA (using total online capacity as the MVA base), and the percent of generation from IBRs ranges from about 6% to 95%. KIUC intends to continue operating both plants in GFM mode going forward and may add additional GFM generation in the future.

No EMT model of the KIUC system was available at the time of either of the two GFM plants' commissioning, so EMT studies were not conducted; instead, issues were addressed by monitoring the plants' performance in the field and working with the plant owners to make control parameter adjustments where necessary. Digital fault recorder data has been crucial for plant performance monitoring. The inverter model for the second plant described was tested extensively at NREL in partnership with the plant owner prior to commissioning and again prior to conversion to GFM.

---

[73] PNNL's and EPRI's GFM IBR models were provided both in EMT and positive sequence.

[74] ESIG-GFM-batteries-brief-2023.pdf

[75] https://www.youtube.com/watch?v=2e5ET0L1j5g

HECO Experience

Hawaiian Electric (HECO) conducted extensive EMT studies of GFL and GFM solar PV+BESS and stand-alone BESS plants.[76] Studies showed that GFM controls are crucial to stability of the HECO system in the near future.[77] The first GFM plant in HECO is expected to come online in 2023 with several more to follow in subsequent years. As part of HECO's preparation, they also worked with NREL to test a 2.2 MVA BESS inverter's performance by using power hardware-in-the-loop (PHIL) simulation to connect it to a real-time EMT simulation of Maui's near-future transmission system.[78] The commercially available inverter tested at NREL can operate in GFM or GFL mode. It was used to represent a planned 30 MVA facility. The PHIL tests established that with the hardware inverter in conventional GFL mode, the Maui transmission system is unstable in certain very low inertia dispatch scenarios. They then demonstrated that with the inverter in GFM mode, the system is stable and resilient to a severe fault and an N-1 generation trip for several dispatch scenarios, including a zero inertia (zero synchronous machine) scenario.[79] This study also indicated that, for the Maui system, approximately 30% of online generation capacity needs to be GFM to maintain adequate damping.[80]

Australia Experience

The Australian Energy Market Operator (AEMO) published *Application of Advanced Grid-Scale Inverters in NEM* in August 2021,[81] describing GFM technology and application in the National Electricity Market (NEM). The Dalrymple BESS (30 MW/8 MWh) was the first transmission-connected GFM project in the NEM.[82] The South Australia Hornsdale Power Reserve (HPR) BESS plant has been upgraded from GFL to GFM control with the capabilities of providing grid inertia service[83] in July 2022. The HPR project is described below in more detail. Lastly, development of GFM BESS in Australia continues with BESS plants in New South Wales including:[84]

- Wallgrove GFM BESS by Tesla (50MW/75MWh): Transgrid began commercial operation in December 2022.
- Broken Hill BESS: AGL Energy is commissioning a 50MW/100MWh GFM BESS, construction started in fall 2022 and will be operational in 2023[85].
- Riverina and Darlington Point Energy Storage System: Edify Energy secured financing for three Tesla GFM BESS[86] projects (with total capacity of 150MW/300MWh)
- New England BESS: ACEN has started construction of 50MW/50 MWh GFM BESS in spring 2022 with expected completion date of 2023.[87]
- On December 17, 2022, the Australian Renewable Energy Agency (ARENA) announced co-funding of additional eight large scale GFM batteries across Australia with total project capacity of 2 GW/4.2 GWh, to be operational by 2025.[88]

---

[76] https://dms.puc.hawaii.gov/dms/DocumentViewer?pid=A1001001A21F14B62327F00172

[77] http://www.hawaiianelectric.com/documents/clean_energy_hawaii/selling_power_to_the_utility/competitive_bidding/20211015_exhibit_8_S3_hawaii_model_ESPA.pdf

[78] Power HIL Validation of a MW-Scale Grid-Forming Inverter's Stabilization of Otherwise Unstable Cases of the Maui Transmission System (nrel.gov)

[79] https://www.nrel.gov/docs/fy22osti/83545.pdf

[80] On the HECO systems, additional GFM capacity may be needed to account for possible momentary cessation of GFL generation during transmission faults, which can cause voltage dropping very low in the whole system wide. This conclusion may not apply to the other larger systems where a fault does not reduce voltage system wide.

[81] https://aemo.com.au/-/media/files/initiatives/engineering-framework/2021/application-of-advanced-grid-scale-inverters-in-the-nem.pdf

[82] Dalrymple ESCRI-SA Battery Project – ElectraNet

[83] https://www.pv-magazine-australia.com/2022/07/27/hornsdale-big-battery-begins-providing-inertia-grid-services-at-scale-in-world-first/?utm_source=dlvr.it&utm_medium=linkedin

[84] Upgrade at Tesla Battery Project Demonstrates Feasibility of 'Once-In-A-Century Energy Transformation' for Australia - World-Energy

[85] Broken Hill Battery Energy Storage System | How We Source Energy | About AGL | AGL

[86] https://edifyenergy.com/energy-storage-systems/financial-close-on-the-largest-approved-grid-forming-battery/

[87] https://www.pv-magazine-australia.com/2022/05/26/acen-commences-construction-of-new-england-big-battery/

[88] https://arena.gov.au/news/arena-backs-eight-grid-scale-batteries-worth-2-7-billion/

Hornsdale Power Reserve (HPR) Experience

The HPR BESS project (150MW/193.5MWh) upgraded from GFL to GFM control to enhance grid stability. The process involved four phases, including:

- **Phase 1 – GFM control testing and benchmarking on EMT model and HIL:** One functional behavior of the upgraded GFM control is shown on a single machine infinite bus (SMIB) testing system. The GFM control performances of the EMT model are well benchmarked with HIL using a variety of disturbance tests. The benchmark results of virtual inertial response test is shown in Figure A.2.

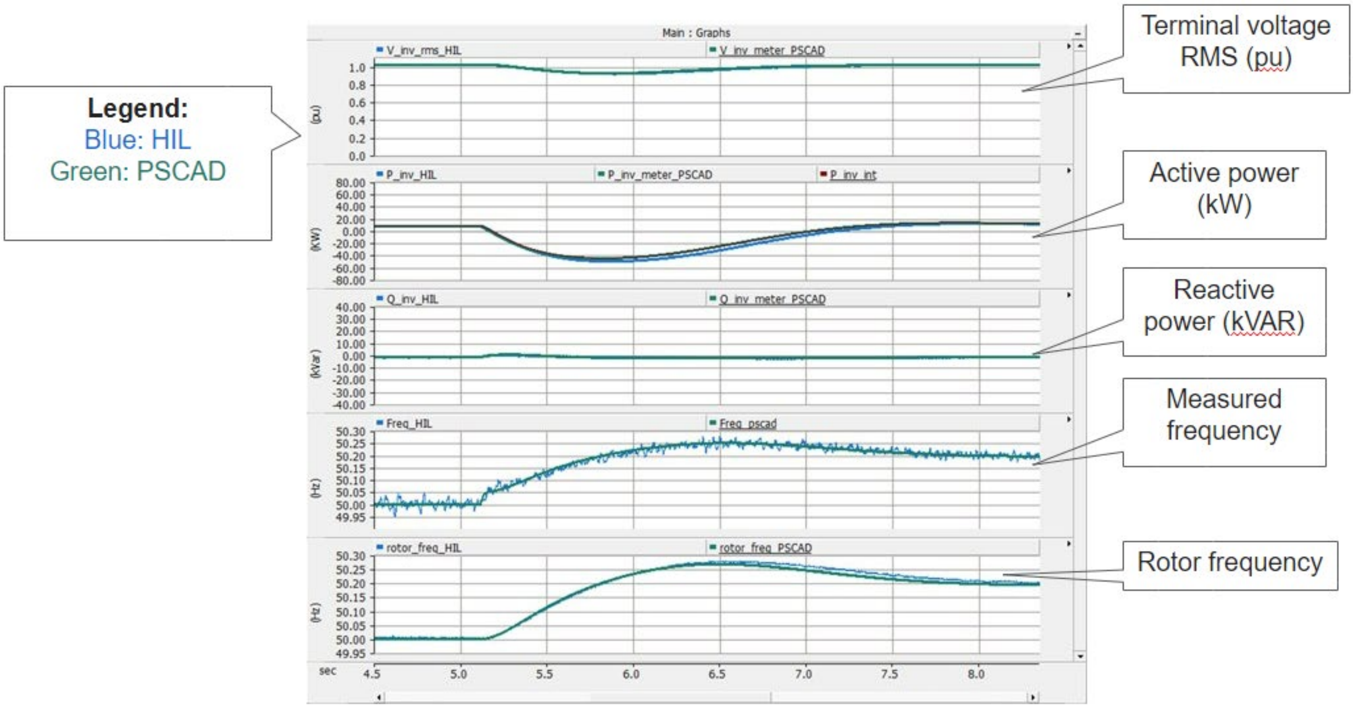


Figure A.2: EMT and HIL (Hardware-in-loop) benchmarking

- **Phase 2 – Trialed GFM control mode at 2 out of 294 inverter at the HPR plant:** The two test inverters were upgraded with the actual GFM firmware while the rest of 292 inverters ran on grid following controls. This verified the different GFM and GFL control responses for the same disturbance. **Figure A.3** and **Figure A.4** show the GFL and GFM active power response, respectively, to the change in frequency. The GFM control contributes maximum power earlier than the GFL control, which is important to support the frequency nadir and avoid underfrequency load shedding. This test shows GFM controller has faster response for overfrequency as well.

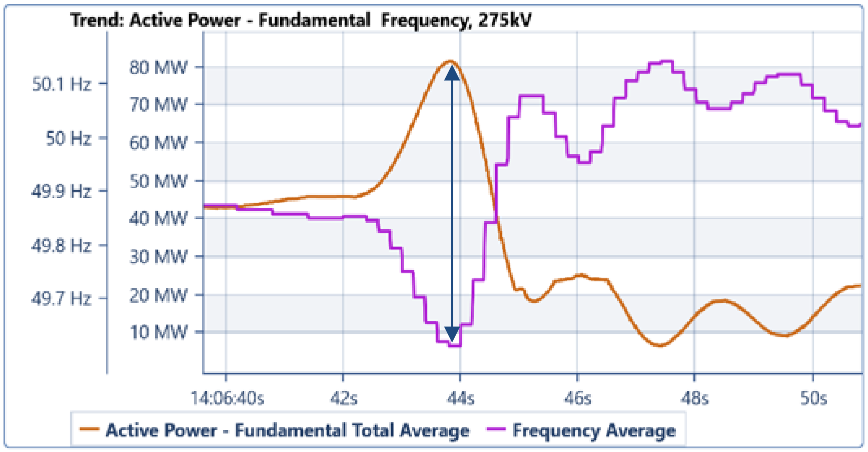


Figure A.3: GFL IBR Response to Frequency Event

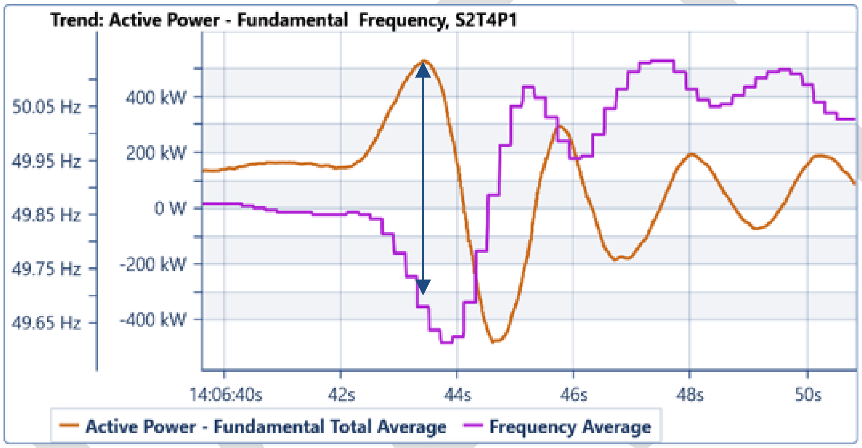


Figure A.4: GFM IBR Response to Frequency Event

- **Phase 3 – A new system interconnection study was performed under national electricity rule NER 5.3.9:**[89] This required to prove that the grid performance of the new grid forming resource is similar or better than the previous grid following resource. The HPR plant virtual kinetic inertial support (2000 MW.s) for South Australia was validated[90] and it was noted grid forming BESS help improve system damping.
- **Phase 4 – After studies were approved, GFM controls were enabled for all inverters at the site:** The HPR GFM plant performances are verified with the recorded site Elspec data which are also used to validate the BESS EMT model. The site Elspec data performance and the EMT model validation for a voltage dip are shown in **Figure A.5**. The HPR plant GFM controls provide damping to power oscillations and inertial energy to limit grid ROCOF and also provide voltage support from sub-cycle current injection when the voltage waveform changes at the inverter terminals.

---

[89] NER Rule 5.3: Establishing or Modifying Connection - AEMC Energy Rules

[90] hornsdale-power-reserve-virtual-machine-mode-testing-summary-report.pdf (arena.gov.au)

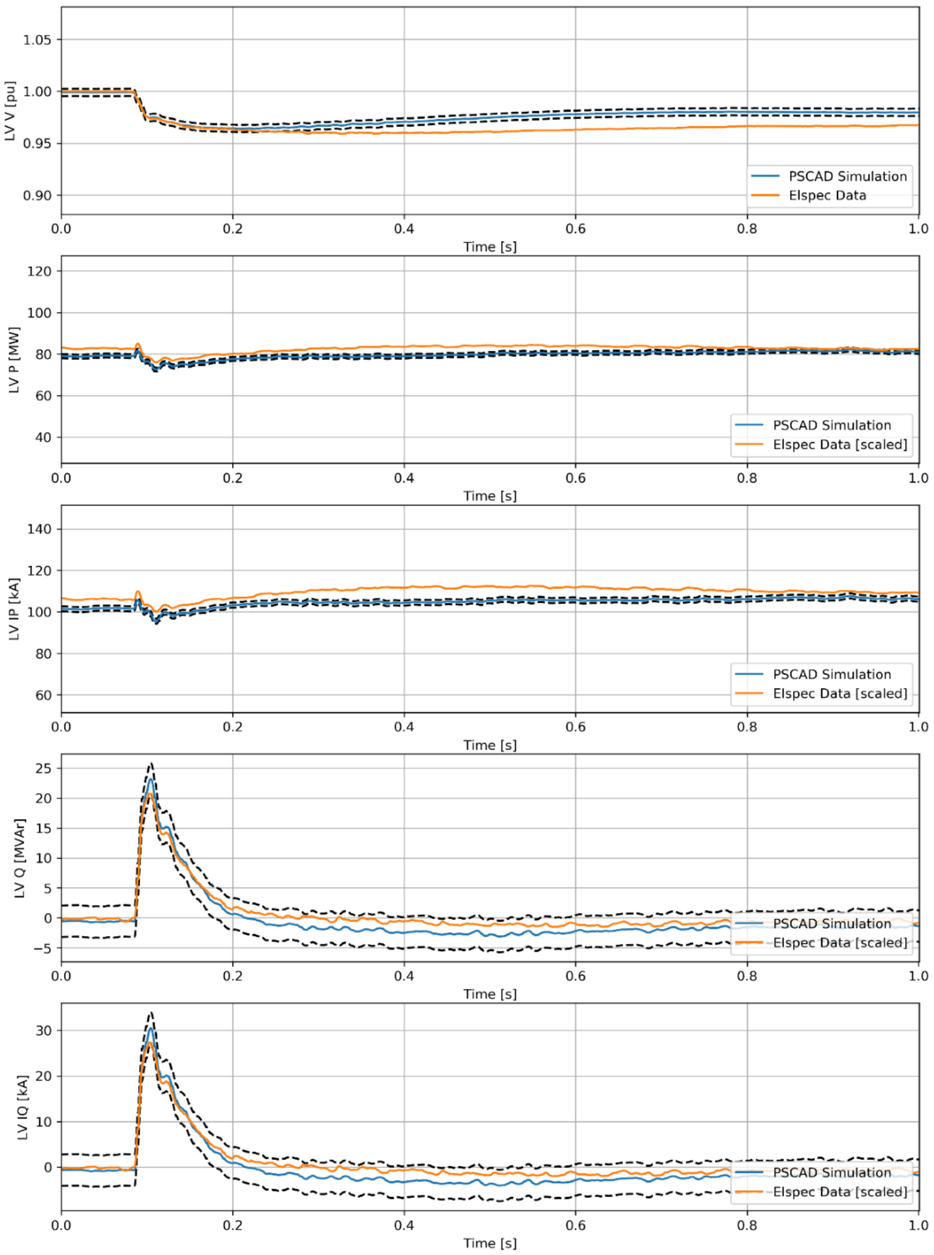


Figure A.5: Response from the inverter during voltage disturbance on the grid

Appendix B: Example of GFM Functional Test with Different OEM

To demonstrate diversity in commercially available GFM technologies and potential differences in their controls and corresponding responses, the GFM functional tests described in Chapter 2 were repeated with a different GFM BESS model provided by another OEM, using the same initial condition and droop parameters. Despite the differences in their dynamic behavior, both OEMs' BESS EMT models passed all three verification tests and are verified to be GFM. Tests results are shown below in **Figure B.1 – B.3**.

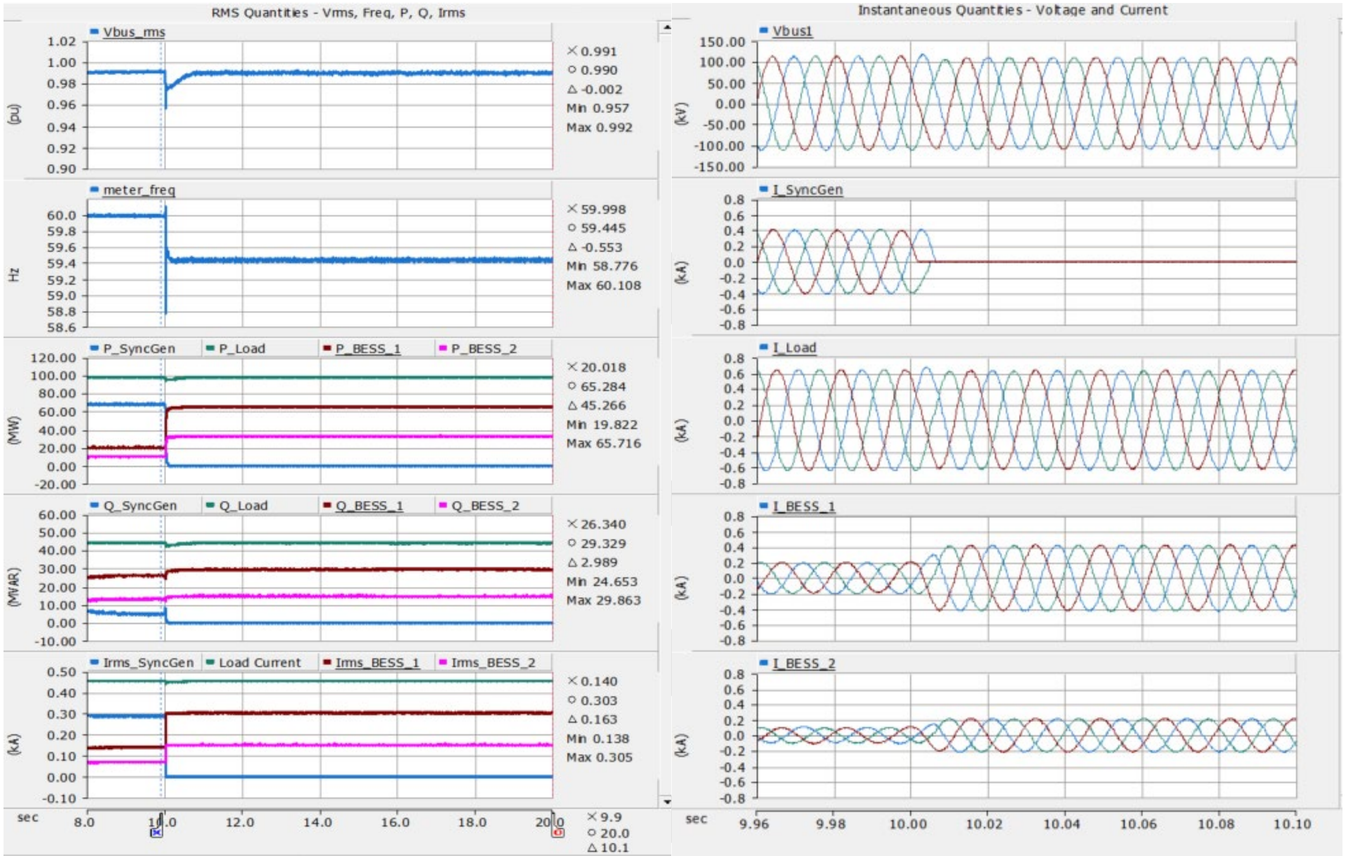


Figure 1 Test 1 Results with Different GFM Model

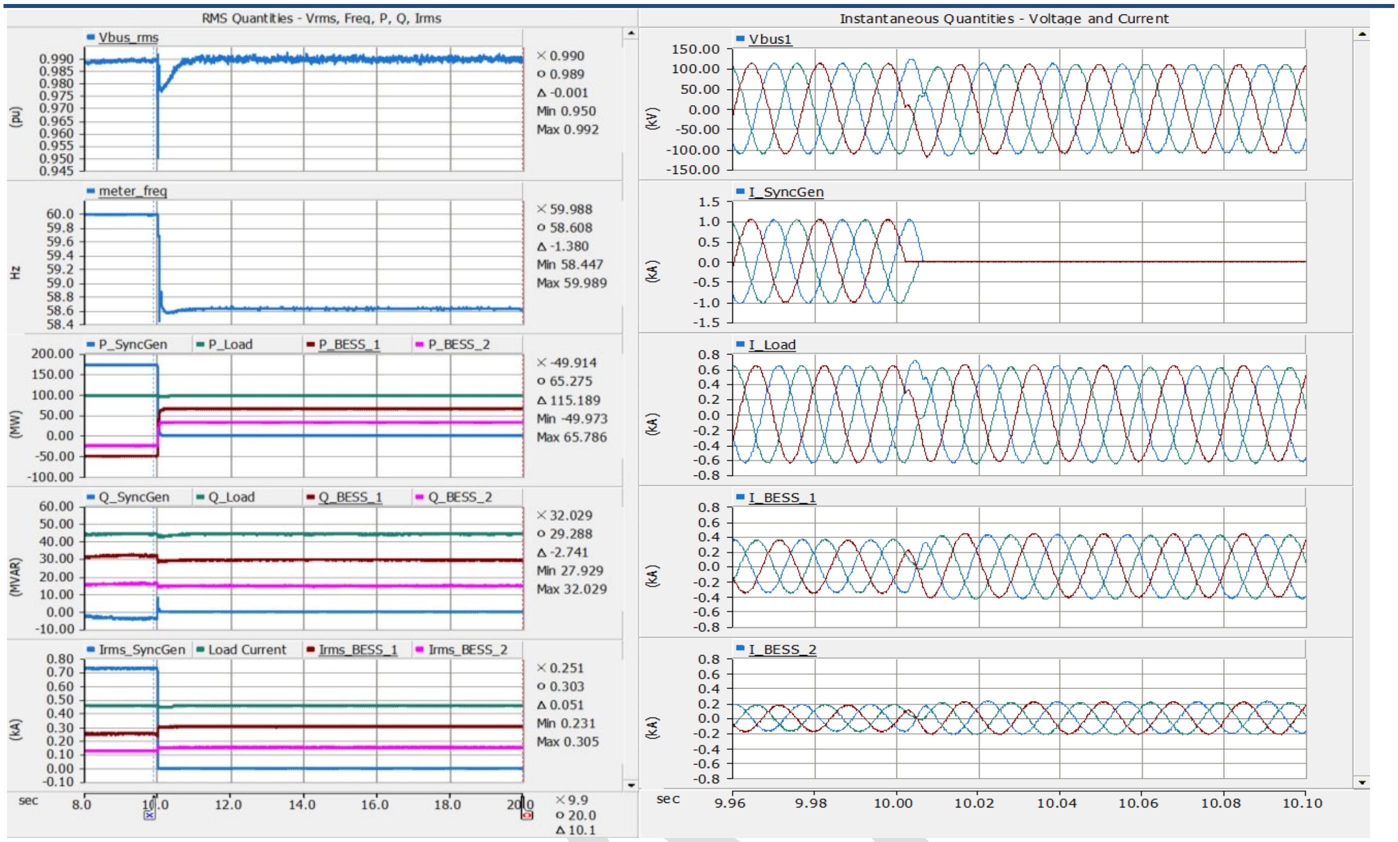


Figure 2: Test 2 Results with Different GFM Model

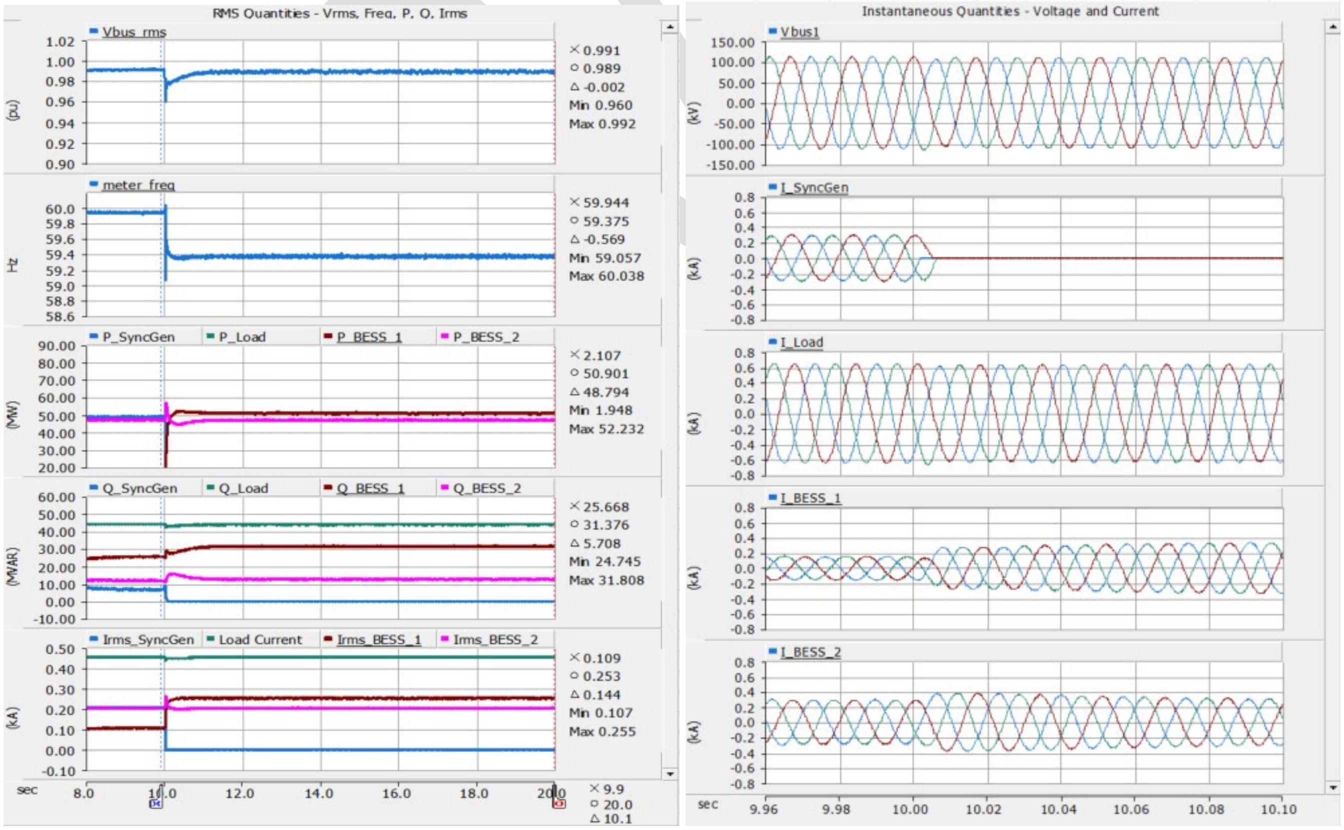


Figure B.3: Test 3 Results with Different GFM Model

Appendix C: Acknowledgements

NERC gratefully acknowledges the invaluable contributions and assistance of the following industry experts in the creation of this paper.

Name	Company
Andy Hoke	National Renewable Energy Laboratory (Primary Contributor)
Andrew Isaacs	Electranix Corporation (Primary Contributor)
Lukas Unruh	Electranix Corporation (Primary Contributor)
Prashant Kansal	Tesla, Inc. (Primary Contributor)
Deepak Ramasubramanian	Electric Power Research Institute (Primary Contributor)
Julia Matevosyan	Energy Systems Integration Group (IRPS Chair) (Primary Contributor)
Jimmy Zhang	Alberta Electric System Operator (Primary Contributor)
Sam Maleki	Electric Power Engineers, LLC (Primary Contributor)
Siddharth Pant	General Electric Company (Primary Contributor)
Hongtao Ma	North American Electric Reliability Corporation (IRPS GFM Specification Co-Coordinator)
Ryan Quint	North American Electric Reliability Corporation (Primary Contributor)
Alex Shattuck	North American Electric Reliability Corporation (IRPS Coordinator)
Aung Thant	North American Electric Reliability Corporation (EMTTF Coordinator)
Rajat Majumder	Invenergy (IRPS Vice-Chair)
Wenzong Wang	Electric Power Research Institute
Amin Banaie	Electric Power Research Institute
Dinesh Pattabiraman	TMEIC
Jing Xie	Pacific Northwest National Laboratory
Thomas McDermott	Pacific Northwest National Laboratory
Lucas Meubrink	SMA Solar Technology AG
Allan Montanari	SMA Solar Technology AG
Li Yu	Hawaiian Electric
Wei Du	Pacific Northwest National Laboratory
Nilesh Modi	Australian Energy Market Operator
Phil Hart	General Electric Company
Sergey Kynev	Siemens Energy, Inc.
Wen-Cheng Huang	Tesla, Inc.

Name	Company
Roberto Favela	El Paso Electric Company
Fred Huang	Electric Reliability Council of Texas
Michael Ropp	Sandia National Laboratory
Brad Rockwell	Kaua'i Island Utility Cooperative
Cameron Kruse	Kaua'i Island Utility Cooperative

NERC also gratefully acknowledges the comments received from Industry provided by the following organizations:

Organization		
EMTP	Arizona Public Service Company	AES Clean Energy
MITRE	Trina Energy Storage	Beacon Power
Natural Resources Canada	ITC Holdings	Edison Electric Institute
Manitoba Hydro	American Transmission Co.	REV Renewables
Evergy	Electric Reliability Council of Texas	Bonneville Power Administration
Western Electric Coordinating Council	Midcontinent Independent System Operator	Advanced Energy United
General Electric	Southern Company	

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Grid Forming Functional Specifications for BPS-Connected Battery Energy Storage Systems

June 2023

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

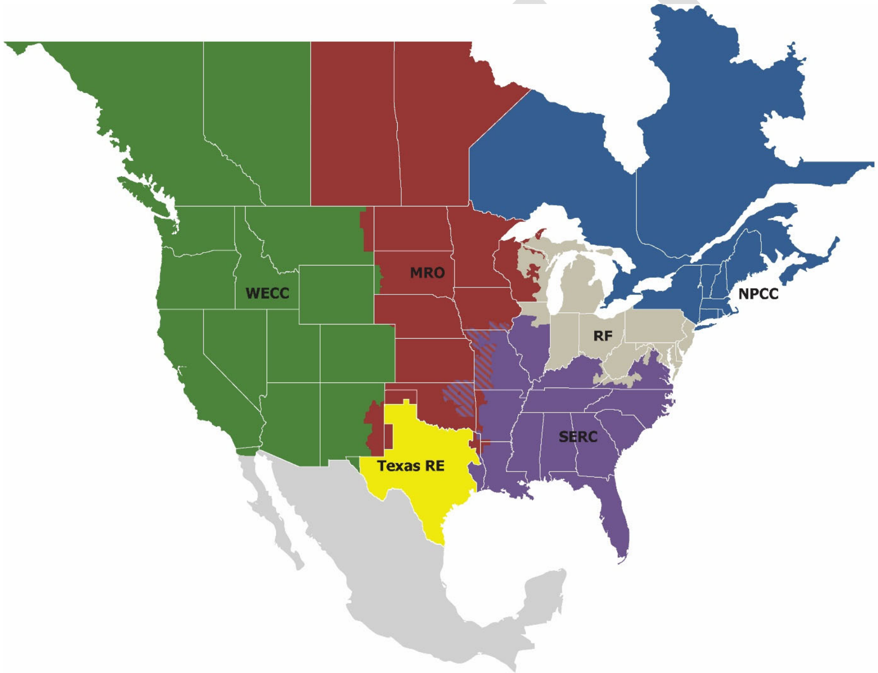
Preface

Formatted

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of NERC and the six Regional Entities, is a highly reliable, resilient, and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six Regional Entities as shown on the map and in the corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Executive Summary

Formatted

Studies have shown that grids dominated by inverter-based resources (IBR), in the absence of supplemental synchronous machine-based solutions, need grid forming (GFM) IBRs to maintain stable operation. While some smaller islanded systems are already facing these challenges today, it is expected that the need for GFM technology will accelerate with the rapid growth of IBRs across North America and the world. Industry needs to proactively plan to ensure sufficient GFM IBRs are installed on the system under these future operating conditions. One of the most significant obstacles of deploying GFM on the bulk power system (BPS) is establishing clear interconnection requirements regarding the expected performance, testing, and validation of the technology. This paper addresses how Transmission Owners (TOs), Transmission Planners (TPs), and Planning Coordinators (PCs) can establish these requirements and test interconnecting resources to ensure they meet the GFM specifications. Generator Owners (GOs) will also have clear performance expectations for GFM resource interconnections and can work with their respective equipment manufacturers prior to interconnection studies being conducted to help streamline the interconnection queue process, where possible. TPs and PCs will need to test new project models to ensure they meet the GFM specifications. The recommended set of GFM tests are provided in this paper, designed to verify the unique characteristics of GFM. The paper also addresses GFM model quality and accuracy as a prerequisite to any studies being conducted.

A common question posed by industry stakeholders is "how many future IBRs should be deployed with GFM functionality enabled?" The answer is system-specific and requires detailed reliability studies to determine, and studies conducted thus far indicate these numbers may be upwards of 30%.[1,2,3] Since the current percentage of GFM resources is near zero in nearly all large interconnected power systems, it is recommended to start requiring and enabling GFM in all future Battery Energy Storage System (BESS) projects for multiple reasons. GFM technology is commercially available but has not yet been widely deployed. ~~and~~ While this technology has great potential in its ability to~~can~~ help improve stability and reliability in areas with high IBR penetration or low system strength areas, responsible entities should ~~study~~ evaluate GFM IBR benefits and performance on their system before following-up with wide-scale implementation[4]. ~~Furthermore, existing BESS can potentially be retrofitted with GFM technology and new~~ New BESS can be equipped with GFM technology at a relatively low incremental ~~project~~ controller and hardware cost.[5][6] Retrofitting an existing BESS projects to implement GFM controls only requires controls changes. However, these changes to an existing plant, as a material modification, will require additional studies to determine any impacts to BPS reliability. Due to the potential costs, time delays and complexities ~~of retrofitting BESS~~of this retroactive process, it is recommended that all new BESS projects are commissioned with the ability to perform GFM control, with GFM controls being enabled after being sufficiently studied. Enabling GFM in all future BESS projects is a relatively low-cost solution that helps ensure system-wide stability that is difficult to quantify today due to study limitations. Industry should begin specifying, requiring, and implementing GFM for all new BPS-connected BESS quickly to mitigate any potential BPS reliability risks that could be posed under high IBR penetration levels expected in the near future. Though the focus in this paper is on near--term BESS applications, GFM technology may need to be considered when developing new ~~IBR~~inverter-based transmission applications, such as –STATCOMs or HVDC converter stations ~~with short-term energy storage~~.

---

[1] https://ieeexplore.ieee.org/document/9875186

[2] Using the full capabilities of modern inverters may enable lowering this threshold somewhat.

[3] This percentage results from a studies performed outside of the North American BPS and is intended to be informational. In order to determine an appropriate percentage for a specific area, similar studies should be performed using large area EMT models.

[4] For example, ERCOT presented the results of ERCOT Assessment of GFM Energy Storage Resources at the Inverter-Based Resource Working Group meeting on 8/11/2023. As the next step, ERCOT will work on the requirements for GFM Energy Storage Resources including but not limited to performance, models, studies, and verification. See Appendix B:~~Appendix B~~ of this paper for more details.

[5] New interconnection studies ~~is~~ are recommended for the existing GFL project updated to GFM.

[6] Cost to implement GFM technology varies due to variations in the hardware on-site and the performance intended to be enabled.

Key Takeaways and Recommendations

The following key takeaways and recommendations should be considered and implemented by the associated entities for adoption of GFM to improve overall BPS reliability under conditions of increasing penetrations of IBRs:

- GFM technology is commercially available and field-proven for ~~BPS-~~transmission-connected applications, particularly for BESS (including standalone BESS[7] in ac-coupled hybrid plants) as well as dc-coupled solar photovoltaic (PV)+BESS[8] applications. GFM requirements, policies, and/or market incentives should be developed for BESS or hybrid plants including BESS, as mentioned above. (Original Equipment Manufacturers (*OEM~~s~~)*, *developers, GOs,* ~~*GOPs*~~*Generator Operators (GOP), TPs, PCs, Transmission Operators (TOPs), Reliability Coordinators (RCs), regulatory entities, policymakers)*

- All newly interconnecting BPS-connected BESS should be designed, carefully studied ~~and coordinated with~~by responsible entities ~~before implementationplanned~~, and commissioned with GFM controls[9] enabled to improve overall system stability across the BPS, particularly with increasing levels of IBRs. Developers and GOs can ensure requirements[10] are in contractual language with OEMs. Existing BESS may be able to be retrofitted at relatively low incremental controller and hardware costs; however, they will need to be restudied by the TP~~ and ~~,PC, TOP, RC, or BA and potentially retuned, as determined by the study results. In cases where the responsible entities conclude that barriers to deploying GFM BESS exist today, ~~owners and developers~~responsible entities should consider specifying IBRs that can be configured for both GFL controls and GFM controls; this will allow the controlled testing of the technology under both owner and responsible utility oversight. *(GOs, TPs, PCs, RCs, TOP, BA developers, OEMs)*

- TOs in consultation with their TPs and PCs, should leverage the information in this white paper to begin the process of establishing ~~clear~~ GFM functional specifications for BESS in their interconnection requirements (or provisions in power purchase agreements) in anticipation of future GFM BESS installations. ~~using the materials contained in this guideline.~~ ~~*(TOs, TPs, PCs)*~~ ~~As alwayswith any other technology~~As with any other resource, GFM BESS should be studied to assess its ~~effect~~ impact on the BPS before in~~s~~terconnection. Additionally, It is recommended to require adequate fault recording and sequence of event recording equipment before installing a GFM IBR to ensure adequate assessment of the performance of the GFM controls during BPS disturbances.

- TPs and PCs should begin training their staff in conducting studies to assess the functional differences in GFM controls so that they can be properly prepared to integrate GFM functional testing requirements in their interconnection study processes ~~that~~ ensur~~e~~ing that newly connecting GFM is able to meet the performance requirements for GFM. *(TPs, PCs)*

- GFM technology ~~can~~ has been shown to operate reliably and provide stabilizing characteristics in transmission systems outside of the BPS in areas of high IBR penetrations and areas of low system strength. GFM BESS presents a unique opportunity to support system stability (e.g., transient, oscillatory, voltage) with a relatively low incremental cost to all resources and end-use consumers. *(Developers, OEMs, GOs, GOPs, TPs, PCs, TOPs, RCs)* While the results seen by others outside of the North American BPS ~~is~~are very encouraging, careful testing and validation of GFM performance by responsible entities is still needed -before broad deployment of this technology in their system.

- GFM technology will continue to develop and improve beyond where it is today. Future research efforts can help aid in accelerated development and adoption, particularly focusing on GFL-to-GFM conversion possibilities, equipment standardization, GFM in blackstart applications, technical specifications for GFM blackstart, and GFM controls in other IBR technologies such as wind and solar PV. *(US Department of Energy, national laboratories, research institutes, academic institutions)*

---

[7] World's largest 'grid-forming' battery to begin construction in Australia – pv magazine International (pv-magazine.com)

[8] Hybrid Solar and Storage in Hawaii | T&D World (tdworld.com)

[9] As functionally specified in this paper

[10] See, for example: Appendix J-1 Oahu RDG PSA (hawaiianelectric.com)

Introduction

Background

NERC *White Paper: Grid Forming Technology*[11] defined GFM controls for IBRs as:

> **Grid Forming Control for BPS-Connected Inverter-Based Resources** are controls with the primary objective of maintaining an internal voltage phasor that is constant or nearly constant in the sub-transient to transient time frame. This allows the IBR to immediately respond to changes in the external system and maintain IBR control stability during challenging network conditions. The voltage phasor must be controlled to maintain synchronism with other devices in the grid and must also regulate active and reactive power appropriately to support the grid.

This uniquely differs from conventional grid following (GFL) IBR controls in that the primary GFL control objective in the sub-transient time frame is to maintain a constant output *current* phasor magnitude and angle, with adjustments~~. Subsequently, T~~t~~he current phasor begins changing within the sub-transient time frame (e.g., 5 cycles after a disturbance)~~ to control~~-~~ the ~~-~~desired active and reactive power being injected into the network.~~ In the shortest [sub-transient] time frames (e.g., 0-5 cycles after a disturbance), a conventional GFL inverter's control objective is to maintain a desired active power and reactive power~~, ~~so~~ Hence, ~~it~~ GFL does not maintain fixed voltage magnitude or phase angle on those timescales. On longer timescales (seconds), it can also pursue other control objectives such as maximum power point tracking, frequency response, and voltage regulation.

A GFM inverter's control objective, on the other hand, in the shortest [sub-transient] time frames (e.g., 0-5 cycles after a disturbance), is to maintain *voltage* phasor magnitude and angle internally, and prioritize the support of terminal voltage. Therefore, it does not maintain fixed active or reactive power on those time frames. On longer time frames, a GFM inverter must also synchronize with other sources and may also pursue other objectives including tracking of active power and reactive power set point. In all cases, the inverter controls could be restricted by the inverter and primary energy source capability limits (e.g., available energy, current limits, voltages).

Benefits of Enabling GFM Controls in BPS-Connected BESS

It is estimated that there was 427 GW of BESS capacity (includinge~~es~~ both standalone BESS capacity and BESS capacity as a part of hybrid plants) in the interconnection queues around the US as of the end of 2021.[12] By the end of 2022 this number increased to 680 GW[13]. In the absence of any requirements or incentives for GFM capability, all of these resources are being planned with GFL controls. Many of these BESS will be deployed in IBR-dominated areas of the BPS with existing stability constraints. Installing these resources as GFL will likely further reduce stability margins and may result in new stability constraints. This will lead to further reduction of low-cost generation from existing IBRs in these areas (i.e., curtailment of IBRs during real-time operation) due to stability constraints that could be addressed by GFM, thus increasing overall energy costs. To relieve these constraints without considering GFM in BESS, additional transmission assets such as synchronous condensers[14] , GFM STATCOM[15] with energy storage, or new transmission lines[16] will be needed which will drive transmission costs higher.

GFM controls can provide grid stabilizing characteristics that support reliable operation of the BPS under increasing penetration of IBRs. Enabling GFM in BPS-connected BESS allows for system-wide enhancement of stability margins

---

[11] https://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_Grid_Forming_Technology.pdf

[12] https://emp.lbl.gov/sites/default/files/queued_up_2021_04-13-2022.pdf ~~and https://emp.lbl.gov/sites/default/files/queued_up_2022_04-06-2023.pdf~~

[13] https://emp.lbl.gov/sites/default/files/queued_up_2022_04-06-2023.pdf

[14] https://aemo.com.au/-/media/files/electricity/nem/security_and_reliability/congestion-information/sa-transition-to-fewer-synch-gen-grid-reference.pdf?la=en

[15] STATCOM Technology Evolution for Tomorrow's Grid (nxtbook.com)

[16] Adding new transmission lines will decrease the transfer impedance (make it a stiffer/stronger system)

as these resources are interconnected. Therefore, system stability enhancements can be achieved at much lower cost than through the addition of transmission assets.[17] As discussed above, GFM controls can be implemented on any type of IBR including new solar photovoltaic and wind plants with some limitations; however, GFM controls in BESS are particularly low hanging fruit for assuring BPS reliability since they already have the needed energy buffer on the dc side which makes the enhancement purely software-based (minimizing much more costly hardware-based improvements and/or the moderate level of curtailment that may be needed for other IBR technologies).

While some areas like the Hawaiian islands already need to enable GFM BESS to maintain grid stability and prevent large-scale outages, many areas of the US are reaching relatively high penetrations of IBRs now or in the future and will face similar challenges. Industry is faced with a unique window of opportunity to procure, test, and gain experience with GFM technology now before significant adverse reliability issues are faced with insufficient GFM controls installed in the future.

Testing and Demonstration of Services Ahead of Requirements

Existing GFL technology can provide a number of essential reliability services to the BPS. Demonstration projects[18] have illustrated these capabilities for many years, and modern IBR facilities can provide regulation services, primary and fast frequency response, dynamic voltage support, etc. GFM control do not preclude a resource from providing any of these critical features to the BPS. Rather, GFM controls enable additional features from BESS beyond what can be provided from GFL today. Examples include operating in low system strength conditions, improving overall system stability, helping stabilize the system following large generator loss events (supporting arresting frequency changes), and potentially enabling blackstart capability from IBRs.

Multiple GFM projects around the world have been deployed, with more GFM projects under procurement See **Table I.1** and more details in Error! Reference source not found.~~**Appendix A**~~. However, widespread adoption has been relatively slow due to limited pilot projects (particularly of large numbers of GFM resources in one area) and difficulties establishing GFM performance specifications and testing procedures. Furthermore, detailed studies of GFM technology require electromagnetic transient (EMT) modeling, which is challenging for large areas ~~and industry is challenged conducting large EMT studies~~ due to lack of expertise and computational limitations today.

Table I.1: GFM BESS Projects Deployed or~~-~~ under Construction

Project Name	Location	Size (MW)	Time
Project #1	Kauai, USA	13	2018
Kauai PMRF	Kauai, USA	14	2022
Kapolei Energy Storage	Hawaii, USA	185	2023
Hornsdale Power Reserve	Australia	150	2022
Wallgrove	Australia	50	2022
Broken Hill BESS	Australia	50	2023
Riverina and Darlington Point	Australia	150	2023
New England BESS	Australia	50	2023
Dalrymple	Australia	30	2018
Blackhillock[19]	Great Britain	300	2024
Bordesholm[20]	Germany	15	2019

While GFM capability in batteries can be delivered at relatively low incremental cost, there may still be some costs associated with project and product development simply due to the newness of the technology. Widespread

---

[17] Transmission assets still serve critical roles for overall BPS reliability in addition to the considerations for GFM BESS presented in this paper.

[18] Demonstration of Essential Reliability Services by a 300-MW Solar Photovoltaic Power Plant (nrel.gov)

[19] Zenobē breaks ground on pioneering 300MW battery in Blackhillock - Zenobē (zenobe.com)

[20] The Bordesholm stand-alone grid ensures power supply even in the event of a grid failure - Sunny. SMA Corporate Blog (sma-sunny.com)

adoption of GFM IBRs will ensure an adequate level of BPS reliability moving forward. In addition, market operators may establish market-based mechanisms that can drive GFM adoption at a rapid pace, where appropriate.

The Cost of Inaction

This is a unique moment in the industry when a need is becoming fully understood and an effective, relatively low-cost GFM solution has emerged. GFM capability in BESS is a viable and effective solution to address declining stability margins system-wide and to manage decreasing system strength and the issues that arise under these conditions (e.g., wind and solar PV curtailments). The industry is at the cusp of a rapid growth of BESS capacity on the system in the next few years. Without GFM functional specifications and test procedures established by TOs, TPs, and PCs, and the appropriate incentives or requirements in place, much or all of the newly installed BESS capacity will likely not have GFM capability enabled (either precluding the possibility of GFM or requiring significantly more costly retrofits or network upgrades). If GFM capability is not adopted very soon, the outcome will be reduced transfer limits for existing IBRs and consequently growing levels of solar PV and wind curtailment, and additional costs of supplemental stabilizing equipment (e.g., synchronous condensers) in the future.

ISOs/RTOs/utilities should work with stakeholders to carry out studies of the implementation of GFM technology in low grid strength areas[21] and act quickly to implement pilot projects (similar to how the provision of ancillary services from GFL IBRs has been tested in the past). Experience from GFM BESS project installations around the world, particularly Great Britain and Australia (see Error! Reference source not found.~~**Appendix A**~~), can be used as a guide.

Presently, the recommendation is that all new BESS connecting to the BPS should have the capability for GFM operation or future capability to be upgraded with GFM controls (if necessary). TOs should establish this requirement in their interconnection requirements or power purchase agreements (PPAs). Developers and GOs can also ensure that these requirements are in contractual language with the equipment manufacturers. To support enhanced BPS reliability, ~~I~~it is strongly recommended that newly interconnecting ~~resources~~ BESS enable GFM capability, or have the capability for ~~the~~ GFM controls. Additionally, GFM controls should be enabled only after being studied by responsible entity as with any new resource or qualified change. ~~to support enhanced BPS reliability.~~

Functionally Defining GFM Performance

Although the concept of GFM technology has been around for many years, mainly in small islanded systems or microgrids, the term has presented confusion in recent years when the concept is applied to the BPS. Various documents have proposed definitions to try and reduce confusion (see Appendix A for reference). Most definitions agree that at a minimum GFM controls tend to hold their voltage magnitude and angle at the device terminals constant in the period immediately following a system event. This tends to provide a resistance to change in the external system and thereby grants certain stabilizing properties. Although there is general consensus on what GFM is as a concept, opinions differ on the degree and extent the concept should be used when qualifying an interconnecting device as GFM, as well as how to test the capability. Specifying GFM may be done in a number of ways, including the following:

1. Control topology: The theoretical behavior of a device may be defined based on specific types of control topologies such as virtual synchronous machine or droop-based topologies. It is not recommended to define GFM behavior based on control topology, to leave the room for innovation.
2. *Quantitative response metrics:* The precise behavior of a device in response to external system events can be defined, with no regard to the internal control topology. Quantities like active and reactive power rise time in response to a network event can be used to test whether the controls provide the stabilizing influence expected from GFM.
3. *Frequency domain characterization:* GFM controls tend to have signature responses to stimuli with varying frequencies. It is likely possible to provide an accurate determination of the GFM capabilities of a device by

---

[21] Due to loss of last synchronous machine, an extremely low system strength scenario manifests in the tests described in this document

measuring its response to external perturbations across a range of frequencies[22]. Significant promising research work is underway in this field.[23] [24]

4. *General testing definition (***Recommended***):* It is possible to determine whether a device functionally meets the definition for GFM control by observing whether the device is capable of performing well during certain well-defined simulation tests. For example, GFM IBRs can be subjected to severe external events that are generally difficult or impossible for conventional GFL devices to stably operate through. For example, a GFM device, like a synchronous generator, is able to operate and serve load with no other synchronous machines in service. It is generally able to operate in synchronism with other synchronous machines, continue stable operation when those machines are disconnected, and continue stable operation when those machines are re-connected. GFL IBRs are generally not able to do all of these things. Even if a GFM plant will not be subjected to these events in real-time operation, the tests indicate that the controls can provide the stability benefits needed.

To avoid confusion and conflicts in understanding, the fourth approach is proposed and further described in Chapter 2, until sufficient research and field experience is available to fairly and effectively use other methods. This method provides confidence that GFM controls will provide the necessary stabilizing characteristics even if the specific test scenarios never occur during real-time operations. The general testing definitions in this white paper are not intended to be overly prescriptive and should be used to inform the development of future qualitative GFM performance requirements. The method is simple to implement and agnostic to GFM control topologies, and similar approaches have been successfully implemented in BESS procurements around the world[25] [26].

Minimum Necessary Capacity of GFM Inverters for Future High IBR Grids

It is well understood that as the penetration of IBRs continues to rise and ~~therefore~~ the stabilizing ~~characteristics~~effects provided by synchronous machines decrease~~s~~, the grid will need some amount of GFM-enabled resources to ensure system stability[27]. This logically raises the question of a necessary or recommended capacity (presumably a % value) of GFM-enabled IBRs relative to the total capacity of IBRs and/or machines on the BPS. While industry does not currently have a rule-of-thumb to prescribe the minimum necessary capacity of GFM IBRs needed to stabilize a given system, recent research provides a few points of reference. This section outlines current industry recommendations on this topic.

Relatively few studies have been performed, particularly for large interconnected power systems. However, smaller islanded systems have explored this issue in much more detail. For example, power hardware in the loop (PHIL) tests of the HECO Maui system illustrated the percentage of GFM inverters needed for stability at various system inertia levels.[28] This work found that as system inertia dropped towards zero (an entirely inverter-based system), the amount of GFM inverters necessary to maintain system stability increased relatively linearly. When the system has zero mechanical rotating inertia system inertia, the percentage of GFM inverters relative to total system capacity (consisting of only GFM and GFL inverters) was around 30% (see **Figure I.1**~~**Figure I.1**~~). The GFL IBRs in this system consisted primarily of IBRs with no voltage or frequency support capability, with only a few grid-supportive GFL IBRs providing voltage support or fast frequency response. HECO also highlighted needing some reliability margin, therefore recommending that this ratio be increased to account for unexpected issues like legacy distributed energy resource momentary cessation issues or unexpected inverter tripping issues. This study also highlighted that the

Formatted: Font: Calibri, Font color: Blue

---

[22] Small-signal frequency-domain methods can be used as screening methods which are typically followed up by time-domain verification that consider both large and small-signal stability.
[23] Sequence Impedance Measurement of Utility-Scale Wind Turbines and Inverters - Reference Frame, Frequency Coupling, and MIMO/SISO Forms (nrel.gov)
[24] https://www.nrel.gov/docs/fy23osti/84604.pdf
[25] https://www.nationalgrideso.com/document/250216/download
[26] https://www.youtube.com/watch?v=2e5ET0L1j5g
[27] Note that, alternatively, adequately sized and placed synchronous condensers can also be used to ensure system stability with high IBR. However, with GFM capability provided by IBRs themselves, installation of these additional grid assets can be avoided.
[28] https://ieeexplore.ieee.org/abstract/document/9875186

necessary capacity of GFM IBRs does not necessarily depend on the total percentage of generation from IBRs (which was above 95% in all cases studied). Instead, low total online synchronous machine capacity (as quantified via system inertia constant, for example) was a much better predictor of the need for GFM.

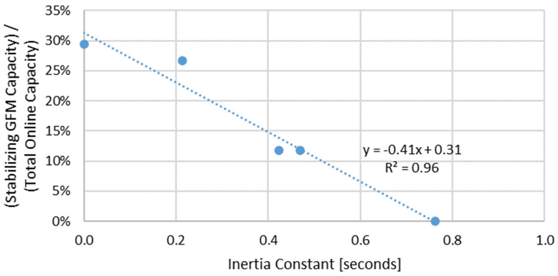


Figure I.1: HECO Study of GFM Needed for Stability at Various Inertia Levels

Similarly, a recent paper[29] from the European Union-funded project, MIGRATE, studied the composition of GFM and GFL inverters in various systems and identified a need for at least a 37% ratio of GFM IBRs to total IBRs in the system. There were sensitivities based on numerous factors that modified that number slightly.

It is important to note that the actual GFM capacity needed for system stability will vary from system to system and can also depend on the type of contingency being studied. Issues could be system-wide (e.g., need for stable fast frequency response) or could be more localized (e.g., need for operation in low short circuit strength networks). This could drive the need for stabilizing services from additional resources, or from existing installed resources. The needed capacity of GFM is also impacted by the dynamic characteristics of other sources in the network such as GFL inverters and load. With the approval of FERC Orders 842 and 827 and IEEE 2800-2022, the response of GFL resources may be more advanced than that of legacy IBRs, which could impact the necessary capacity of GFM to maintain grid stability.

As an example, a study on an island power network[30] identified that the minimum percentage of GFM required to maintain frequency and voltage stability was 11% if frequency and voltage support were provided by other IBR resources per IEEE 2800-2022. However, if GFL IBRs had no frequency and voltage response capability, the study identified that a minimum of 23.5% GFM IBR was necessary to maintain stability. Therefore, it is important that TOs, TPs, and PCs ensure adequate levels of GFM resources moving forward to maintain system stability, with suitable margin to avoid any adverse reliability impacts from unexpected performance issues.

---

[29] https://www.h2020-migrate.eu/_Resources/Persistent/5d0f8339650bcf53cd24a3006556daa1da66cb42/D3.4%20-%20New%20Options%20in%20System%20Operations.pdf

[30] “Services from IBR for future systems”, 2022 ESIG Reliability Working Group Meeting, October 2022.

Chapter 1: Functional Specifications for GFM BESS

Formatted

This chapter defines the recommended functional specifications for GFM BESS that applicable entities can use to inform inclusion of GFM specifications in their requirements. For effective and efficient adoption of GFM technology, TOs will need to establish functional specifications that define GFM functionality. The GFM specification can then be provided to OEMs by developers and GOs to ensure procurement of GFM resources.

Functional Specifications for GFM and GFL Battery Energy Storage

All BPS-connected generating resources are required to meet applicable interconnection requirements and performance-based standards. Requirements often establish specifications related to, but not limited to, the following:

- **Dispatchability:** Capability of the facility to be dispatched (or curtailed) to a specific active power set point
- **Steady-State Voltage Control:** Capability of the facility to control steady-state voltage at the point of interconnection to a specific voltage schedule (set point and operating band)
- **Dynamic Reactive Power Support:** Capability of the facility to provide dynamic reactive support in response to normal and emergency grid conditions within the expected ride-through performance range
- **Active-Power Frequency Control:** Capability of the facility to respond to changes in system frequency by changing active power output when the resource has available headroom/tailroom
- **Disturbance Ride-Through Performance[31]:** Capability of the facility to ride through normal grid disturbances within a defined set of parameters or expectations including but not limited to faults, and phase jumps
- **Fault Current and Negative Sequence Current Contribution:** Capability of the facility to provide fault current, including negative sequence current to mitigate unbalanced voltage conditions and facilitate relay operation[32]
- **Security:** Capability of the facility to ensure cyber and physical controls are in place to ensure resilience to potential threats.

Functional Specifications Defining Grid Forming BESS

Additionally, the functional specifications need to be clearly defined for the GFM-specific functions. The following are performance characteristics specific to GFM BESS: These characteristics shall be provided within GFM BESS equipment rating limits:

- **GFM-Specific Voltage and Frequency Support:** GFM shall provide autonomous, near-instantaneous frequency and voltage support by maintaining a nearly-constant internal voltage phasor in the sub-transient time frame, including:
    - **Phase Jump Performance:** GFM shall resist near-instantaneous voltage magnitude and phase angle changes by providing appropriate[33] levels of active and reactive power output in the sub-transient time frame.
    - **System Strength Support:** GFM shall help reduce the sensitivity of voltage change for a given change in current in the sub-transient time scale.

---

[31] GFM BESS FRT capability and performance during and after the fault is critical to grid stability and should be tested just as it would be for a GFL facility

[32] This can be achieved, for example, by maintaining balanced GFM resource internal voltage during asymmetrical faults.

[33] As an example, if the phase difference between the inverter terminal and the grid increases, the resource should increase (or make less negative) its active power injection in the sub-transient time scale. If the phase difference reduces, it should result in a reduction of its active power injection in the sub-transient time scale.

- **Ability to Stably Operate with Loss of Last Synchronous Machine:** GFM shall be able to stably operate through and following the disconnection of the last synchronous machine in its portion of the power grid[34].

There are additional desirable characteristics for GFM performance; however, present technology may not be able to widely meet this performance specification today. Therefore, they are listed here for consideration in specification for future GFM technology. They include the following:

- **Passivity:** GFM should present a non-negative resistance and present a passive characteristic to the grid within a wide frequency range (0–300 Hz) to prevent adverse interactions.
- **Negative Sequence Current during Continuous Operating Region:** GFM Plant should provide negative sequence current.
- **Balanced GFM Internal Voltage:** The GFM resource should also ensure its internally generated voltage remains balanced during all near-nominal operating conditions (e.g., 0.9–1.1. pu voltage range).

Blackstart Considerations

GFM and blackstart-capable are not synonymous terms; however, GFM functionality is a prerequisite for an inverter-based resource (IBR) to be eligible for blackstart capability. The TO, TOP, or RC may establish additional requirements for blackstart capability[35] beyond the general specifications for GFM, which may necessitate extended capability for the short-term overcurrent, more stringent ride-through capability, longer energy duration needs or additional hardware to supply sufficient and reliable start-up power to restore the electricity system from a blackout. These unique local requirements may preclude certain GFM resources from participating in blackstart services. It should be noted that a GFM IBR does not necessarily have to provide blackstart services, and blackstart capability requirement should be specified separately.

Additional Considerations

The following are additional considerations for the functional specification of GFM in BESS:

- All the functional specifications listed above are applicable when the BESS is within its limits of the energy source behind the inverter and the equipment ratings of the inverter[36]. These functional specifications do not impose any requirements for fault current capability beyond equipment ratings.
- GFM BESS shall continue providing GFM operational characteristics even at its highest and lowest allowable state of charge. If the BESS remains connected to the network, it shall remain in GFM mode as defined in the Introduction of this document. There should be no state of charge condition where the BESS should need to operate in GFL mode.
- Performance requirements for BPS-connected inverter-based resources such as, for example, IEEE 2800 may also apply to GFM resources unless explicitly stated by the local interconnection requirements. To the extent that existing requirements in IEEE 2800 may create any barriers to GFM applications, exceptions may need to be considered and specified by the TO, TOP, RC, or BA. Simultaneously, industry can contribute towards improvements of the relevant standards to accommodate the requirements for GFM.

---

[34] While generation capacity in the system can still meet the load.

[35] https://www.hawaiianelectric.com/documents/clean_energy_hawaii/selling_power_to_the_utility/competitive_bidding/20220531_exh_5.pdf

[36] Transient conditions can cause GFM BESS to reach current limits, resulting in transient behavior that differs from the GFM performance characteristics described above.

Chapter 2: Verifying GFM Functionality

This chapter describes the functional performance verification tests that determine whether an interconnecting BESS can be classified as GFM. TPs and PCs should integrate these tests as part of the interconnection study process in coordination with TOs, PCs, BAs, or TOPs establishing GFM requirements for newly interconnecting BESS. GOs, developers, OEMs can ensure that planned facilities meet these functional specifications prior to interconnection studies, which will help expedite the process. Verifying GFM functionality with test simulations[37] (referred to herein as "GFM functional tests") using accurate and detailed electromagnetic transient (EMT) models provided and certified directly from the OEM is necessary, in addition to attestations and detailed descriptions of the control modes from the OEMs.

Model Quality Fundamentals

The most important prerequisite to model-based performance verification is establishing confidence in the model quality. Ensuring an accurate and verified model is a fundamental pre-requisite to conducting any reliability studies using the models, and clear model quality requirements and checks should be established by TPs and PCs in all instances. As with all model representations of actual facilities, the following fundamental aspects of modeling and verification are needed before GFM-specific testing is conducted:

- OEM-provided validated models and validation test reports against lab or field test, or hardware-in-the-loop test of the product to be used in this project. This model validation test may include a generic representation of the overall facility but must include the actual control and converter level protection of the product that will be installed in the project. The following validation tests are recommended at a minimum:[38]
  - Balanced and unbalanced faults
  - Grid voltage disturbance – step change in magnitude and phase
  - Grid frequency disturbance – step change in frequency and frequency ramp at slow and fast ROCOF
  - Active and reactive power dispatch command step change
  - Loss of the last synchronous generator[39]
  - Load rejection
- Attestation from the inverter OEM(s) that the model provided matches the expected as-built configuration and settings to the degree known at the time of model submission.[40]
- Attestation from the plant-level controller(s) OEM(s) that the model provided matches the expected as-built configuration and settings to the degree known at the time of model submission.
- Model quality checks conducted by the TP/PC to ensure appropriate representation and parameterization of the model provided by the GO/developer.
- Model documentation is provided that describes the functionality and operation of the resource being deployed and model used.
- The model meets the quality criteria outlined in the NERC EMT Reliability Guideline[41]

---

[37] One of the best mechanisms to gain confidence in simulation models is to compare them against real event data. Currently availability of this type of data is limited for GFM installations, but as more are obtained in the coming years it will be beneficial to review this performance and integrate the learning into future GFM guides.

[38] Refer to IEEE 2800.2 once published for additional benchmarking test that could supplement or augment those listed.

[39] For model validation using hardware testing, OEMs may choose to leverage tests similar to those outlined in "Verification Test for GFM Functionality" section.

[40] The final tuning parameters/setting of the project should be accompanied with the provided model parameters/settings update to GO/TO.

[41] https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Reliability_Guideline-EMT_Modeling_and_Simulations.pdf

Description of GFM Functional Test System

The GFM functional test system (see **Figure 2.1**) consists of the following components connected to a single bus without any impedance:

- A synchronous generator with a simple excitation system model (e.g., SCRX) and turbine-governor model (e.g., TGOV1), with circuit breaker[42]
- A load[43] with both active and reactive power (inductive) components, with a maximum power factor of 0.9
- The GFM BESS plant model under test
- A duplicate of the GFM BESS plant model, rated at or near half (MVA and MW) of the model under test [44]

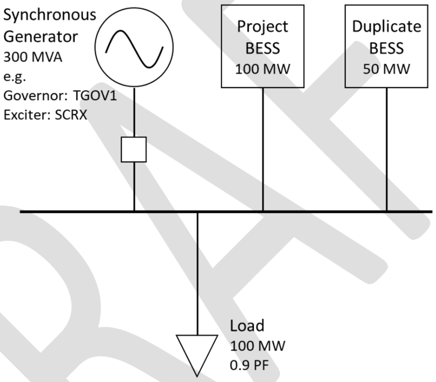


Figure 2.1: GFM Functional Test System[45]

The combined MVA rating of the BESS models must be sufficient to fully supply the load upon disconnection of the synchronous generator. The synchronous generator MVA rating must be sufficient to simultaneously serve the load and charge both BESS at their rated maximum charge power. Both BESS models should be in voltage control mode with the same voltage and frequency droop settings and set points. All protection settings in the BESS should reflect the equipment planned to be installed in the field; however, settings should be set as wide as possible within the equipment ratings and capabilities (as recommended in NERC reliability guidelines)[46] since the tests are intended to subject the GFM BESS to extreme frequency, voltage, and phase jump events.

Description of GFM Functional Tests and Success Criteria

Using simulated disturbances that only a GFM BESS meeting the functional specifications could survive, the following suite of GFM functional tests are designed to ensure that each proposed project meets the GFM BESS functional specifications as described in this document.[47] [48]

---

[42] For simulating the loss of the synchronous generator

[43] Constant impedance load model is used in the example tests described later in this chapter

[44] The purpose of adding the duplicate BESS is to consider control interaction between multiple GFM devices, including droop response and to provide flexibility in post event power balancing.

[45] BESS ratings and synchronous generator ratings are for example only.

[46] https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Reliability_Guideline-EMT_Modeling_and_Simulations.pdf

[47] TP/PC may require additional tests such as load rejection, faults, etc.

48 For example: Hawaiian Electric Facility Technical Model Requirements and Review Process, August 2022: https://www.hawaiianelectric.com/documents/clean_energy_hawaii/selling_power_to_the_utility/competitive_bidding/20210901_cbre_rfp/20210825_redline_lanai_appxb_att3.pdf

- **Test 1 – BESSs Initially Discharging and Ends at Higher Level of Discharging:** This test assesses the GFM BESS performance following the generator trip when operating within its limits and in discharging state.
- **Test 2 – BESS Initially Charging and Ends Discharging:** This test assesses the GFM BESS performance when operating within its limits and transitioning from charging state to discharging state after the generator trips.
- **Test 3 – BESS GFM Performance at Maximum Active Power:** This test assesses the GFM BESS performance following the generator trip when operating at or near its limits.

Each test is conducted using different initial operating conditions, as outlined in Table 2.1~~Table 2.1~~–Table 2.3~~Table 2.3~~. Once the system is stable at the given power flow conditions (without oscillations), the synchronous generator is disconnected. Each test then includes a set of pass/fail success criteria that *all* must be met. TPs/PCs should add additional qualitative or quantitative criteria specific to their own systems, as applicable. GFM BESS under test must pass all three tests to qualify as GFM. [49]

Formatted: Font: (Default) Calibri, Font color: Blue

Formatted: Font: Calibri, Font color: Blue

Although the tests require the BESS to be operated in the absence of any synchronous generation, many GFM BESS will never be operated that way. Regardless, the ability to survive such tests indicates that the controls have the necessary properties from GFM in grid-connected conditions. Conversely, if the resource is unable to meet the performance requirements in these tests, the controls will not have the desired characteristics for future BPS operating conditions.

These tests do not guarantee that the facility will be stable for a specific location on the grid. Interconnection studies are critical for ensuring reliable operation of the BPS for each specific interconnecting resource.[50] If settings change during interconnection studies, the model with the new settings should still pass these tests.

Test 1: BESSs Initially Discharging and Ends at Higher Level of Discharging

Table 2.1: Test 1 – Setup and Success Criteria	
Initial Dispatch	
• The project BESS is dispatched at 20% of its maximum discharge power limit. • The duplicate BESS is dispatched at 20% of its maximum discharge power limit	
Test Sequence:	
1. Run until the system is stable at the given power flow conditions, without oscillations. 2. Trip the synchronous generator.	
Success Criteria	
Pre-Trip:	**Pass/Fail**
a. BESSs active power outputs match dispatched levels.	
b. Synchronous generator active power output matches the rest of the load.	
c. Frequency should be 1 pu.	
d. Voltage at Bus 1 should be within 5% of nominal.	
e. Phase voltage and current waveform should not be distorted.	
f. There should not be oscillations in the RMS quantities.	

---

[49] GFL BESS can potentially form an island with load under very specific power flow and resonance conditions. Hence, it's important to subject the project model to all three tests.

[50] Other tests such as ride-through capability, voltage control, etc. are necessary to be conducted for all resources, including GFM and GFL.

Table 2.1: Test 1 – Setup and Success Criteria

g. Reactive power output from all devices should be within limits.	
Post-Trip:	**Pass/Fail**
a. Immediately following the trip, BESS output should be well controlled. System frequency and voltage should not oscillate excessively or deviate from steady state levels for any significant amount of time.	
b. Voltage settles to a stable and acceptable operating point.	
c. The final voltage is as expected based on the droop and deadband settings.	
d. Frequency settles to a stable operating point.	
e. The final frequency is as expected based on the droop and deadband settings.	
f. Any oscillation shall be settled.	
g. Any distortion observed in phase quantities should dissipate over time.	
h. Active power from each BESS should move immediately to meet the load requirement and settle according to its frequency droop setting.	
i. Reactive power from each BESS should move immediately and settle according to its voltage droop setting.	

Test 2: BESS initially charging and ends up discharging

Table 2.2: Test 2 – Setup and Success Criteria	
Initial Dispatch	
• The project BESS is dispatched at half of its maximum charge power limit. • The duplicate BESS is dispatched at half of its maximum charge power limit.	
Test Sequence:	
1. Run until the system is stable at the given power flow conditions, without oscillations. 2. Trip the synchronous generator.	
Success Criteria	
Pre-Trip:	**Pass/Fail**
a. BESSs active power outputs match dispatched levels.	
b. Synchronous generator active power output matches the ~~rest of the load~~load and BESS charging.	
c. Frequency should be 1 pu.	
d. Voltage at Bus 1 should be within 5% of nominal.	
e. Phase voltage and current waveform should not be distorted.	
f. There should not be oscillations in the RMS quantities.	
g. Reactive power output from all devices should be within limits.	
Post-Trip:	**Pass/Fail**
a. Immediately following the trip, BESS output should be well controlled. System frequency and voltage should not oscillate excessively or deviate from steady state levels for any significant amount of time.	
b. Voltage settles to a stable operating point	
c. The final voltage is as expected based on the droop and deadband settings.	
d. Frequency settles to a stable operating point	
e. The final frequency is as expected based on the droop and deadband settings.	
f. Any oscillation shall be settled.	
g. Any distortion observed in phase quantities should dissipate over time.	
h. Active power from each BESS should move immediately to meet the load requirement and settle according to its frequency droop setting.	
i. Reactive power from each BESS should move immediately and settle according to its voltage droop setting.	

Test 3: BESS GFM Performance at Maximum Active Power

Table 2.3: Test 3 – Setup and Success Criteria

Initial Dispatch	
• The project BESS is dispatched at 0 MW. • The duplicate BESS is dispatched at its steady state maximum discharge power limit.	
Test Sequence:	
1. Run until the system is stable at the given power flow conditions, without oscillations. 2. Trip the synchronous generator (no fault).	
Success Criteria	
Pre-Trip:	**Pass/Fail**
a. BESSs active power outputs match dispatched levels.	
b. Synchronous generator active power output matches the rest of the load.	
c. Frequency should be 1 pu.	
d. Voltage at Bus 1 should be within 5% of nominal.	
e. Phase voltage and current waveform should not be distorted.	
f. There should not be oscillations in the RMS quantities.	
g. Reactive power output from all devices should be within limits.	
Post-Trip:	**Pass/Fail**
a. Immediately following the trip, BESS output should be well controlled. System frequency and voltage should not oscillate excessively or deviate from steady state levels for any significant amount of time.	
b. Voltage settles to a stable operating point	
c. The final voltage is as expected based on the droop and deadband settings.	
d. Frequency settles to a stable operating point	
e. The final frequency is as expected based on the droop and deadband settings.	
f. Any oscillation shall be settled.	
g. Any distortion observed in phase quantities should dissipate over time.	
h. Active power from BESS 1 should move immediately to meet the load requirement and settle according to its frequency droop setting. Active power from BESS 2 should not exceed its max discharge power limit at steady state.[51]	
i. Reactive power from each BESS should move immediately and settle according to its voltage droop setting.	

Example Conducting GFM Functional Tests

To illustrate conducting the GFM functional tests, an OEM-provided GFM model, including a power plant controller model, was subjected to each test outlined above. Error! Reference source not found.~~Appendix B~~ provides additional

---

[51] BESS 2 output may exceed momentarily depending on the active power availability at the inverters.

examples of the GFM functional tests applied to a GFM model supplied by a different OEM. **Table 2.4** shows the BESS voltage and frequency droop settings used for these tests.

Table 2.4: BESS Voltage and Frequency Droop Settings for Example Tests

Parameter	Value
Voltage Droop	2% (on Qmax)
Frequency Droop	2% (on Pmax)
Frequency Deadband	0.03 Hz

Test 1: BESSs Initially Discharging and Ends at Higher Level of Discharging

The test system is initialized with power flow conditions shown in **Figure 2.2**. BESSs are discharging at a quarter of their maximum discharge site limit, with the synchronous generator servicing the rest of the load.

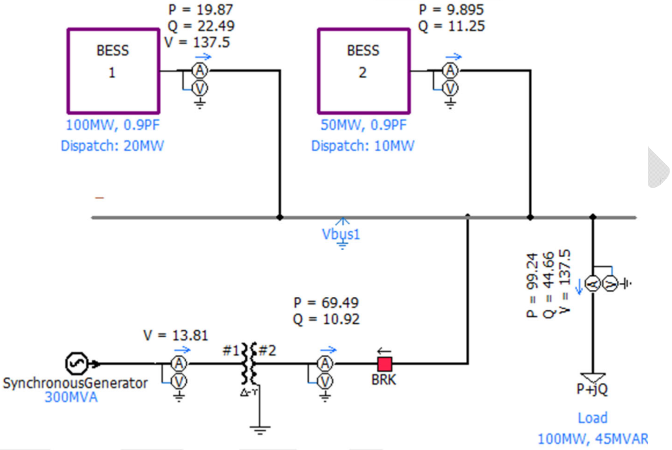


Figure 2.2: Example Test 1 – Initial Power Flow

Figure 2.3 shows the RMS quantities of the Test 1 simulation results including bus voltage (Vbus1_rms), frequency, active power (synchronous generator power (P_SyncGen), load power (P_Load), project BESS (BESS 1) power (P_BESS_1) and duplicate BESS (BESS 2) power (P_BESS_2)), reactive power, and current. The following observations are made:

- Near-instantaneous jump in active and reactive power from both BESS (see Point 1), followed by dynamics driven by specific GFM control topology and parameters.
- Minimal deviation in voltage thus resulting in small change in voltage-dependent load power (see Point 2)
- Final steady-state quantities (see Point 3 for values indicated by O-marker at *t = 40 sec* in **Figure 2.3**) can be verified against the droop parameters in **Table 2.4**.

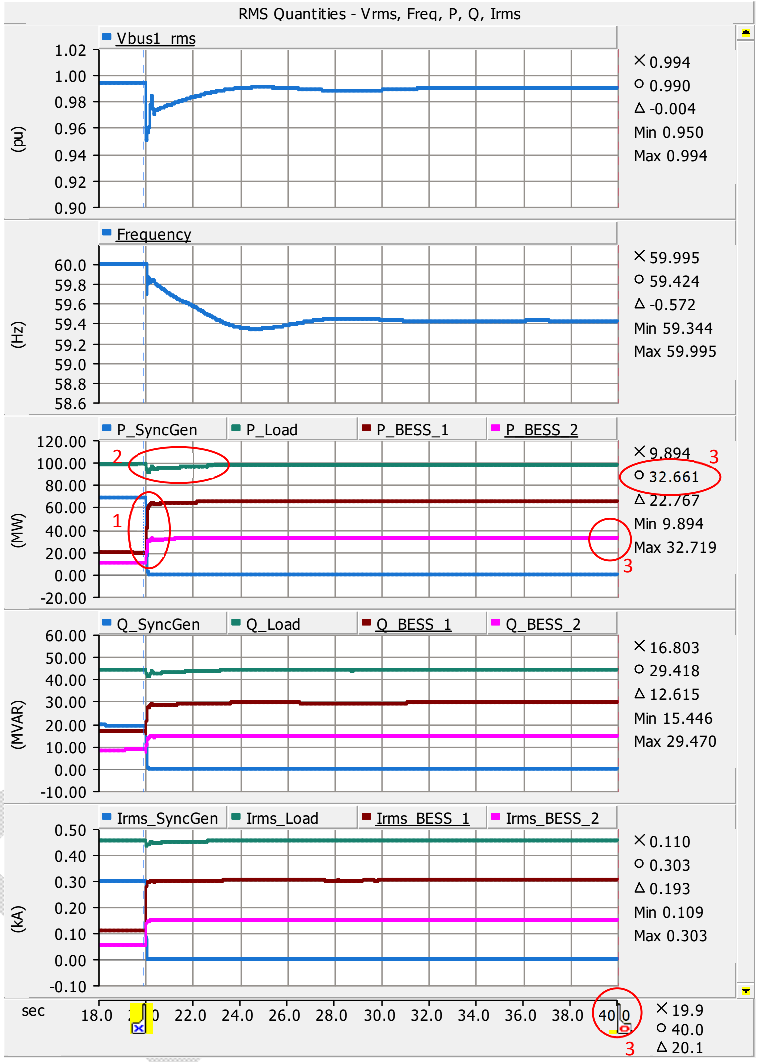


Figure 2.3: Test 1 Results – RMS Quantities

Figure 2.4 shows the instantaneous quantities of the Test 1 simulation results including bus voltage (Vbus1), synchronous generator current (I_SyncGen), load current (I_Load), BESS 1 current (I_BESS_1) and BESS 2 current (I_BESS_2), with the following observations made:

- Phase angle shift in bus voltage (see Point 1)
- Sub-cycle increase in BESS currents (see Point 2)
- Sub-cycle change in BESS current phase angle; this is more observable in the Test 2 results

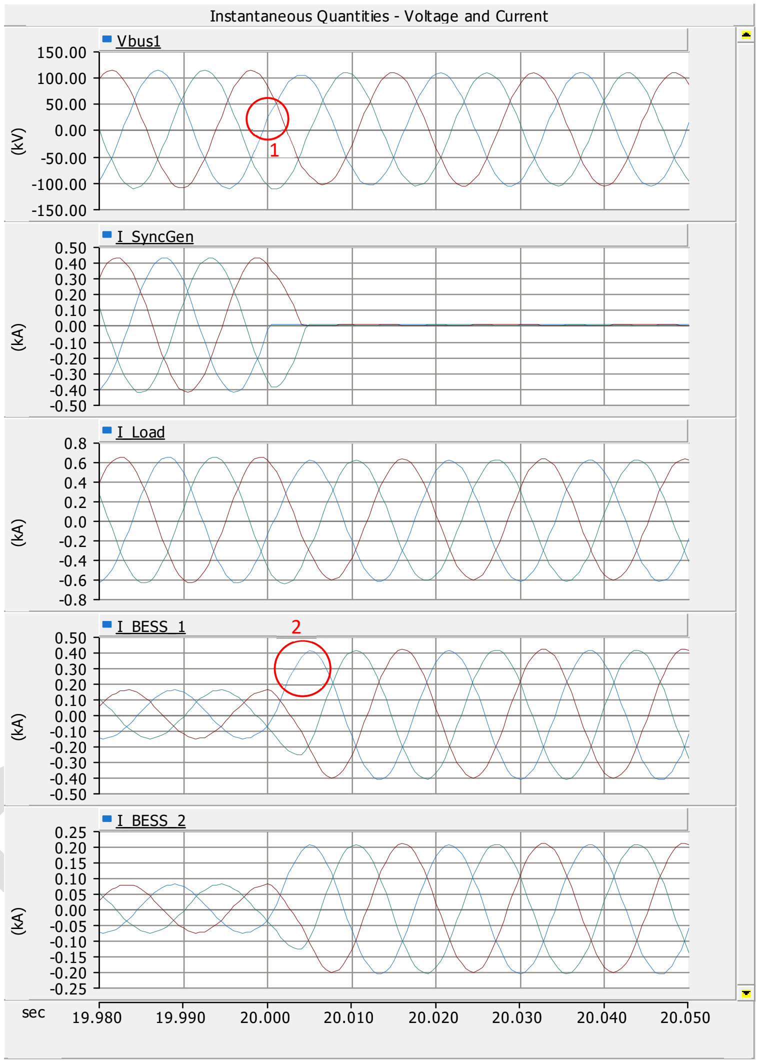


Figure 2.4: Test 1 Results – Instantaneous Quantities

As summarized in Table 2.5, the model passed Test 1.

Table 2.5: Evaluation of Test 1 Results

Pre-Trip:	**Pass/Fail**
a. BESSs active power outputs match dispatched levels.	Pass
b. Synchronous generator active power output matches the rest of the load.	Pass
c. Frequency should be 1 pu.	Pass
d. Voltage at Bus 1 should be within 5% of nominal.	Pass
e. Phase voltage and current waveform should not be distorted.	Pass
f. There should not be oscillations in the RMS quantities.	Pass
g. Reactive power output from all devices should be within limits.	Pass
Post-Trip:	**Pass/Fail**
a. Immediately following the trip, BESS output should be well controlled. System frequency and voltage should not oscillate excessively or deviate from steady state levels for any significant amount of time.	Pass
b. Voltage settles to a stable operating point	Pass
c. The final voltage is as expected based on the droop and deadband settings.	Pass
d. Frequency settles to a stable operating point	Pass
c. The final frequency is as expected based on the droop and deadband settings.	Pass
f. Any oscillation shall be settled.	Pass
g. Any distortion observed in phase quantities should dissipate over time.	Pass
h. Active power from each BESS should immediately move to meet the load requirement and settle according to its frequency droop setting	Pass
i. Reactive power from each BESS should move according to its voltage droop setting.	Pass

Test 2: BESS Initially Charging and Ends Discharging

The test system is initialized with power flow conditions shown in Figure 2.5. BESS are initially charging at half of their maximum charge rating, with the synchronous generator supplying power to the load and both BESS.

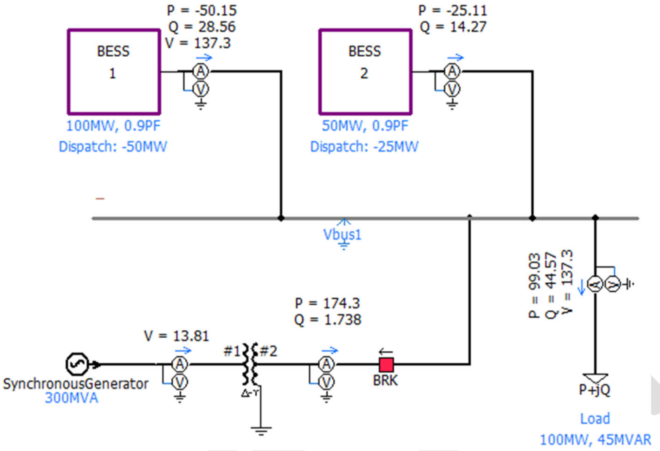


Figure 2.5: Example Test 2 – Initial Power Flow

In addition to similar observations as those from Test 1, the following can be noted in Figure 2.6 which shows the RMS quantities of the Test 2 simulation results.

- Due to the larger differences between initial output power level and final settled output power level, driven by load, the frequency settled to a greater deviation according to the frequency droop setting[52].
- Frequency spike (see Point 1) is an artifact of frequency measurement algorithm in response to the shift in voltage phase angle (see Point 1 in Figure 2.7).

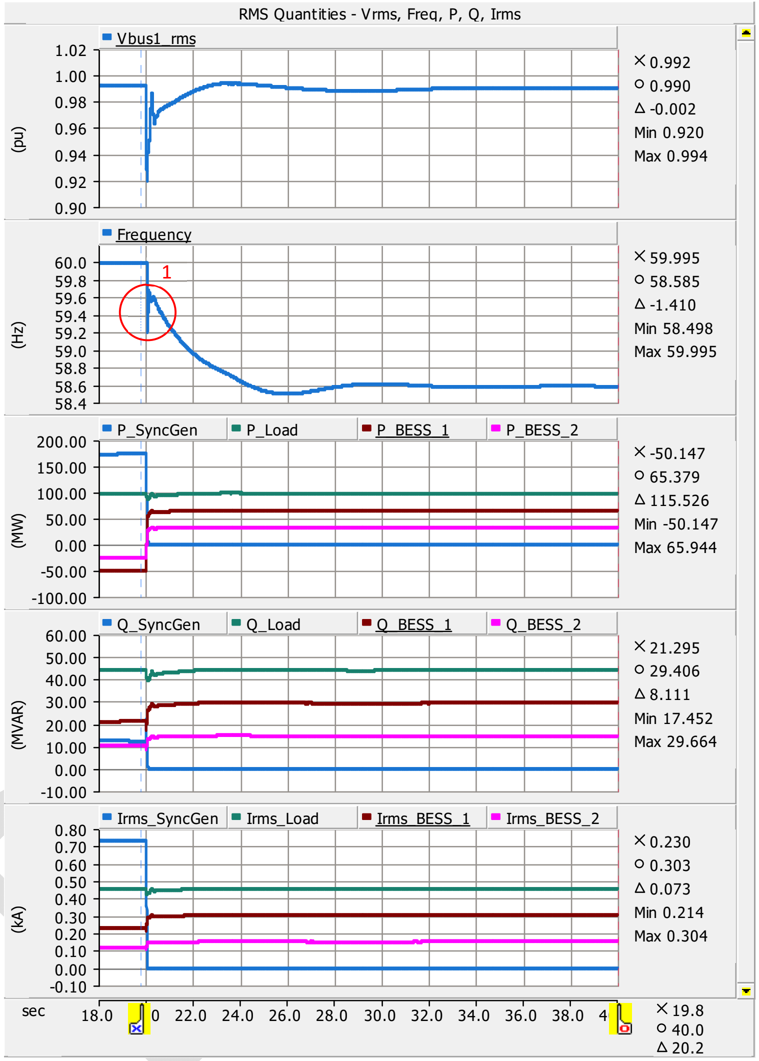


Figure 2.6: Test 2 Results – RMS Quantities

Figure 2.7 shows the instantaneous quantities of the Test 2 simulation results, with the following observations made:

- Current from both GFM BESS's increased within a quarter-cycle to make up for the loss of synchronous generator current (see Point 2)
- Change in BESS current phase angle as BESS's transition from charging to discharging within a quarter-cycle to serve the load (see Point 3)

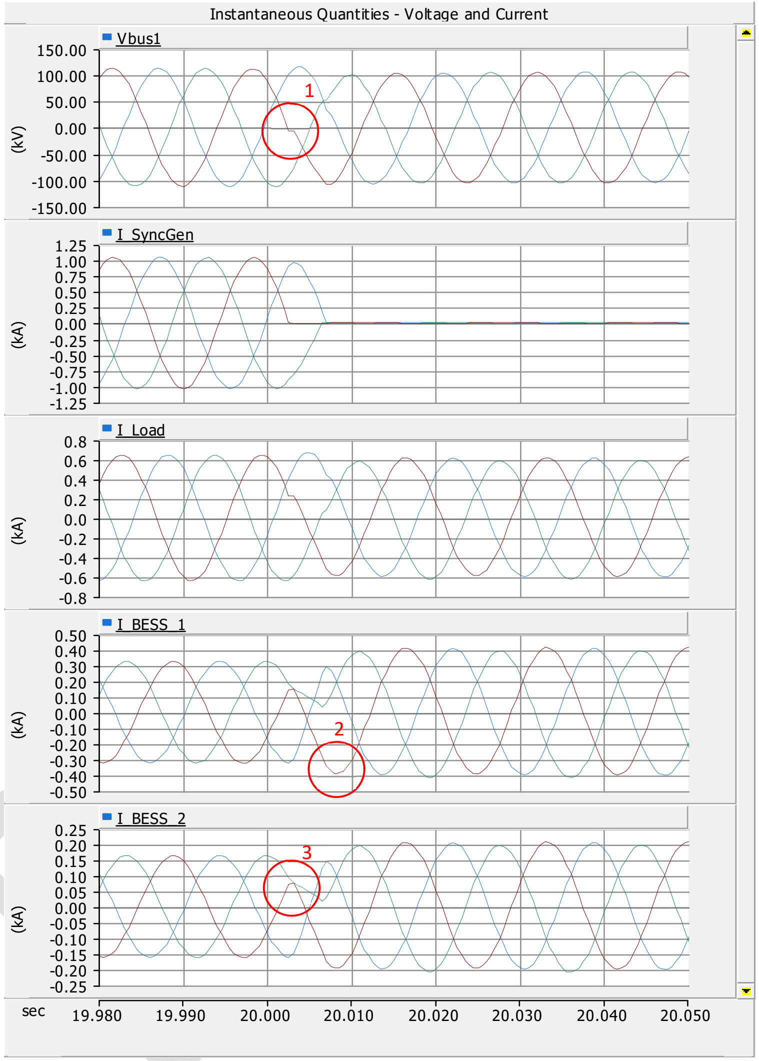


Figure 2.7: Test 2 Results – Instantaneous Quantities

As summarized below in **Table 2.6**, the model also passed Test 2.

Table 2.6: Evaluation of Test 2 Results

Pre-Trip:	**Pass/Fail**
a. BESSs active power outputs match dispatched levels.	Pass
b. Synchronous generator active power output matches the rest of the load.	Pass
c. Frequency should be 1 pu.	Pass
d. Voltage at Bus 1 should be within 5% of nominal.	Pass
e. Phase voltage and current waveform should not be distorted.	Pass
f. There should not be oscillations in the RMS quantities.	Pass
g. Reactive power output from all devices should be within limits.	Pass
Post-Trip:	**Pass/Fail**
a. Immediately following the trip, BESS output should be well controlled. System frequency and voltage should not oscillate excessively or deviate from steady state levels for any significant amount of time.	Pass
b. Voltage settles to a stable operating point.	Pass
c. The final voltage is as expected based on the droop and deadband settings.	Pass
d. Frequency settles to a stable operating point.	Pass
e. The final frequency is as expected based on the droop and deadband settings.	Pass
f. Any oscillation shall be settled.	Pass
g. Any distortion observed in phase quantities should dissipate over time.	Pass
h. Active power from each BESS should move immediately to meet the load requirement and settle according to its frequency droop setting.	Pass
i. Reactive power from each BESS should move immediately and settle according to its voltage droop setting.	Pass

Test 3: BESS GFM Performance at Maximum Active Power

The test system is initialized with power flow conditions shown in Figure 2.8. BESS 1 is dispatched to zero active power and BESS 2 is dispatched to its steady state maximum discharge site active power limit. The synchronous generator serves the remainder of the load.

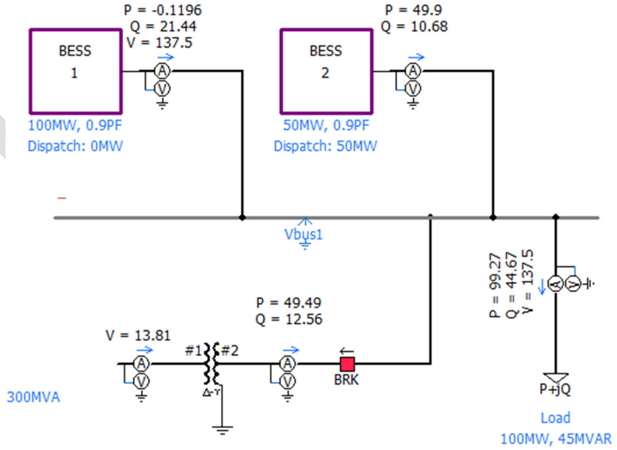


Figure 2.8: Example Test 3 - Initial Power Flow

Figure 2.9 shows the Test 3 simulation results with the following observations made that are unique to this test:

- BESS 2 (discharging at maximum active power) will not follow the droop curve past its maximum discharge power limit (see Point 1). BESS 1 makes up the active power difference to meet load demand, reaching the final frequency based on droop and deadband settings.[53]

---

[53] BESS 2 has extra power capability at the inverter level, allowing it to momentarily exceed site power limit.

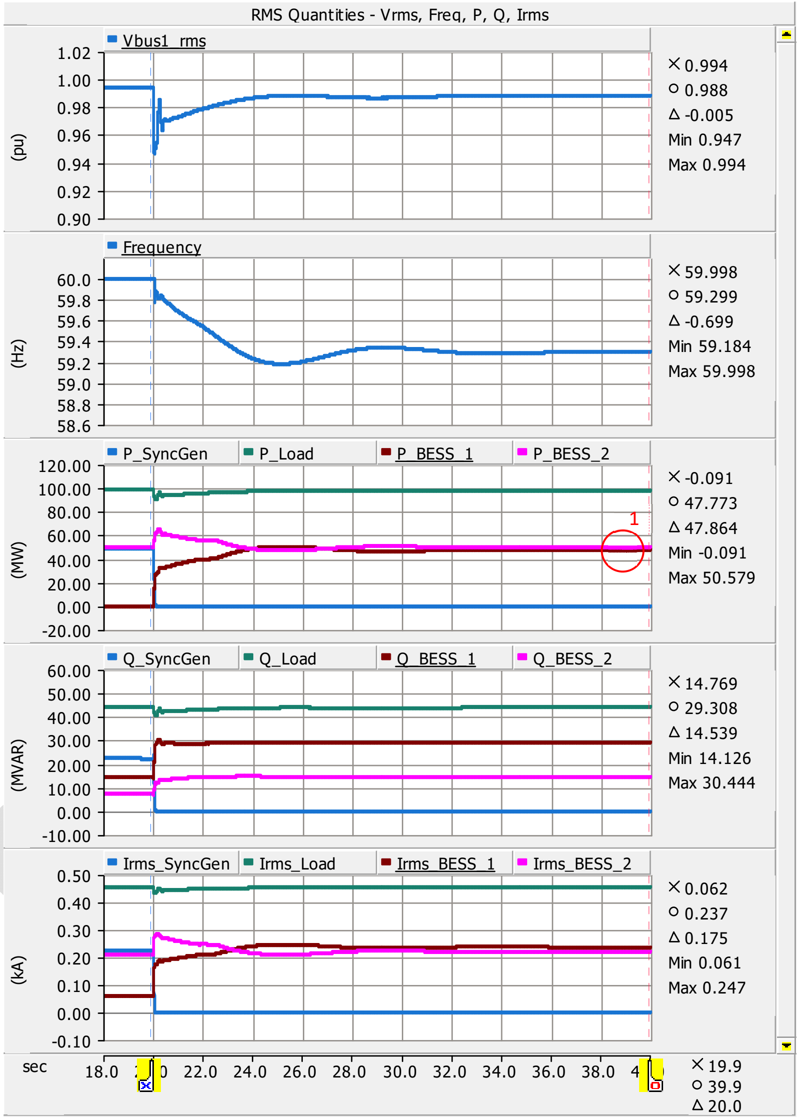


Figure 2.9: Test 3 Results – RMS Quantities

Figure 2.10 shows the instantaneous quantities of the Test 3 simulation results. Similar to the previous tests, it shows GFM BESS currents changed within a quarter cycle to match the load current (see Point 1).

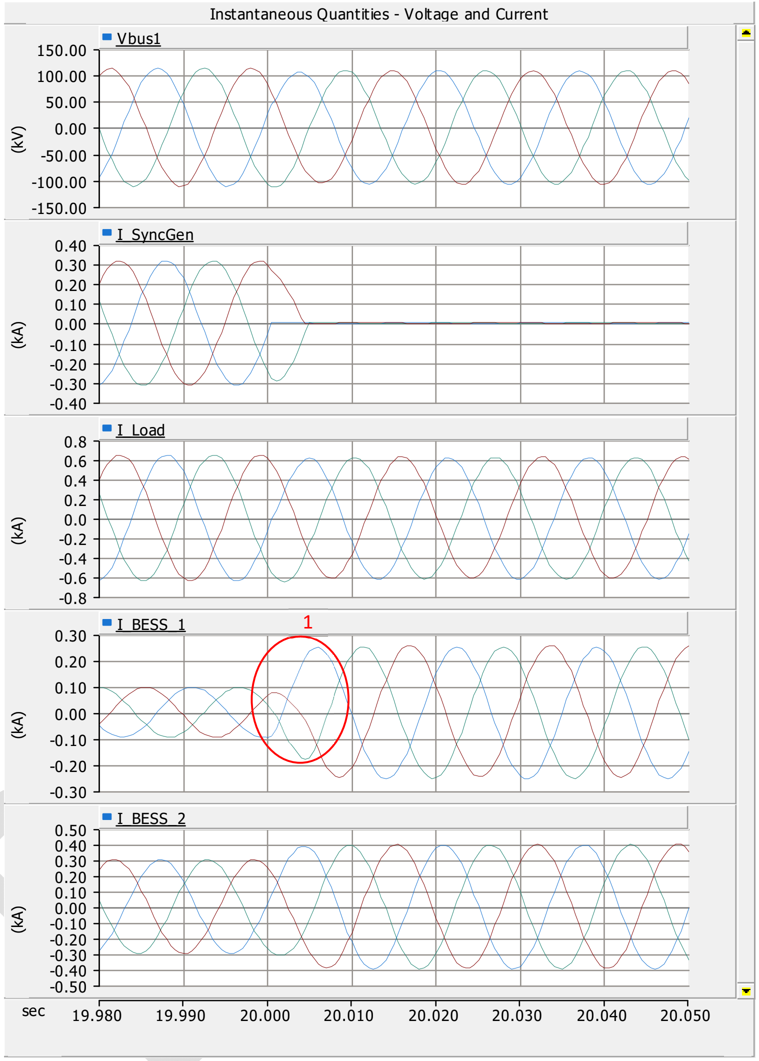


Figure 2.10: Test 3 Results – Instantaneous Quantities

As summarized below in **Table 2.7**, the model also passed Test 3.

Table 2.7: Evaluation of Test 3 Results

Pre-Trip:	**Pass/Fail**
a. BESSs active power outputs match dispatched levels.	Pass
b. Synchronous generator active power output matches the rest of the load.	Pass
c. Frequency should be 1 pu.	Pass
d. Voltage at Bus 1 should be within 5% of nominal.	Pass
e. Phase voltage and current waveform should not be distorted.	Pass
f. There should not be oscillations in the RMS quantities.	Pass
g. Reactive power output from all devices should be within limits.	Pass
Post-Trip:	**Pass/Fail**
a. Immediately following the trip, BESS output should be well controlled. System frequency and voltage should not oscillate excessively or deviate from steady state levels for any significant amount of time.	Pass
b. Voltage settles to a stable operating point.	Pass
c. The final voltage is as expected based on the droop and deadband settings.	Pass
d. Frequency settles to a stable operating point.	Pass
e. The final frequency is as expected based on the droop and deadband settings.	Pass
f. Any oscillation shall be settled.	Pass
g. Any distortion observed in phase quantities should dissipate over time.	Pass
h. Active power from BESS 1 should move immediately to meet the load requirement and settle according to its frequency droop setting. Active power from BESS 2 should not exceed its max discharge active power limit in steady state.	Pass
i. Reactive power from each BESS should move immediately and settle according to its voltage droop setting.	Pass

Illustration of GFM versus GFL Performance in Functional Tests

To illustrate the response of a grid following BESS for comparison with GFM, the same EMT model is put through Test 1 on the same test system *without* GFM functionality enabled. Note that frequency and voltage trip settings were widened to demonstrate the unstable behavior. **Figure 2.11** shows GFL failing Test 1 criteria and resulting in instability.

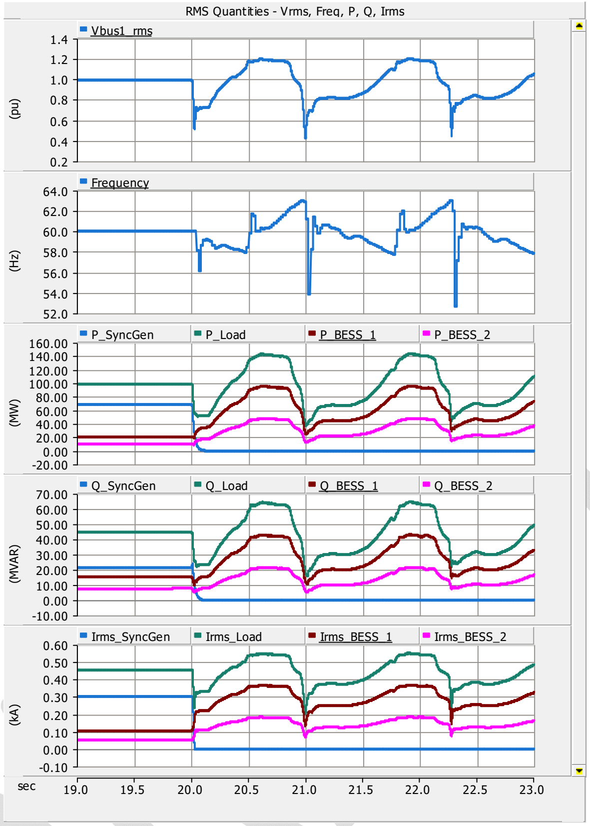


Figure 2.11: Test 1 Results with GFL

As summarized in **Table 2.8**, the BESS in GFL mode failed to settle to a steady state operating point, although the distortion in voltage and current waveforms are reasonable.

Table 2.8: Evaluation of GFL for Test 1

Pre-Trip:	**Pass/Fail**
a. BESSs active power outputs match dispatched levels.	Pass
b. Synchronous generator active power output matches the rest of the load.	Pass
c. Frequency should be 1 pu.	Pass
d. Voltage at Bus 1 should be within 5% of nominal.	Pass
e. Phase voltage and current waveform should not be distorted.	Pass
f. There should not be oscillations in the RMS quantities.	Pass
g. Reactive power output from all devices should be within limits.	Pass
Post-Trip:	**Pass/Fail**

Table 2.8: Evaluation of GFL for Test 1

a. Immediately following the trip, BESS output should be well controlled. System frequency and voltage should not oscillate excessively or deviate from steady state levels for any significant amount of time.	Fail
b. Voltage settles to a stable operating point	Fail
c. The final voltage is as expected based on the droop and deadband settings.	Fail
d. Frequency settles to a stable operating point	Fail
c. The final voltage is as expected based on the droop and deadband settings.	Fail
f. Any oscillation shall be settled.	Fail
g. Any distortion observed in phase quantities should dissipate over time.	Pass
h. Active power from each BESS should move immediately to meet the load requirement and settle according to its frequency droop setting.	Fail
i. Reactive power from each BESS should move immediately and settle according to its voltage droop setting.	Fail

Figure 2.12~~Figure 2.12~~ and Figure 2.13~~Figure 2.13~~ are zoomed in versions of Figure 2.11~~Figure 2.11~~to compare the GFL response (left) to GFM response (right). Notable differences include:

- Sub-cycle response in GFM current that GFL does not provide (see Point 1 in Figure 2.12~~Figure 2.12~~)
- Fast active and reactive power response from GFM that GFL does not provide (see Point 2 in Figure 2.13~~Figure 2.13~~)

Formatted: Font: Calibri, Font color: Blue

Formatted: Font: Calibri, Font color: Blue

Formatted: Font: Calibri, Font color: Blue

Formatted: Font: (Default) Calibri, Font color: Blue

Formatted: Font: (Default) Calibri, Font color: Blue

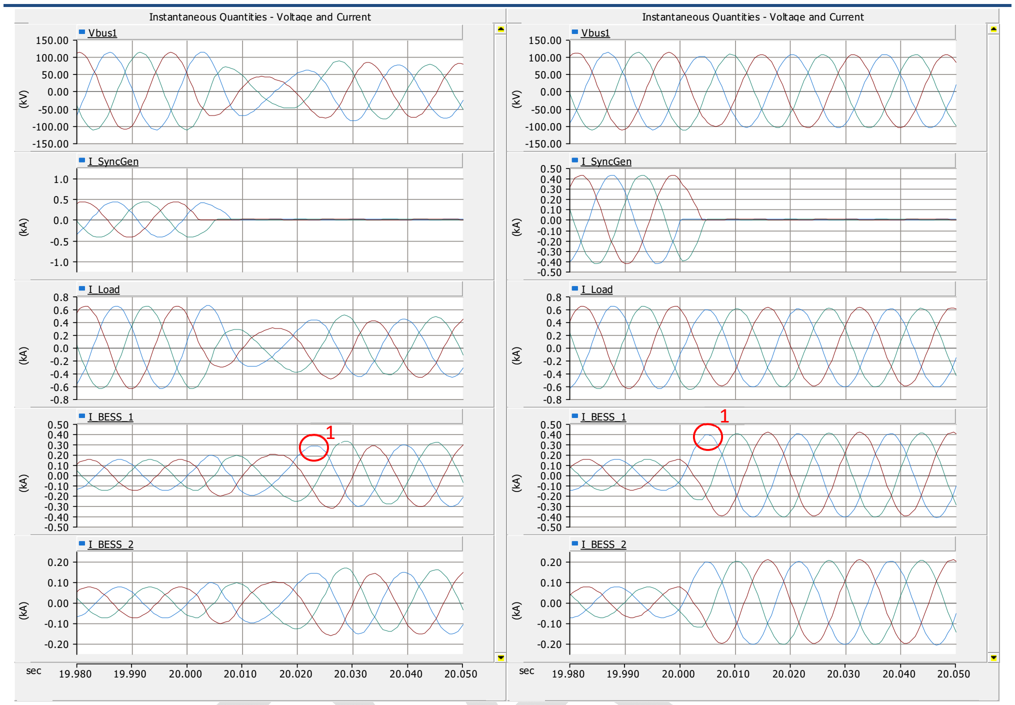


Figure 2.12: Comparison between GFL (Left) and GFM (Right) Responses – Instantaneous Quantities

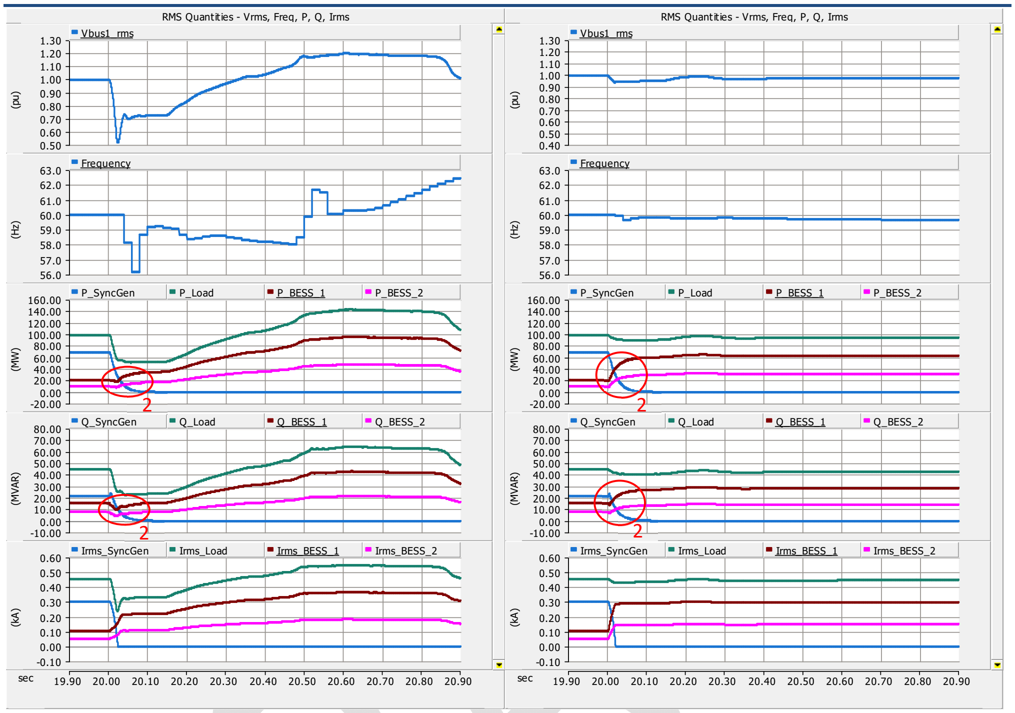


Figure 2.13: Comparison between GFL (Left) and GFM (Right) Responses – RMS Quantities

Formatted

Appendix A: Industry Experience with GFM Integration

This appendix shares industry experience with integrating and operating GFM BESS technology on the BPS around the world.

Forum Network Technology/Network Operation (FNN) Guideline

The German FNN institute has published a guideline[54] on GFM behavior of HVDC systems and dc-connected power plant modules in 2020. The guideline is a supplement to VDE-AR-N-4131.[55,56] The FNN guideline describes the dynamic active power–frequency behavior and dynamic voltage control without reactive current specification. It consists of a conformity verification procedure for GFM resources, which includes methods for specifying the reference behavior, test description (networks and scenarios) as well as validation criteria. GFM resources are characterized with an immediate response and "network-stabilizing behavior" expected to counteract system events. This guideline includes tests that cover:

- Phase angle steps of 10 and 30 degrees
- Linear frequency change with 2 Hz/s ROCOF during 0.5 seconds
- Voltage magnitude step of 5% and 10% within normal operational ranges
- Grid distortion including the presence of negative sequence (2% unbalance in one phase), harmonics (including ranks 2, 5, 7, 19 and 31), and low frequency subharmonics (at 5, 10 and 15.9 Hz)
- Changes in the network impedance leading to short circuit ratio reductions from 20 to 5, from 5 to 2, and from 2 to 1
- Islanding in an active network, with only load or including another GFM converter

Conformity verification is based on time varying reference "envelopes" that can be applied to instantaneous value signals giving special attention to the initial behavior up to the first peak. These signals can be obtained from field measurements, electromagnetic transient (EMT) simulations, or hardware in the loop (HIL) simulations. Verification can include recalculated quantities to be determined over a certain time period such as active and reactive power. Conformity proof includes delivery of a technical verification report and a digital model with the installation manual and benchmark report.

Massive Integration of Power Electronic Devices (MIGRATE)

The European Union-funded MIGRATE project provides requirements for upcoming IBR-dominated power systems to maximize IBR penetration levels while maintaining stability and reliability.[57] In 2019, MIGRATE proposed high-level definition of GFM functions including:

- Behave as a voltage source
- Be synchronized with other grid forming sources
- Operate in standalone after seamless islanding
- Limit output current magnitude (preserving voltage source behavior and preferably avoiding control switches during voltage dips, for instance)
- Be compatible with all devices connected on the system, especially synchronous machines and GFL IBRs

---

[54] VDE/FNN Guideline: Grid forming behavior of HVDC systems and DC-connected Power Plant Modules, August 2020: https://shop.vde.com/en/fnn-guideline-hvdc-systems-2

[55] VDE is the Europe's largest technical scientific associations Verband der Elektrotechnik

[56] Technical Connection Rule for the connection of HVDC systems and generation plants connected via HVDC systems

[57] PowerPoint-Präsentation (h2020-migrate.eu)

Additionally, within this project a number of studies were carried out demonstrating compatibility of GFM IBRs with various control types operating in parallel in a fully IBR system.

European Network of Transmission System Operators for Electricity (ENTSO-E) Report

ENTSO-E published *High Penetration of Power Electronic Interfaced Power Sources and the Potential Contribution of Grid Forming Converters*[58] defining seven properties of a GFM inverter:

- Creates system voltage (does not rely on being provided with firm clean voltage)
- Contributes to fault level (positive and negative sequence within first cycle)
- Contributes to total system inertia (limited by energy storage capacity)
- Supports system survival to allow effective operation of low frequency demand disconnection (LFDD) for rare system separations
- Controls act to prevent adverse control system interactions
- Acts as a sink to counter harmonics and inter-harmonics in system voltage
- Acts as a sink to counter unbalance in system voltage

While the MIGRATE definition focuses on capabilities regarding standalone operation and synchronization, the ENTSO-E paper adds a response deployment dimension.

Great Britain Grid Code GC0137

Grid Code GC0137 *Minimum Specification Required for Great Britain GFM Capability*[59] was approved and published in February 2022. This grid code was applied by National Grid Electricity System Operator (NGESO) to address grid stability issues arising from increasing penetration of IBRs. Although the requirements are non-mandatory, the provider of GFM IBRs will declare how much capability is available so that these GFM IBRs could be selected and remunerated for those capabilities.[60] Successful implementation of this grid code would provide additional grid stability services by these GFM resources. To help relevant IBR stakeholders understand the GFM requirements, NGESO released the *GBGF Best Practice Guide*[61] in April 2023. GFM IBRs are expected to provide the same type of performance as synchronous generator to:

- Limit the rate of change of system frequency
- Inject instantaneous active power and instantaneous fast fault current into the grid
- Contribute to damping power
- Limit vector shift
- Contribute to synchronizing torque
- Contribute to voltage performance during a fault

GC0137 specifies the following minimum technical, design, and operational capability for GFM IBRs:

- Withstand 2 Hz/sec ROCOF over a rolling 500 ms period

---

[58] https://euagenda.eu/upload/publications/untitled-292051-ea.pdf

[59] GC0137 Authority Decision (ofgem.gov.uk)

[60] https://www.nationalgrideso.com/industry-information/codes/grid-code/code-documents

[61] https://www.nationalgrideso.com/document/278491/download

- Operate at a minimum short circuit level of zero MVA at the grid interconnection point
- Fast short circuit current injection on both magnitude (typical 1 pu or 1.5 pu at zero voltage) and response speed (start in 5 ms and full in 30 ms)
- Active power responds to changes in the grid at bandwidths below 5 Hz to avoid ac system resonance problems
- Provide damping factor between 0.2 and 5.0

UK Stability Pathfinder

While a market for GFM capability is under development, NGESO needs some of the stability services such as improved system strength and inertia in certain locations today. Currently those are being procured through a series of tenders called Stability Pathfinder.[62] Phase 1 was only open to synchronous solutions and awarded to a number of synchronous condensers. Phase 2 was open to new technologies and five GFM BESS projects[63] were awarded in April 2022 with in-service dates between March 2024 and April 2026. These projects must comply with the requirements set forth in GC0137. Stability Pathfinder tenders are an exploratory temporary solution for broader procurement of stability services from a variety of capable technologies. NGESO is currently in the process of designing a market for new stability services, which will allow to them to procure additional stability services through a market mechanism.

Optimal System Mix of Flexibility Solutions for European Electricity (OSMOSE)

EU-funded project OSMOSE Deliverable 3.3 *Analysis of Synchronization Capabilities of BESS Power Converters*[64] was released in March 2022, defining GFM minimum technical capabilities, technical requirements to formulate these capabilities, and recommendations to add these requirements into European-level and national grid codes. According to this specification, GFM units shall within its rated power and current be capable of self-synchronization, standalone operation, and provide synchronization services. The GFM capabilities shall include:

- Standalone operation
- Synchronizing active power (in response to phase-jump)
- Inertial response (immediate active power output following a frequency change)
- System strength (immediate reactive power output in response to grid voltage variation)
- Fault current (immediate current output within installation capabilities following voltage dips, active/reactive current sharing during the first instances of the fault dependent on system impedance (not control action), during asymmetrical voltage dips prioritization between positive and negative sequence current can be defined by a system operator.)

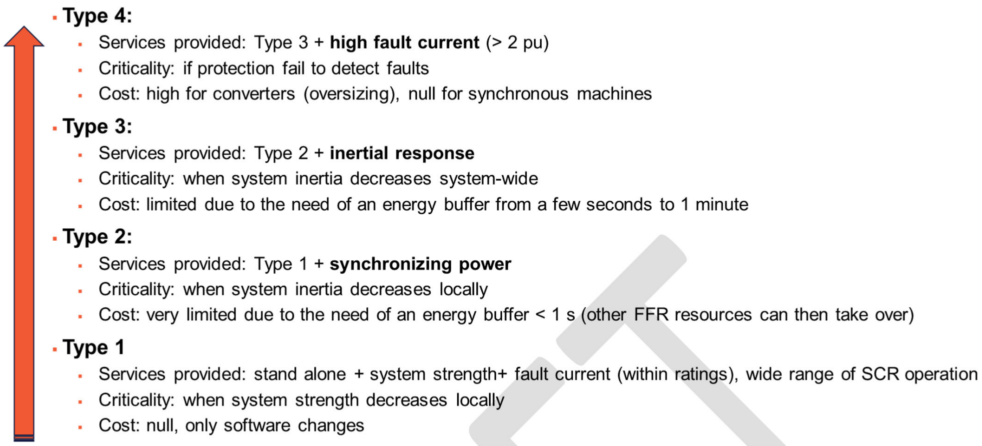
The report proposed separating GFM resources into four types based on the capabilities shown in **Figure A.1**.

---

[62] https://www.nationalgrideso.com/future-energy/projects/pathfinders/stability

[63] Stability Phase 2 Master Results Final with Tech Type.xlsx (live.com)

[64] https://www.osmose-h2020.eu/wp-content/uploads/2022/04/D3.3-Analysis-of-the-synchronisation-capabilities-of-BESS-power-converters.pdf



- **Type 4:**
  - Services provided: Type 3 + **high fault current** (> 2 pu)
  - Criticality: if protection fail to detect faults
  - Cost: high for converters (oversizing), null for synchronous machines
- **Type 3:**
  - Services provided: Type 2 + **inertial response**
  - Criticality: when system inertia decreases system-wide
  - Cost: limited due to the need of an energy buffer from a few seconds to 1 minute
- **Type 2:**
  - Services provided: Type 1 + **synchronizing power**
  - Criticality: when system inertia decreases locally
  - Cost: very limited due to the need of an energy buffer < 1 s (other FFR resources can then take over)
- **Type 1**
  - Services provided: stand alone + system strength+ fault current (within ratings), wide range of SCR operation
  - Criticality: when system strength decreases locally
  - Cost: null, only software changes

Figure A.1: Type of Grid Forming Resources as proposed by OSMOSE project[65]

A delineation is made in the report between capabilities that can only be provided by GFM resources versus capabilities that can also be provided by GFL resources (e.g., power oscillation damping, provision of negative sequence current, phase jump withstand capability, harmonics mitigation). The paper defined synchronization services and concluded that due to criticality and geographic dependence, some of these services need to be required at the time of interconnection from all new large transmission-connected IBRs and some additional services should be required from new transmission-connected BESS. It was recognized that synchronous machines may be needed in the interim to provide additional short circuit current or, alternatively, higher overcurrent capability of IBRs can be incentivized.

UNIFI Consortium

The Universal Interoperability for Grid-Forming Inverters (UNIFI) Consortium is a US Department of Energy-funded effort to advance GFM technology. The consortium developed the first version of a set of specifications that outline plant- and unit-level performance requirements for GFM technologies.[66] These specifications are intended to facilitate the integration and seamless operation of GFM resources, particularly unifying their operation smoothly with synchronous generators. The purpose of the UNIFI specifications for GFM IBRs is to provide uniform technical requirements for the interconnection, integration, and interoperability of GFM IBRs of any size in electric power systems of any scale. These specifications establish functional requirements and performance criteria for integrating GFM IBRs in power systems at any scale which includes GFM devices used as the local load, in microgrid, distribution, and transmission system. These specifications cover all GFM technologies including, but not limited to: battery storage, solar PV, wind turbines, HVDC, STATCOM, UPS, supercapacitors, fuel cells, or other yet to be invented technologies. While each GFM resource have different DC side and energy limitations, the specifications focus on the ac side performance requirements.

This UNIFI specifications cover both normal and contingency operation conditions. Under normal operation conditions, performance requirements for GFM include (but are not limited to) autonomous voltage and frequency support of the grid, active and reactive power sharing, robust operation in low system strength grid, and unbalancing

---

[65] Adapted from Carmen Cardozo's OSMOSE project presentation at 2022 ESIG GFM Workshop: https://www.esig.energy/event/2022-special-topic-workshop-grid-forming-ibrs/

[66] B. Kroposki, et. al, "UNIFI Specifications for Grid-forming Inverter-based Resources – Version 1," UNIFI Consortium, UNIFI-2022-2-1, December 2022 [Available at: https://sites.google.com/view/unifi-consortium/publications]

grid operation support of. In contingency operation conditions, performance requirements for GFM include (but are not limited to) fault ride-through behavior, response to asymmetrical faults, response to phase jumps, and intentional islanding event. The requirements are considered to be the minimum capability from GFM resources; additional capabilities such as blackstart capability and short-term over current capability are also covered in the specifications.

ESIG Grid Forming White Paper and Workshop

The Energy Systems Integration Group (ESIG) published a technical report on GFM technology in March 2022.[67] The report covered the following topics

- GFM versus GFL inverter basic principles and an overview of types of GFM controls
- How BPS needs are changing with increasing penetrations of IBRs and the trade-offs between system needs and resource needs
- System services provided by GFM and technical requirements around the world, specifically around breaking the "chicken-and-egg" problem regarding deployment of GFM and requirements/incentives
- Advanced characterization and testing of GFM resources, including field tests
- Simulation tools needs (stability, analytics, economics, etc.) and the need for compatibility
- Recommendations for GFM technology moving forward

ESIG also held a technical workshop dedicated to GFM technology in June 2022, structured around steps needed to solve the "chicken-and-egg" issue around GFM technology deployment.[68] Topics addressed system operator experience with high shares of IBRs, OEMs with commercial GFM products, research and development in this space, and the low-hanging fruit of enabling GFM in BESS to provide core GFM capabilities (excluding high overcurrent and blackstart capability). Key points highlighted that commercial offerings for GFM BESS are already available today from multiple OEMs; however, the absence of clear GFM requirements is leading to customized site-specific applications that drive higher implementation costs. It was also recommended to distinguish between equipment specification/minimum capability requirements and system needs/services.

Finland ~~Grid Code Specification~~Specific Study Requirements for Grid Energy Storage System

A large number of BESS are planned to connect to the transmission grid in Finland. Studies have shown that ~~grid following (~~GFL~~) inverter-based resources (~~IBR~~)~~ are not able to operate in stable manner when the share of the ~~converters~~ IBRs is increasing in the future. The solution is to use GFM ~~controlled~~ IBRs to compensate for the reduction of synchronous generation and improve external system strength required by present GFL inverters to function properly. The need ~~of~~ for GFM control ~~is~~ has been ~~becoming obvious verified~~identified already ~~now~~ in weak grid regions, where connection of more GFL ~~inverters~~ IBRs is not possible without further grid strengthening. As a result, Fingrid defined Specific Study Requirements for BESS (30 MW, ≥110 kV) connected to the specific locations.~~,~~ where use of GFM controls is seen as necessary. The document describes functional requirements, modeling requirements, simulation studies and field tests for GFM BESS.

According to Fingrid requirements, GFM IBR shall be able to self-synchronize, operate in stand-alone mode and provide synchronization services: synchronizing power, system strength, fault current and virtual inertial response (within current inverter rating). The requirements are in addition to existing grid code specifications for energy storage systems, in case of conflict, GFM requirements prevail.

---

[67] https://www.esig.energy/grid-forming-technology-in-energy-systems-integration/

[68] https://www.esig.energy/event/2022-special-topic-workshop-grid-forming-ibrs/

Switching to GFL mode from GFM mode at the current limit is not permitted, when the GFM BESS is reaching the current limit, stability and grid support must still be maintained. GFM BESS shall continue providing GFM operational characteristics even at its highest and lowest allowable state of charge.

GFM shall provide autonomous, near-instantaneous frequency and voltage support by maintaining a nearly constant internal voltage phasor in the sub-transient time frame, including:

- Phase jump performance: resist near-instantaneous voltage phase angle change in sub-transient time frame
- System strength: resisting the change in voltage magn~~g~~itude in the sub-transient time frame
- Seamless transition between islanded operation and grid-connected operation
- Positive damping: GFM shall present a positive resistance to the grid within frequency ranges 0–47 Hz and 53-250 Hz to prevent adverse interactions.

GFM BESS shall provide a closed loop path for unbalanced current to flow, i.e. GFM shall present negative sequence current to ensure that its internally generated voltage remains balanced during normal operation and disturbances.

The specification includes additional clarifications on how existing active power/frequency control and reactive power/voltage control requirements for BESS should be interpreted for GFM BESS.

Similarly to HECO requirements, the document provides a table with the list of disturbances to be tested & acceptance criteria, simulation software and BESS operating scenarios (prescribed values of SOC, P and Q). The list also includes loss of last synchronous generator in test network model, identical to the one recommended in this document, ~~Section XX~~Test 3 in C~~c~~hapter 2.

In addition to software simulations, hardware type test reports are required. The document also provides the list of site tests such as for phase jump, island operation (upstream 110 kV breaker is opened), measurement of power quality, accompanied with high level acceptance criteria.

Fingrid finalized and sent the requirements to their customers in June 2023. They requirements will be ~~published~~ posted on Fingrid's website after summer holidays in beginning of August 2023[69]~~, here~~. ~~https://www.fingrid.fi/en/grid/grid-connection-agreement-phases/grid-code-specifications/grid-energy-storage-systems/~~

Field Code Changed

Currently the plan is to require GFM capabilities from BESS that interconnected to ~~parts of~~ the grid with high penetration of ~~inverters~~IBRs. Fingrid plans to gather more experience from the current GFM projects and aims to make it a general requirement for all BESS ~~systems~~ projects next year.

AEMO GFM Voluntary Specification

AEMO published Voluntary Specification for Grid-forming Inverters in May 2023[70]. The document ~~to~~ provides guidance to stakeholders while the regulatory environment around GFM technology develops. The definition of GFM IBR provided by AEMO is similar to that from NERC.

Similarly to UNIFI, it specifies the 'core' GFM capabilities, which require only a small energy buffer and can be delivered through control changes and 'additional' GFM technical capabilities that require a large energy buffer through hardware or operational practices change as well as over current capably. It is recognized that not all GFM inverters need to provide 'additional' capabilities, but these capabilities are valuable for secure operation of a power system with high share of IBRs.

The core requirements include:

---

[69] https://www.fingrid.fi/en/grid/grid-connection-agreement-phases/grid-code-specifications/grid-energy-storage-systems/

[70] https://aemo.com.au/-/media/files/initiatives/primary-frequency-response/2023/gfm-voluntary-spec.pdf?la=en&hash=F8D999025BBC565E86F3B0E19E40A08E

Field Code Changed

Field Code Changed

Field Code Changed

- Nearly-instantaneous (< 5 ms) **reactive response to an external voltage magnitude step**, to oppose the change in grid voltage.
- Nearly-instantaneous **active power response to a voltage phase angle step**, by injecting or absorbing power to oppose the change in phase angle.
- **Inertial response** from GFM inverters should be inherent (no calculation of frequency), providing a near-instantaneous active power response to a grid disturbance (e.g. load or generation trip). If the inertia is configurable, it needs to be tuned based on network conditions and requirements (high inertia constant may increase risk of power oscillations, particularly in strong systems).
- The response when the inverter is at a limit, and in transition to and from a limit condition, must be smooth and stable.
- The behavior at a limit should not be detrimental to stability and to harmonic performance (for example, clipping of current waveforms).
- **Surviving Loss of Last Synchronous Machine (SM)**: operate stably in a grid without any other GFM inverters or SMs; remain stable for a transition from a grid with SMs to one without (and back); provide frequency and reactive support, unaffected by these transitions. All of that, provided that the resultant state of the system is within the operating envelope of the GFM inverter.
- **Operate stably under a very low short circuit ratio**, as defined by the system operator; provide system strength support to nearby GFL inverters during and after disturbances.
- **Provide positive damping for oscillations**: following a disturbance GFM inverter output should be adequately damped; add damping to the system for the oscillatory phenomena listed in the document.

'Additional' capabilities include higher current capability above the continuous rating, larger headroom and energy buffer and power quality improvements.

AEMO is currently working on the development of a test plan and metrics for each of the qualitative capabilities to quantify requirements and to demonstrate that a device meets the specifications, to be published in 2024. The next step will be development of methodology to account for contributions from GFM devices in planning studies (as some contributions are dependent on the operating point).
~~https://aemo.com.au/-/media/files/initiatives/primary-frequency-response/2023/gfm-voluntary-spec.pdf?la=en&hash=F8D999025BBC565E86F3B0E19E40A08E~~

Field Code Changed

Field Code Changed

ERCOT Assessment of GFM Energy Storage Resources

~~ERCOT "Preliminary assessment of GFM IBR Energy Storage Resources (GFM-IBR-ESR) in the ERCOT Grid".~~

Recent notable events in ERCOT (Odessa 1 in 2021 and Odessa 2 in 2022) have shown the need to strengthen the system and resilience necessary to mitigate the reliability risk. ERCOT continues to focus on improving IBRs' capability and performance combined with improvements on the transmission system, recognizing that both are needed to maintain the reliable operations of the ERCOT grid. Therefore, ~~-~~alongside the adoption of NERC reliability guidelines, IEEE 2800 ride-~~-~~through requirements and recent recommendation for six new synchronous condensers to strengthen West Texas grid, additional improvements ~~of IBRs control~~ will be needed to support the continued growth of IBRs in the ERCOT grid.

Increasing industry interest in GFM controls for improvement of IBR performance and system support have prompted ERCOT to evaluate the potential application of GFM Energy Storage Resources (ESR)[71] in ERCOT grid. The results were

---

[71] Energy Storage Resource (ESR) is a defined term in ERCOT

presented at the ERCOT Inverter-Based Resource Working Group[72] on 8/11/2023. ~~https://www.ercot.com/calendar/08112023-IBRWG-Meeting-_-Webex (see presentation slides under Key Documents)~~

Field Code Changed

ERCOT preliminary GFM ESR evaluation focused on three scenarios:

- Scenario 1: a weak grid condition, a simple test case that mimics known stability challenges in ERCOT (in phasor domain)
- Scenario 2: West Texas grid based on 2022 Q4 Quarterly Stability Assessment case (in phasor domain):
  - West Texas IBRs were dispatched at 55%,
  - Include 22 ESRs (existing and planned) with ~2000 MVA capacity behind West Texas Export transmission constraint, all batteries were modelled as GFL first and then as GFM
  - Include potential new condensers in six locations in West Texas.
- Scenario 3: an actual ERCOT local area (138 kV) with identified stability constraints (tested in both phasor domain and EMT).

Two ~~generic positive sequence~~ GFM IBR~~ESR~~ dynamic models used in these tests were ~~supported~~ developed by Pacific Northwest National Laboratory (PNNL) and Electric Power Research Institute (EPRI)[73]. Both models showed similar performance in the study. ERCOT's ~~preliminary~~ assessment results from all three scenarios indicate thate GFM ESRs could be a viable option to improve system dynamic responses, but require headroom or energy buffer to provide adequate GFM support, proper control setting tuning and coordination. As the next step ERCOT will work on the GFM ESR requirements including but not limited to performance, models, studies, and verification. ERCOT expects GFM ESR to be capable of meeting IEEE 2800 and existing ERCOT requirements along with additional performance requirements specific to GFM.

GFM BESS Projects around the World

BPS-connected GFM BESS are commercially available from different OEMs and projects are quickly growing around the whole world.[74] Some of the major GFM BESS projects are summarized here.

Kauai Experience

Kauai Island Utility Cooperative (KIUC) has had the BESS portion of a 13 MW ac-coupled solar PV+BESS plant operating in GFM mode since 2018, which is a significant portion of the 70 MW system peak load. Field experience has shown the plant to operate stably during grid disturbances while providing instantaneous response to frequency and voltage events, avoiding load shedding and possible system outages.

Since April 2022, portions of a second solar PV+BESS plant on Kauai were converted to GFM mode. The second plant is a 14-MW dc-coupled solar PV+BESS plant that uses a different GFM control technique than the first plant. As of August 2022, the second plant now has all inverters in GFM mode. No adverse interactions between the two GFM plants have been observed in the field to-date.[75]

Both GFM plants have been shown to operate stably at all hours of the day, including times when the system is dominated by synchronous generation and times when it is dominated by inverter-based generation (including one other 30 MW GFL solar PV+BESS plant, three other large (6–12 MW) solar PV plants and about 45 MW of aggregate behind-the-meter solar PV). System inertia constant ranges from about 0.5 MW-s/MVA to 2.7 MW-s/MVA (using total online capacity as the MVA base), and the percent of generation from IBRs ranges from about 6% to 95%. KIUC

---

[72] https://www.ercot.com/calendar/08112023-IBRWG-Meeting-_-Webex (see presentation slides under Key Documents)

Field Code Changed

[73] PNNL's and EPRI's GFM IBR models were provided both in EMT and positive sequence.

[74] ESIG-GFM-batteries-brief-2023.pdf

[75] https://www.youtube.com/watch?v=2e5ET0L1j5g

intends to continue operating both plants in GFM mode going forward and may add additional GFM generation in the future.

No EMT model of the KIUC system was available at the time of either of the two GFM plants' commissioning, so EMT studies were not conducted; instead, issues were addressed by monitoring the plants' performance in the field and working with the plant owners to make control parameter adjustments where necessary. Digital fault recorder data has been crucial for plant performance monitoring. The inverter model for the second plant described was tested extensively at NREL in partnership with the plant owner prior to commissioning and again prior to conversion to GFM.

HECO Experience

Hawaiian Electric (HECO) conducted extensive EMT studies of GFL and GFM solar PV+BESS and stand-alone BESS plants.[76] Studies showed that GFM controls are crucial to stability of the HECO system in the near future.[77] The first GFM plant in HECO is expected to come online in 2023 with several more to follow in subsequent years. As part of HECO's preparation, they also worked with NREL to test a 2.2 MVA BESS inverter's performance by using power hardware-in-the-loop (PHIL) simulation to connect it to a real-time EMT simulation of Maui's near-future transmission system.[78] The commercially available inverter tested at NREL can operate in GFM or GFL mode. It was used to represent a planned 30 MVA facility. The PHIL tests established that with the hardware inverter in conventional GFL mode, the Maui transmission system is unstable in certain very low inertia dispatch scenarios. They then demonstrated that with the inverter in GFM mode, the system is stable and resilient to a severe fault and an N-1 generation trip for several dispatch scenarios, including a zero inertia (zero synchronous machine) scenario.[79] This study also indicated that, for the Maui system, approximately 30% of online generation capacity needs to be GFM to maintain adequate damping.[80]

Australia Experience

The Australian Energy Market Operator (AEMO) published *Application of Advanced Grid-Scale Inverters in NEM* in August 2021,[81] describing GFM technology and application in the National Electricity Market (NEM). The Dalrymple BESS (30 MW/8 MWh) was the first transmission-connected GFM project in the NEM.[82] The South Australia Hornsdale Power Reserve (HPR) BESS plant has been upgraded from GFL to GFM control with the capabilities of providing grid inertia service[83] in July 2022. The HPR project is described below in more detail. Lastly, development of GFM BESS in Australia continues with BESS plants in New South Wales including:[84]

- Wallgrove GFM BESS by Tesla (50MW/75MWh): Transgrid began commercial operation in December 2022.
- Broken Hill BESS: AGL Energy is commissioning a 50MW/50MWh GFM BESS, construction started in fall 2022 with expected in-service date is mid-2023.

---

[76] https://dms.puc.hawaii.gov/dms/DocumentViewer?pid=A1001001A21F14B62327F00172

[77] http://www.hawaiianelectric.com/documents/clean_energy_hawaii/selling_power_to_the_utility/competitive_bidding/20211015_exhibit_8_S3_hawaii_model_ESPA.pdf

[78] Power HIL Validation of a MW-Scale Grid-Forming Inverter's Stabilization of Otherwise Unstable Cases of the Maui Transmission System (nrel.gov)

[79] https://www.nrel.gov/docs/fy22osti/83545.pdf

[80] On the HECO systems, additional GFM capacity may be needed to account for possible momentary cessation of GFL generation during transmission faults, which can cause voltage dropping very low in the whole system wide. This conclusion may not apply to the other larger systems where a fault does not reduce voltage system wide.

[81] https://aemo.com.au/-/media/files/initiatives/engineering-framework/2021/application-of-advanced-grid-scale-inverters-in-the-nem.pdf

[82] Dalrymple ESCRI-SA Battery Project – ElectraNet

[83] https://www.pv-magazine-australia.com/2022/07/27/hornsdale-big-battery-begins-providing-inertia-grid-services-at-scale-in-world-first/?utm_source=dlvr.it&utm_medium=linkedin

[84] Upgrade at Tesla Battery Project Demonstrates Feasibility of 'Once-In-A-Century Energy Transformation' for Australia - World-Energy

- Riverina and Darlington Point Energy Storage System: Edify Energy secured financing for three Tesla GFM BESS[85] projects (with total capacity of 150MW/300MWh)
- New England BESS: ACEN has started construction of 50MW/50 MWh GFM BESS in spring 2022 with expected completion date of 2023.[86]
- On December 17, 2022, the Australian Renewable Energy Agency (ARENA) announced co-funding of additional eight large scale GFM batteries across Australia with total project capacity of 2 GW/4.2 GWh, to be operational by 2025.[87]

Hornsdale Power Reserve (HPR) Experience

The HPR BESS project (150MW/193.5MWh) upgraded from GFL to GFM control to enhance grid stability. The process involved four phases, including:

- **Phase 1 – GFM control testing and benchmarking on ~~PSCAD~~ EMT model and HIL:** One functional behavior of the upgraded GFM control is shown on a single machine infinite bus (SMIB) testing system. The GFM control performances of ~~PSCAD~~ the EMT model are well benchmarked with HIL using a variety of disturbance tests. The benchmark results of virtual inertial response test is shown in Figure A.2.

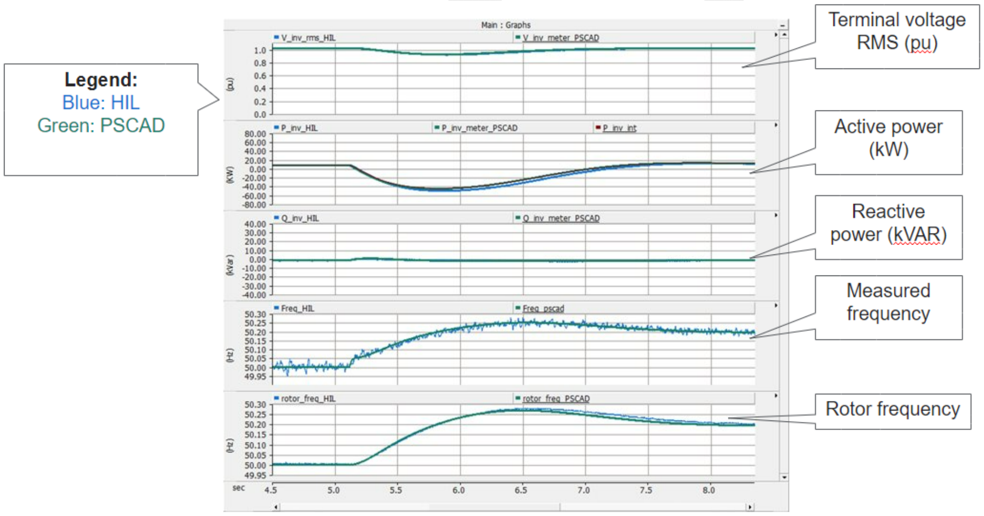


Figure A.2: ~~PSCAD~~ EMT and HIL (Hardware-in-loop) benchmarking

- **Phase 2 – Trialed GFM control mode at 2 out of 294 inverter at the HPR plant:** The two test inverters were upgraded with the actual GFM firmware while the rest of 292 inverters ran on grid following controls. This verified the different GFM and GFL control responses for the same disturbance. **Figure A.3** and **Figure A.4** show the GFL and GFM active power response, respectively, to the change in frequency. The GFM control contributes maximum power earlier than the GFL control, which is important to support the frequency nadir and avoid underfrequency load shedding. This test shows GFM controller has faster response for overfrequency as well.

---

[85] https://edifyenergy.com/energy-storage-systems/financial-close-on-the-largest-approved-grid-forming-battery/
[86] https://www.pv-magazine-australia.com/2022/05/26/acen-commences-construction-of-new-england-big-battery/
[87] https://arena.gov.au/news/arena-backs-eight-grid-scale-batteries-worth-2-7-billion/

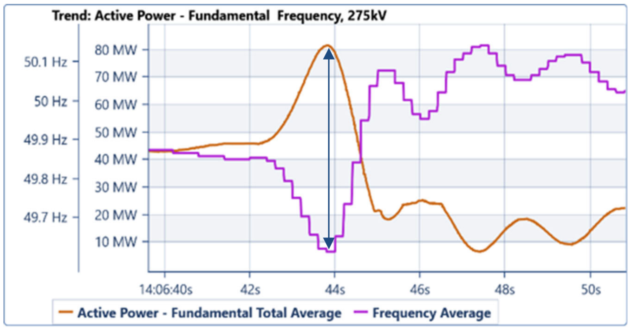


Figure A.3: GFL IBR Response to Frequency Event

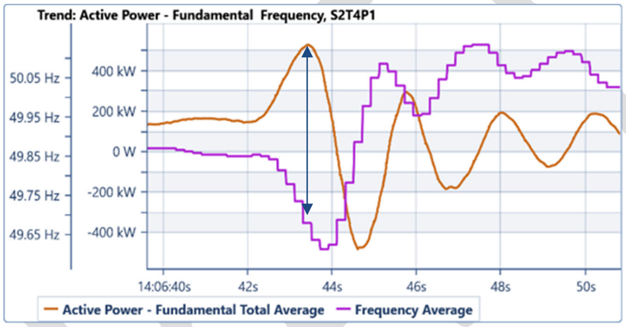


Figure A.4: GFM IBR Response to Frequency Event

- **Phase 3 – A new system interconnection study was performed under national electricity rule NER 5.3.9:**[88] This required to prove that the grid performance of the new grid forming resource is similar or better than the previous grid following resource. The HPR plant virtual kinetic inertial support (2000 MW.s) for South Australia was validated[89] and it was noted grid forming BESS help improve system damping.
- **Phase 4 – After studies were approved, GFM controls were enabled for all inverters at the site:** The HPR GFM plant performances are verified with the recorded site Elspec data which are also used to validate the BESS ~~PSCAD~~ EMT model. The site Elspec data performance and ~~PSCAD~~ the EMT model validation for a voltage dip are shown in **Figure A.5**. The HPR plant GFM controls provide damping to power oscillations and inertial energy to limit grid ROCOF and also provide voltage support from sub-cycle current injection when the voltage waveform changes at the inverter terminals.

---

[88] NER Rule 5.3: Establishing or Modifying Connection - AEMC Energy Rules

[89] hornsdale-power-reserve-virtual-machine-mode-testing-summary-report.pdf (arena.gov.au)

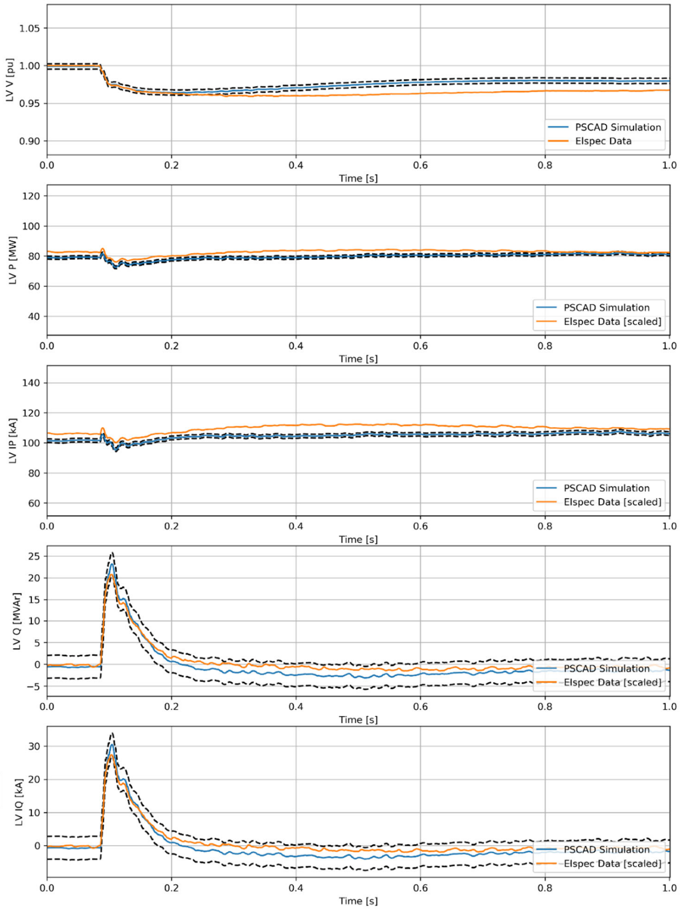


Figure A.5: Response from the inverter during voltage disturbance on the grid

Appendix B: Example of GFM Functional Test with Different OEM

Formatted

To demonstrate diversity in commercially available GFM technologies and potential differences in their controls and corresponding responses, the GFM functional tests described in Chapter 2 were repeated with a different GFM BESS model provided by another OEM, using the same initial condition and droop parameters. Despite the differences in their dynamic behavior, both OEMs' BESS EMT models passed all three verification tests and are verified to be GFM. Tests results are shown below in **Figure B.1 – B.3**.

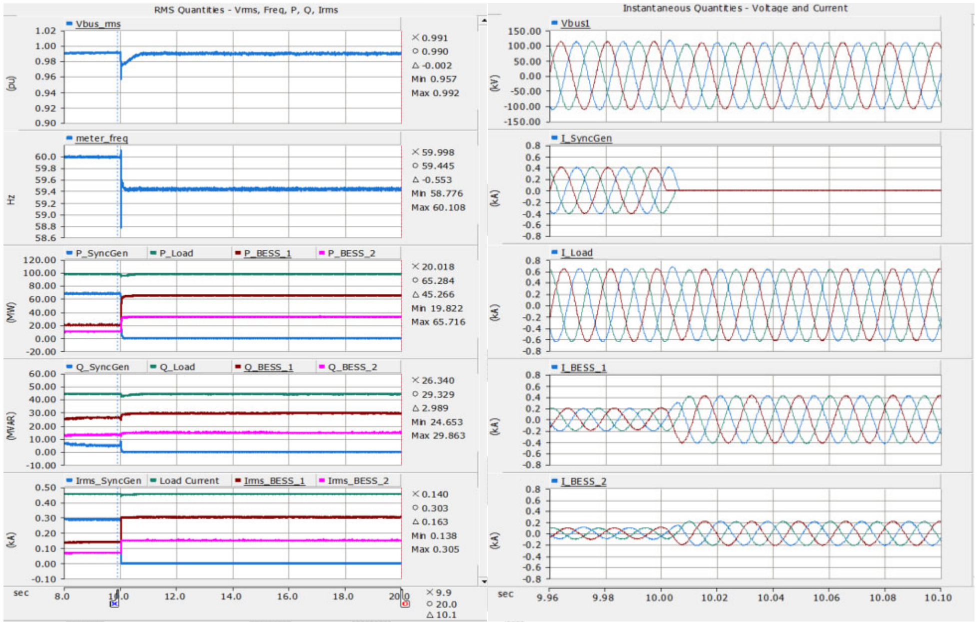


Figure 1~~B.1~~ Test 1 Results with Different GFM Model

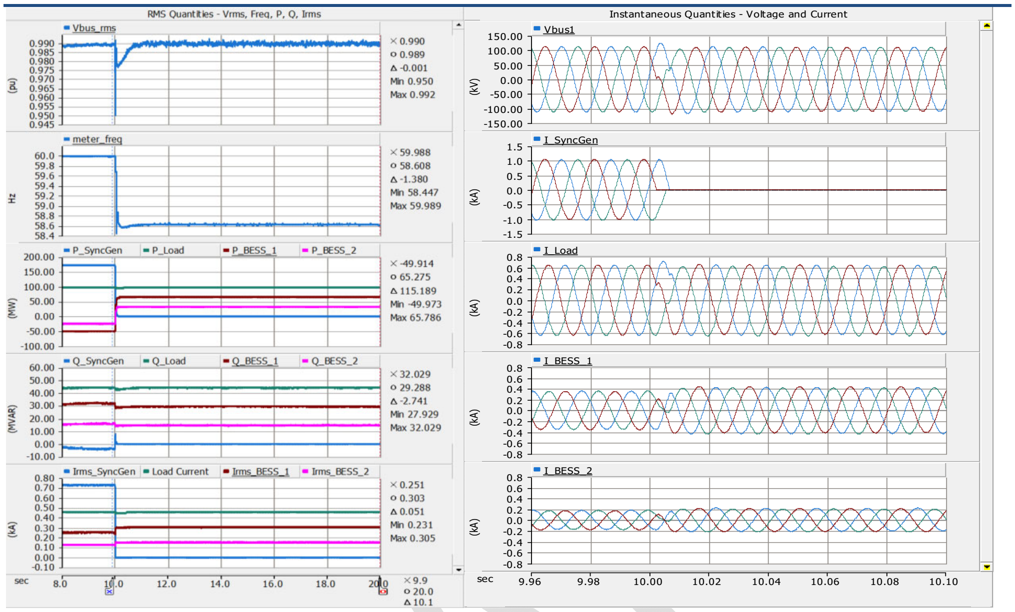


Figure 2~~B.2~~: Test 2 Results with Different GFM Model

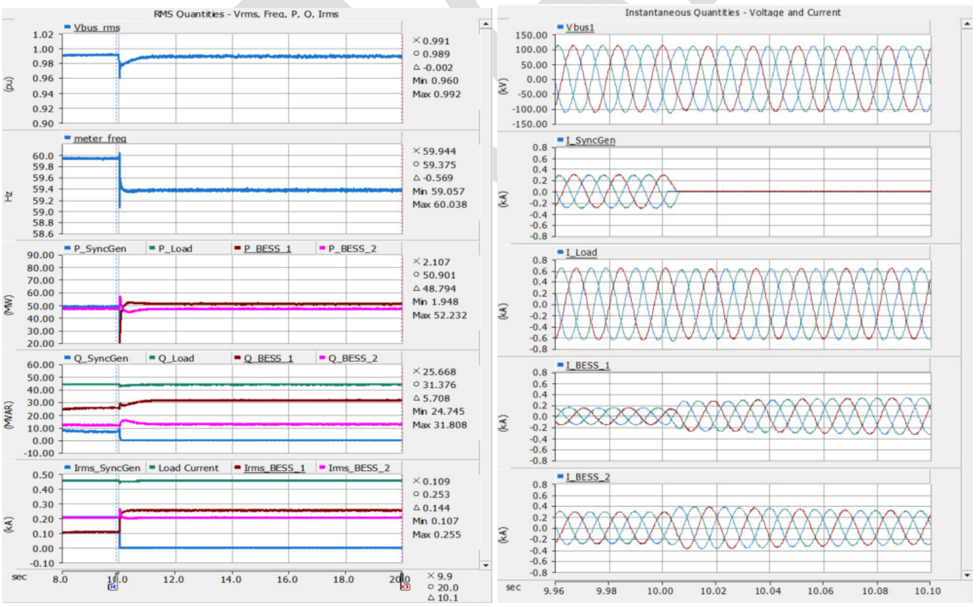


Figure B.3: Test 3 Results with Different GFM Model

Formatted: Font: Tahoma, Bold

Formatted: Centered, Space Before: 6 pt

Appendix C: Acknowledgements

NERC gratefully acknowledges the invaluable contributions and assistance of the following industry experts in the creation of this paper.

Name	Company
Andy Hoke	National Renewable Energy Laboratory (Primary Contributor)
Andrew Isaacs	Electranix Corporation (Primary Contributor)
Lukas Unruh	Electranix Corporation (Primary Contributor)
Prashant Kansal	Tesla, Inc. (Primary Contributor)
Deepak Ramasubramanian	Electric Power Research Institute (Primary Contributor)
Julia Matevosyan	Energy Systems Integration Group (IRPS Chair) (Primary Contributor)
Jimmy Zhang	Alberta Electric System Operator (Primary Contributor)
Sam Maleki	Electric Power Engineers, LLC (Primary Contributor)
Siddharth Pant	General Electric Company (Primary Contributor)
Hongtao Ma	North American Electric Reliability Corporation (IRPS GFM Specification Co-Coordinator)
Ryan Quint	North American Electric Reliability Corporation (Primary Contributor)
Alex Shattuck	North American Electric Reliability Corporation (IRPS Coordinator)
Aung Thant	North American Electric Reliability Corporation (EMTTF Coordinator)
Rajat Majumder	Invenergy (IRPS Vice-Chair)
Wenzong Wang	Electric Power Research Institute
Amin Banaie	Electric Power Research Institute
Dinesh Pattabiraman	TMEIC
Jing Xie	Pacific Northwest National Laboratory
Thomas McDermott	Pacific Northwest National Laboratory
Lucas Meubrink	SMA Solar Technology AG
Allan Montanari	SMA Solar Technology AG
Li Yu	Hawaiian Electric
Wei Du	Pacific Northwest National Laboratory
Nilesh Modi	Australian Energy Market Operator
Phil Hart	General Electric Company
Sergey Kynev	Siemens Energy, Inc.
Wen-Cheng Huang	Tesla, Inc.

Name	Company
Roberto Favela	El Paso Electric Company
Fred Huang	Electric Reliability Council of Texas
Michael Ropp	Sandia National Laboratory
Brad Rockwell	Kaua’i Island Utility Cooperative
Cameron Kruse	Kaua’i Island Utility Cooperative

NERC also gratefully acknowledges the comments received from Industry provided by the following organizations:

Organization		
EMTP	Arizona Public Service Company	AES Clean Energy
MITRE	Trina Energy Storage	Beacon Power
Natural Resources Canada	ITC Holdings	Edison Electric Institute
Manitoba Hydro	American Transmission Co.	REV Renewables
Evergy	Electric Reliability Council of Texas	Bonneville Power Administration
Western Electric Coordinating Council	Midcontinent Independent System Operator	Advanced Energy United
General Electric	Southern Company	

White Paper: Bulk Electric System Operations in Cloud

Action

Approve

Background

Security Integration and Technology Enablement Subcommittee (SITES) formed a sub-team to develop this white paper with the purpose of providing clarity to the electric industry on the applicability of cloud technology concepts and use cases to Bulk Electric System (BES) operations, as well as addressing barriers to adoption such as architecture and resiliency challenges, cloud service provider outages, and facilitating compliance evidence in regulatory audits.

Summary

This SITES white paper informs the electricity sector on viable BES Operations use cases for cloud technologies through both cloud service providers and independent software vendors. The paper offers considerations for establishing technology requirements, including understanding of cloud security through concepts of shared security responsibility models and shared security assurance. The paper explores the challenges with current NERC Critical Infrastructure Protection (CIP) standards and ability to facilitate required compliance evidence for audits and goes further to make industry recommendations to "move the needle". The content and collaboration presented in this paper have inspired one or more Standard Authorization Request (SAR) from the industry, both currently submitted and upcoming.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT

Bulk Electric System Operations in Cloud

NERC Security Integration and Technology Enablement Subcommittee White Paper

September 2023

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

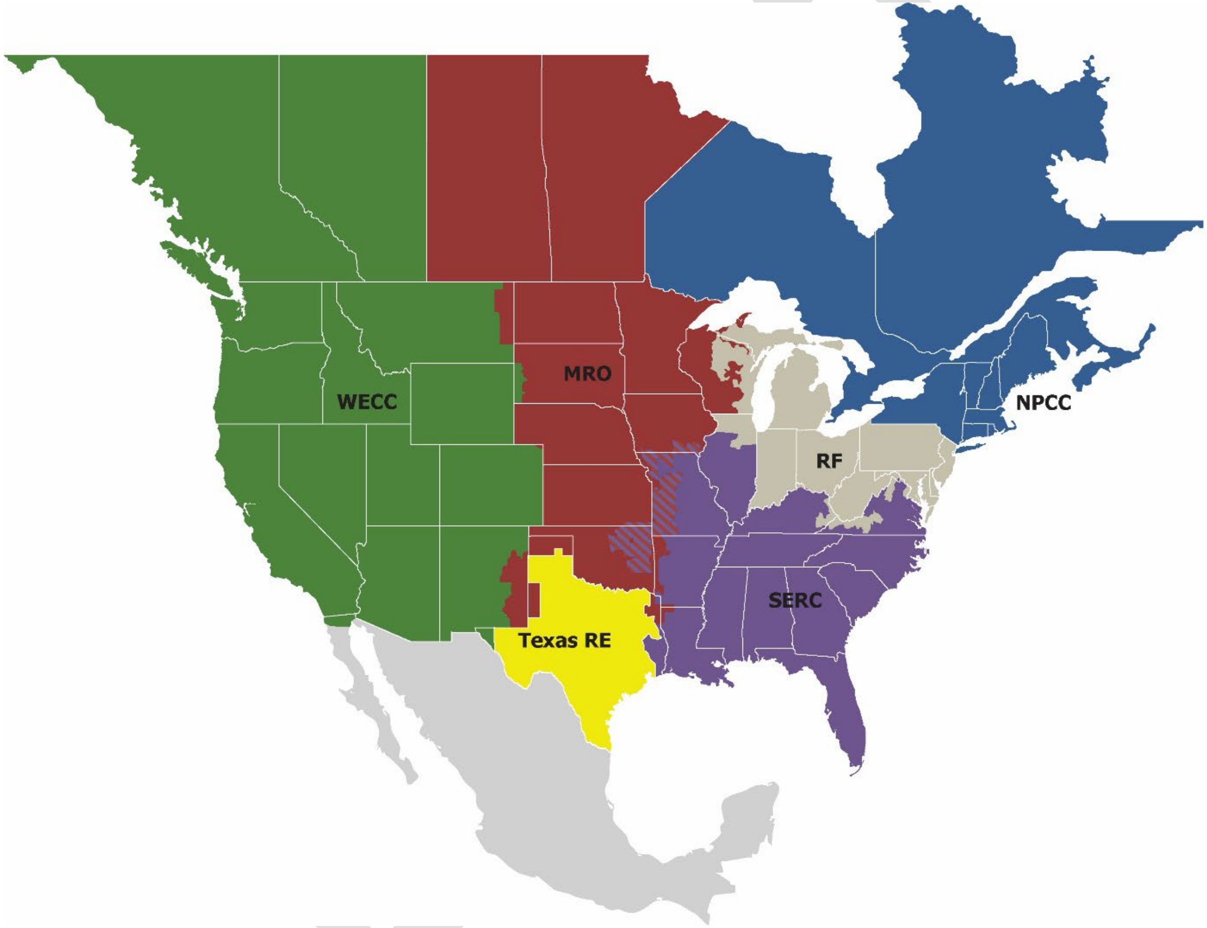
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of NERC and the six Regional Entities, is a highly reliable, resilient, and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six Regional Entities as shown on the map and in the corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Executive Summary

The Security Integration and Technology Enablement Subcommittee (SITES) recognizes industry interest in taking advantage of the benefits of cloud computing technology for various applications in support of the Bulk Electric System (BES). Innovative offerings from vendors within the electric sector are steadily including virtualization and cloud solutions. However, utilities should carefully assess security and reliability risks of migrating systems and applications associated with BES reliability operating services (BROS) to the cloud, especially those critical systems with high availability requirements. SITES identifies that BES operations are broad, and there are many opportunities for large data analysis and systems that are not real-time to benefit from cloud services.

SITES intends to enable the use of the cloud for registered entities but acknowledges that it is ultimately up to individual entities to determine their business objectives, and both the operational and technology requirements determine the use cases that is right for them. SITES strongly recommends that registered entities take a gradual approach to cloud migration by starting with information technology (IT) and non-regulated workloads. Entities should approach cloud migration cautiously for real-time and critical BES field and operations applications and ensure that the entity reaches maturity in its knowledge and capabilities with cloud technology, can verify cloud and application architectures to achieve that entity's requirements for reliability and security, and that the entity is prepared and informed to tackle compliance challenges. Furthermore, SITES recognizes challenges associated with resolving regulatory compliance to NERC Critical Infrastructure Protection (CIP) Reliability Standards for BES operations hosted in cloud service provider (CSP) environments as a barrier to cloud adoption within the industry. SITES has identified the need for enhancements to the basis and capacity for ERO Enterprise auditors to accept the work of others with regards to third party certification of CSPs to cloud security frameworks, and independent cloud risk assessments from registered entities with the end goal of aiding in evidencing NERC CIP compliance of BES operations hosted within CSP clouds.

Introduction

The electric grid industry is entering a new era of digital transformation and driven further by the adoption of cloud computing technology. With the potential to enhance the efficiency, resilience, and innovation of the Bulk Electric System (BES), cloud technology presents an opportunity for industry stakeholders to modernize BES reliability operating services (BROS). However, adopting cloud technology for BES operations comes with challenges, including regulatory compliance, security, and reliability concerns. This white paper aims to explore these challenges and opportunities while educating and providing guidance to entities to better navigate these complexities and make informed decisions about cloud adoption. Examination of business drivers, core concepts, and industry use cases as well as key recommendations to address regulatory constraints make up some of the valuable content found herein.

FERC Order

In December 2020, in an order regarding virtualization and cloud computing services, the Federal Energy Regulatory Commission (FERC) directed NERC "to begin a formal process to assess the feasibility of voluntarily conducting BES operations in the cloud in a secure manner." The order discussed industry comments, including those submitted by NERC, which suggest that using cloud computing services could be expanded for purposes other than BES Cyber System Information (BCSI) storage, including the nine BROS,[1] so long as the risks associated with these technologies are carefully addressed. Evaluating these risks and weighing them against the potential cost savings, enhanced security, and operational resilience is key to developing an effective path forward regarding any additional modifications to the CIP Reliability Standards. In December 2022, NERC made its informational filing regarding BES operations in the cloud. SITES has developed this white paper to further the assessment of securely conducting BES operations in the cloud and to provide industry with clear technical guidance on this topic.

This white paper focuses on the use of cloud computing technologies for BES operations. It builds on past work in the areas of cloud technologies particularly related to storing and accessing BCSI (i.e., "data in storage" and "data in transit"). The FERC directive focuses directly on BES operations using cloud technology (i.e., "data in use"); hence, the goal of this white paper is to provide technical content, findings, and recommendations on this subject.

Related Efforts

Several NERC projects, and other industry stakeholder group work products, exist with relation to virtualization and cloud computing. BCSI in particular has received focus over BES operations. Industry comments in response to the February 2020 FERC Notice of Inquiry (NOI) regarding virtualization and cloud computing for BES operations showed some entities have been voluntarily using virtualization and cloud hosting regarding data storage of BCSI. NERC Project 2016-02 and Project 2019-02 are expected to facilitate the use of virtualization and cloud computing for BCSI and clarify any uncertainties regarding compliance risks associated with using virtualization.

The following efforts and work products are related to virtualization and cloud computing:

- *NERC Standards Project 2016-02: Virtualization*
- *CIP V5 Transition Advisory Group (V5 TAG) White Paper*
- *NERC Standards Project 2019-02: BCSI Access Management*
- *NERC Compliance Monitoring and Enforcement Program (CMEP) Practice Guide: BES Cyber System Information*
- *NERC Security Guideline: Supply Chain Risks Related to Cloud Service Providers*
- *FERC NOI on Virtualization and Cloud Computing Services*

---

[1] See **Appendix B:Explanation of BROS and CIP-002-5.1a**

- Comments on *FERC NOI on Virtualization and Cloud Computing Services*

Intended Audience and Scope

This white paper focuses on applications of cloud technology in the electricity sector suitable for TOs, TOPs, Transmission Planners (TPs), Planning Coordinators (PCs), Reliability Coordinators (RCs), Balancing Authorities (BAs), Generator Owners (GOs), Generator Operators (GOPs), Distribution Providers (DPs), and others. The discussion includes use cases in real-time environments (i.e., operations within 15 minutes), near-real-time control center functions, field applications, and engineering tools for long-term planning and other functions. This white paper is intended for the following:

- Power and utility senior leaders, engineers (operations, planning, system architecture, etc.), cyber security professionals, and compliance teams
- Independent software vendors
- Cloud service providers
- Systems integrators
- Regulatory bodies and policymakers

Drivers for Electricity Sector Adoption of Cloud Technology

The electric delivery landscape is changing, prompting operators to adapt. There are numerous drivers for adoption of cloud technology, many of which are applicable to NERC registered entities and the electricity sector. Among the drivers include the following:

- **Changing Resource Mix:** The changing resource mix towards increasing levels of variable energy resources and distributed energy resources (DERs) is causing more variability and uncertainty on the BPS today and into the future. Entities need faster, smarter and more automated analytics tools for engineering and real-time operational decisions.
- **Digitalization:** The advent of microprocessor-based devices[2] across the entire electricity ecosystem is providing entities with massive amounts of data. While this data can improve situational awareness, decision-making, asset management, and support many other business decisions, most of the data is used ineffectively or completely unused because of the computational burden. Cloud technology offers unique opportunities to leverage the data more effectively and efficiently.
- **Resilience:** Cloud infrastructure could support a resilient energy infrastructure by enabling multi-region data storage and computing power that is highly dispersed geographically and highly redundant. This may help with business continuity plans, incident response, disaster recovery (natural or human-made), and other key business needs.
- **Advanced Analytics:** With all this data, entities are constantly focused on improving business decisions—better long-term planning and asset management decisions, more accurate and effective operational decisions, and better situational awareness. This requires advanced analytical tools that can leverage the increase in available data. Software vendors, solutions architects, and systems integrators need to ensure that data storage tools, applications, and front-end tools are able to leverage the data effectively. This presents challenges for the utility industry—whose tools and applications typically use legacy protocols and standards due to the long lifetime of different types of assets on the system. Cloud computing can unlock new decision frameworks and advanced algorithms, such as including machine learning and artificial intelligence.

---

[2] This could include microprocessor-based relays, remote terminal units (RTUs), phasor measurement units (PMUs), advanced metering infrastructure (AMI), smart meters, the Internet of Things (IoT), and many other forms measuring devices in generation, transmission, and distribution environments.

- **Widespread Adoption of Cloud Technology in Other Sectors:** Many other industries have moved toward the use of cloud technology in different forms, including other critical infrastructure (e.g., financial services, healthcare, life sciences). Many solutions providers, software vendors, and other third-parties offer cloud technology solutions. As providers continue to innovate and shift to cloud-first approaches, on-premises solutions may be discontinued or may be unable to meet the needs of utilities.
- **Managing Costs:** With the cross-sector movement toward cloud technology offerings, it may become cost restrictive to continue using more legacy tools and approaches in the future since technology providers would need to create "one-off" solutions for utilities. Therefore, entities will need to balance costs while ensuring sufficient reliability and security of their systems.
- **Available Expertise and Resources:** The rapid technology evolution is creating challenges of obtaining and retaining highly skilled security professionals in the electric sector broadly. Cloud security is increasingly a part of cyber security training curricula for security professionals graduating today and in the future. It will become increasingly difficult to find skilled professionals that understand legacy systems and security measures, which makes finding individuals with the necessary skills in cloud security and legacy systems a challenge as well.
- **Focus on Core Business Activities:** Use of cloud infrastructure, services, and expertise enables utilities to focus on core business activities rather than time-consuming administrative tasks, such as provisioning hardware and managing IT infrastructure. Utility IT and security professionals are able to focus more heavily on securing the systems and critical infrastructure under their responsibility rather than managing networks and systems.

Chapter 1: Overview of Cloud Computing for BES Operations

Cloud Technology Service Models

"Cloud computing" generally refers to on-demand delivery of information technology (IT) resources via the Internet with scale-on-demand resources and pay-as-you-go pricing. Instead of buying, owning, and maintaining data centers and servers, organizations acquire technology (compute power, storage, databases, and other services) on an as-needed basis. CSPs manage and maintain the infrastructure and access to these resources for their customers to develop and run applications. However, the term "cloud" is not a standardized definition. Cloud technology embodies a range of technological capabilities of which data center infrastructure is just one component. CSPs may offer one or more service models presenting different capabilities to meet different business and operational needs of their customers as shown in Figure 1.1. Cloud technology and service offerings include the following:

- **Infrastructure as a Service (IaaS):** A cloud computing service where customers rent or lease servers for compute and storage in the cloud. This eliminates the need to manually provision and manage physical on-premises servers in data centers. Most operating systems or applications can be run on the IaaS.
- **Platform as a Service (PaaS):** A category of cloud computing services that allows customers to provision, instantiate, run, and manage a modular bundle that is comprised of a computing platform and one or more applications. This is done without the complexity of building and maintaining the infrastructure typically associated with developing and launching the applications. As a result, this allows developers to create, develop, and package such software bundles.
- **Software as a Service (SaaS):** A software distribution model in which CSPs and independent software vendors (ISVs) offer applications that are hosted in the cloud and makes them available to end users over the internet
- **Hybrid Cloud:** An option where servers can be deployed at on-premises data centers to run various services offered by the CSP. This creates high speed, local compute capabilities and off-site redundancy and backup. This allows users to distribute their workloads between on-premises and cloud infrastructure based on their needs.

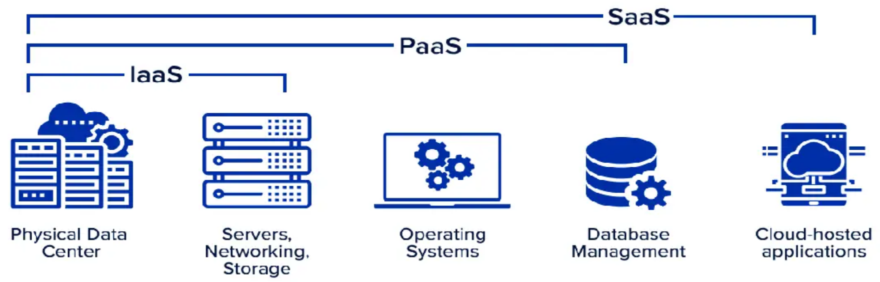


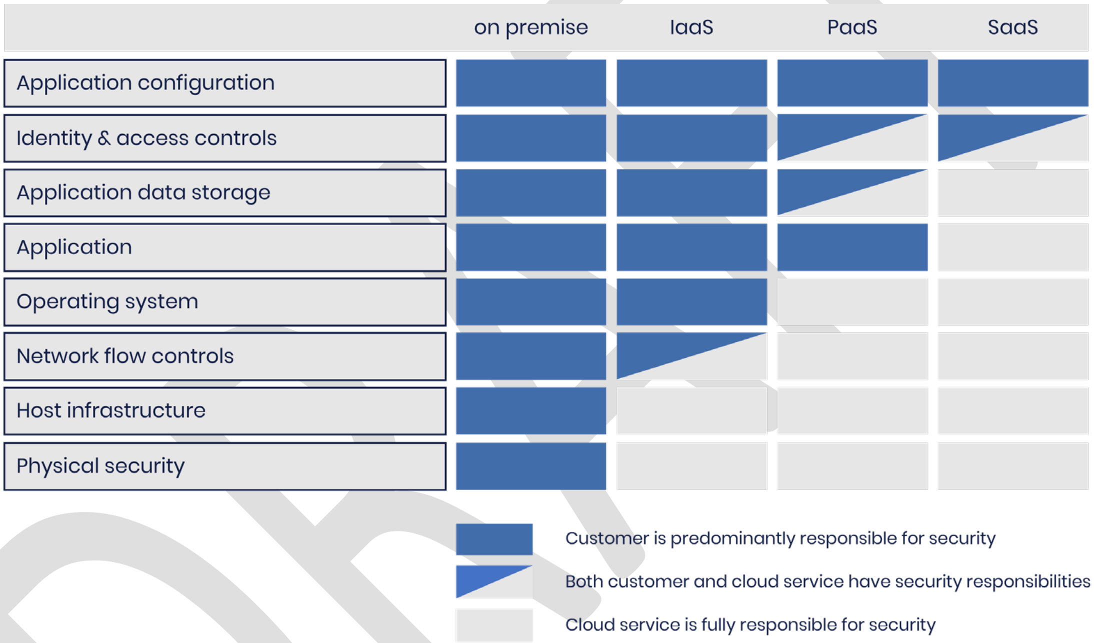
Figure 1.1: Cloud Service Models

The terms "underlay" and "overlay" are commonly used to establish a helpful abstraction between systems provided and supported by the CSP within a given service model versus the systems or applications built and/or configured by the customer within the hosted cloud environment. The underlay represents all components managed by the CSP, and the overlay represents the components managed by the customer and essentially built on top of the underlay. For example, in an IaaS model, the overlay includes any systems built by an entity within the provided virtual environment. Whereas in a SaaS model, the overlay may simply be the entity's data and configurations within a hosted application. These terms help create further clarity when leveraged in the discussion of responsibility for securing the cloud environment and cloud hosted systems.

Shared Responsibility Model

In a typical on-premises security model, customers are responsible for the end-to-end security in their data centers. When working with a cloud service provider, security and compliance is a shared responsibility between the cloud service provider and the customer. This shared model can help relieve the utility's operational burden as the CSP is responsible for the operation, management, and controls from the physical security of the facilities in which the service operates up to the host operating system and virtualization layer. In the case of PaaS and SaaS models, the CSP's responsibilities may extend further.

In an IaaS service model, the registered entity assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of security tools provided by the CSP such as firewall rules. Utilities should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their on- premises or other cloud environments, and applicable laws and regulations. This differentiation of responsibility is commonly referred to as Security "of" the Cloud versus Security "in" the Cloud.



	on premise	IaaS	PaaS	SaaS
Application configuration	🟦	🟦	🟦	🟦
Identity & access controls	🟦	🟦	◩	◩
Application data storage	🟦	🟦	◩	⬜
Application	🟦	🟦	🟦	⬜
Operating system	🟦	🟦	⬜	⬜
Network flow controls	🟦	◩	⬜	⬜
Host infrastructure	🟦	⬜	⬜	⬜
Physical security	🟦	⬜	⬜	⬜

🟦 Customer is predominantly responsible for security

◩ Both customer and cloud service have security responsibilities

⬜ Cloud service is fully responsible for security

Figure 1.2: Shared Responsibility Model

CSP Responsibility "Security *of* the Cloud" or "Underlay"

CSPs providing IaaS are responsible for protecting the infrastructure that runs all of their cloud services. This infrastructure is composed of the hardware, software, networking, and data center facilities that run the cloud services. CSPs providing PaaS and SaaS services can be responsible for securing the operating system, data, and even application layer. ISVs offering PaaS and SaaS products may build upon their own infrastructure or host their services on other CSP infrastructure offered as IaaS. In those instances, from the customer or registered entity's perspective, the ISV is the ultimately responsible party for ensuring protection of the complete cloud underlay including infrastructure. The ISV is party to the customer or registered entity's a contract agreement or service level agreement (SLA).

Entity Responsibility "Security *in* the Cloud" or "Overlay"

Registered entity responsibility will be determined by the CSP and cloud services that they select as a customer. This determines the amount of configuration work the customer must perform as part of their security responsibilities. It may be necessary for the entity to procure and implement their own security tools for systems built within the cloud overlay, such as the deployment of endpoint detection response (EDR) or network detection response (NDR) agents. Alternatively, security tools may be provided and built-in to the services provided by the CSP within the cloud. In such cases there is a shared responsibility of the security controls; the CSP's support of the tool within the underlay, and the entity's control configuration with the tool within the overlay. E.g., a virtual software firewall provided by an IaaS CSP and configured by the entity to perform traffic flow control, or application access roles provided by a SaaS vendor and configured by the entity for identity and access management.

The concept of shared responsibility should also be considered when obtaining security assurances through the acceptance of certifications and accreditations regarding the security of a cloud service provider or vendor leveraging a cloud service provider's products or services. Utilities should ensure that contractual agreements are in place regarding items such as certifications, accreditations and security controls, and that they are well understood by all parties.

Inherited Controls, Certifications and Accreditations

A key consideration in assessing and selecting a CSP is the security and compliance status of their services. This can be evaluated by assessing their certifications and accreditations. There are various certifications and accreditations a CSP can obtain to demonstrate that they can "secure the cloud." These may include any or all of the following:

- FedRAMP Moderate and High (United States federal government standards)
- DoD (US Department of Defense) SRG
- PCI (Credit card processing)
- HIPAA (healthcare and medical record processing)
- SEC (securities and exchange commission) standards

In addition, CSPs may meet various security and process requirements including:

- SOC 1, 2, and 3
- ISO/IEC 27001:2013, 27017:2015, 27018:2019, 27701:2019, 9001:2015,
- CSA STAR CCM v3.0.1

To maintain certification and accreditation to these security and compliance requirements, CSPs are often being continuously audited. These controls are audited by independent third parties with cloud security expertise. CSPs providing any cloud service model should be able to provide their set of accreditations to utilities to ensure their services achieve the required security control objectives. Selection of a vendor or their cloud services that do not match an entity's requirements will result in elevated security or compliance risk for that entity unless alternate steps are taken to mitigate the residual risk.

Shared Security Assurance

Similar to the shared responsibility model, entities should understand their responsibility for assuring security and compliance of systems hosted within a CSP's cloud environment. Registered entities have responsibility for any internal or external audits, including NERC CIP for any BES systems or BCSI leveraging CSP services. Additionally, due diligence by registered entities should involve periodic verification (trust, but verify) that CSP certification is still in place.

It should be further noted that PaaS or SaaS vendors which are reliant on a separate IaaS provider may need to achieve and maintain specific certification or accreditations to match those held and attributed to the IaaS platform.

For example, a large CSP may provide a FedRAMP Moderate certified IaaS underlay, but a dependent software vendor may fail to acquire or maintain FedRAMP Moderate for their SaaS applications built on top in the overlay. In such a case, to claim FedRAMP Moderate certification, the software vendor would need to seek FedRAMP authorization for the SaaS application independent of the CSP for the controls that are the software vendor's responsibility. Figure 4 provides a major CSP example of the shared responsibility for security compliance assurance.

Customer
Responsible for obtaining and maintaining certifications and accreditations through internal/external audits (as required) for their end-user system leveraging AWS and Vendors.

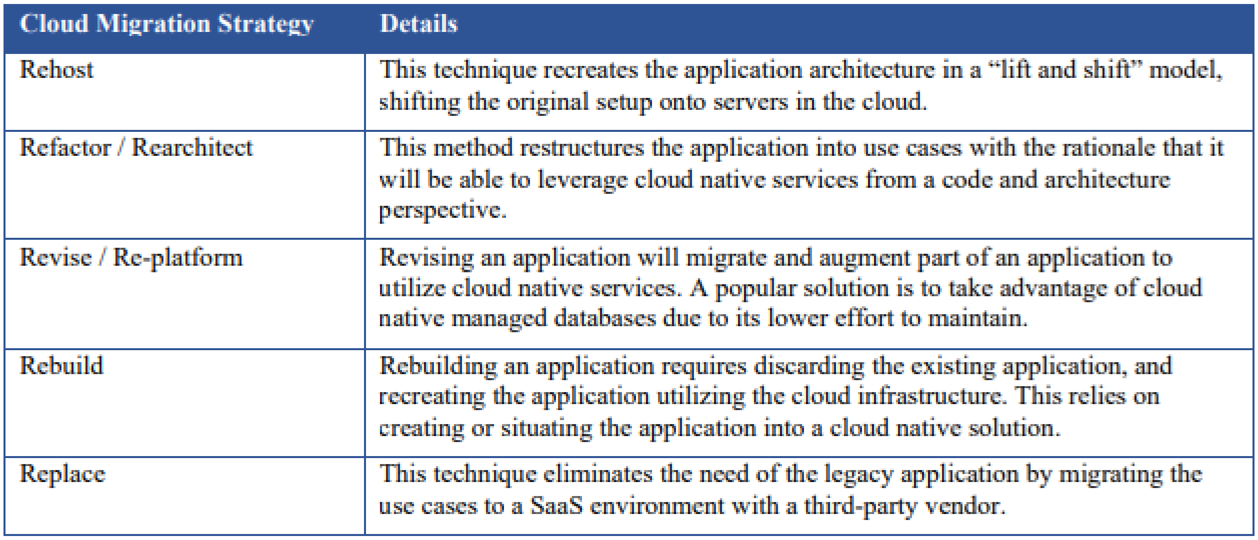
Vendor
Responsible for obtaining and maintaining certifications and accreditations through external audits (as required) for their cloud offerings.

AWS Security Assurance
Responsible for obtaining and maintaining AWS infrastructure certifications and accreditations through external audits.

Figure 1.3: Shared Security Assurance for Amazon Web Services (AWS)

Cloud Migration Strategies

Moving system functions and operations into the cloud can be a daunting prospect for utilities when faced with the myriad of options presented by software vendors, system engineering professional services, as well as cloud service provider offerings. Understanding business and technical requirements, constraints such as aging on-premises infrastructure and limited staff knowledge and experience, or challenges like change management and funding should all play a part in the selection of a cloud migration strategy. Entities may adopt multiple strategies to fit different projects and different applications. CISA provides a wealth of technical information to assist with cloud migration in their published Cloud Security Technical Reference Architecture[3] which utilities may find useful as they take on this challenge. The common cloud migration strategies are listed in Figure 5.



Cloud Migration Strategy	Details
Rehost	This technique recreates the application architecture in a "lift and shift" model, shifting the original setup onto servers in the cloud.
Refactor / Rearchitect	This method restructures the application into use cases with the rationale that it will be able to leverage cloud native services from a code and architecture perspective.
Revise / Re-platform	Revising an application will migrate and augment part of an application to utilize cloud native services. A popular solution is to take advantage of cloud native managed databases due to its lower effort to maintain.
Rebuild	Rebuilding an application requires discarding the existing application, and recreating the application utilizing the cloud infrastructure. This relies on creating or situating the application into a cloud native solution.
Replace	This technique eliminates the need of the legacy application by migrating the use cases to a SaaS environment with a third-party vendor.

---

[3] https://www.cisa.gov/sites/default/files/publications/Cloud%20Security%20Technical%20Reference%20Architecture.pdf

Figure 1.4: Cloud Migration Strategies from CISA Cloud Security Technical Reference Architecture v2.0

Communications Links

Utilities considering migration of critical services to the cloud should carefully consider their connectivity requirements with the cloud environment. As a best practice rule, when evaluating the migration of any systems to the cloud, the level of network redundancy maintained for an on-premises configuration of the same system should become the baseline of redundancy for connectivity between on-premises datacenters and the cloud environment that will house the migrated system. For example, if there is N-1 redundancy for networking between control centers and a data center hosting an EMS system, then it may be justifiable for EMS system components migrated to the cloud to be supported by N-1 or greater redundancy of communication links between the end users and the cloud.

As there are multiple choices of cloud technologies to meet a utility's operational needs, entities also have multiple choices to communicate with the cloud environment through a variety of communications network options such as public Internet, dedicated cable, private fiber, 4G/5G wireless, and satellite. Achieving the necessary redundancy and resiliency of communications between an entity and the CSP cloud environment may involve leveraging multiple communications media by working with multiple telecommunications companies. Private dedicated bandwidth fiber connections between entity data centers to large CSP clouds may offer state-of-the-art security (e.g., IEEE 802.1AE MAC Security Standard (MACsec) encryption for 10Gbps and 100Gbps connections), allowing for natively encrypted, high-speed, dedicated communications.

Chapter 2: Assessing Security of BES Operations in the Cloud

Quality of Service and Resilience

Quality of service (QoS) is a description or measurement of the overall performance of a service, particularly as experienced by the users of the network. Understanding operational requirements is critical when assessing possible cloud migration. Types of operational requirements for quality of service include, but are not limited to, the following: availability, latency, throughput, criticality, redundancy, failure rate, recovery time, etc. These operational requirements determine how a possible cloud solution will be architected. This information influences resilient architecture design including possible use of redundant communications paths, private networks, multi-region cloud architecture, and other factors. Utilities should consider service level agreements (SLAs) and service level objectives (SLOs) that commit cloud service providers to providing a certain level of service. Utilities can review SLAs and SLOs by service against the operational requirements for their workloads to help determine if the services can meet the needs of each use case. When considering service requirements, utilities should also recognize that their architectural decisions play a role in meeting their operational requirements.

The reality is that CSPs large and small can experience outages, therefore, this must be part of a utility's equation for resiliency and business continuity needs. Consideration should be given to the overall architecture of the application(s) and how high-availability and redundancy is achieved relative to operational or business requirements. Larger scale or critical systems may need architectures to mitigate against regional disturbances by use of multi-region or hybrid cloud failover. For example, a utility may utilize both cloud hosted and on-premises server(s) in an active primary/backup configuration for a critical application, or utilize one location as a live backup for disaster recovery.

Data Residency

CSPs may allow customers to choose and control the geographic location(s) among CSP data centers where their data will reside physically. For example, customers may be able to select which regions or areas that their data will be stored and the CSP will not move customer data without customer consent or request. These residency restrictions may include limiting to Registered Entity's country (or countries, depending on entity), however this should be carefully considered[4]. The registered entity needs the capability to fully assess and manage the residency of its data. Contractual and technical protections should be in place to ensure that data is held within these areas when selected by the entity. For national security reasons, wherever possible, BCSI information should reside within the country's boundary for which that entity operates. In cases such as an ISO/RTO that spans multiple countries while their members do not, open dialogue should be conducted between entities to form an agreement on data handling policies.

Security Objectives

Registered entities interested in migrating BES operations to the cloud should consider a number of security objectives to ensure availability, integrity, and confidentiality of the systems and applications trusted to the CSP's hosted cloud environment. Security objectives may differ based on the cloud service model and application use case at play. Entities should ensure controls are in place to meet the following non-exclusive list of priority security objectives are achieved either through tools provided in the overlay by the CSP, or procured and implemented by the entity within the cloud overlay (and on-premises) when necessary:

- Securing cloud to on-premises communication, including encryption and authentication
- Security logs and monitoring
- Data protection and data recovery including backups for servers, databases, or unstructured file data

---

[4] For example, Ukraine's law change in 2022 to allow government data and some private sector data to be hosted outside its own country allowed for the imminent backup of critical data during military invasion by Russia.

- Identity and access management
- Vulnerability management tools including patching and vulnerability scanning
- Malicious code detection or prevention
- Network security including IPSec VPN, access control lists, and secure service gateways

The Security Working Group (SWG) in collaboration with NERC, the ERO, and Azure performed an audit tabletop of BCSI in the cloud. They have produced a technical reference package includes tabletop findings, lessons learned, completed practice RSAWs, as well as a risk evaluation with contract considerations of data handling, recovery, and protection controls. The technical reference package is expected to be published in Q2 2023.

Evaluation Criteria for Selecting CSPs and Cloud Services

Registered entities should establish evaluation criteria, at the beginning and then as new information is captured, to ensure relevant factors are considered. During the cloud service provider selection process, new information may continually come to light as options and technology evolve. An organization should develop criteria for its evaluation process that captures business objectives, organizational use cases, technical requirements or restrictions, QoS requirements, and security and compliance needs including data residency, protection, and recovery. The following sections explore topics for consideration during CSP evaluation.

Use Cases & Business Justification

Defining IT and OT use cases in advance provides an opportunity to organize and define a roadmap for adoption. Selecting the appropriate cloud service provider that can support the majority of the key roadmap deliverables will be key to creating a sustainable cloud integration and implementation program.

An example of use cases that support a successful adoption may include starting with IT and non-regulated workloads first. IT and OT business teams can become more aware of core functionality, opportunities and features without risking compliance and regulatory challenges. Workloads that may be appropriate include; drone video storage, vegetation management, alternative energy management, remote non-regulated workloads, outage management systems, asset management and training environments. Presently, vendors already offer cloud-based solutions for many of these use cases today.

Future-looking business-related factors such as mergers and acquisitions should be considered early when developing business cases for cloud adoption. Additionally, developing cloud infrastructure may position an entity for new lines of business, increase talent draw, and offer beneficial tax opportunities.

As we look at the business elements, some cloud service provider use cases can help entities' structure the deals to support emerging financial models. With capital expense (CapEx) models, entities may be able to support the investment with their Public Utilities Commission versus an operating expense (OpEx) model, by including support, development and a longer-term infrastructure. Using the business case to present cloud adoption as a factor in improving grid reliability, security, and resiliency may allow for rate basing the technology investments alongside system infrastructure projects.

Integration with Existing Technology

Additionally, registered entities with existing IT Cloud products and services may want to evaluate and assess the ease of integration with existing cloud infrastructures, applications or services.

Existing infrastructure constraints, such as those associated with on-premises assets and data centers, need to be evaluated for connectivity, transition support and decommissioning. Current technology contracts, administration, licensing and support are important considerations on the timing and flexibility options available to registered entities on their roadmap to cloud adoption. By leveraging cloud, migrations from legacy platforms and systems can be conducted quickly in concert with the cloud service provider. When configured properly, cloud solutions can help set up the entity for future-proof system evolutions.

Telecommunication Infrastructure

Telecommunication infrastructure options play a key role in evaluating bandwidth and resiliency requirements. Extending the enterprise local-area network (LAN) to the cloud may streamline connections for on-premises users. Site-to-site communications may be more efficient because they allow entities to connect straight to the cloud environment rather than having dedicated circuits connecting back to the main headquarters or communications hub. Reducing dependencies on any one location may provide greater flexibility and resiliency should the main location suffer a communications failure. In this way, should there be an interruption, data and information can continue to be gathered, and command and control of remote sites can be maintained. Additional benefits may be realized by reducing the bandwidth usage and providing more predictability in sustaining costs of dedicated corporate internet access.

Telecommunications requirements for real-time monitoring and alerting create inflexible dependencies on corporate networks. Developing alternative data paths and utilizing hybrid architecture leveraging cloud-based edge devices may facilitate cloud adoption solutions for real-time and field use cases.

Compliance Requirements

Entities using cloud-based solutions or CSP services need to ensure that the entity's NERC CIP requirements as defined by their entity registration, BES cyber system impact category, and other compliance requirements, can be met. Additional compliance may consist of customer and employee privacy, HIPAA, PCI, PRIEDA, CESA and State Privacy laws. Entities should evaluate other regulations and statutes that are relevant to their business and geography.

Other Considerations for CSPs and Cloud Services

- *Mobile workforce teams* such as deployment, maintenance or other crews may be able to connect to the cloud for work orders, designs and other necessary information easier than depending on corporate remote access solutions.
- *Remote workforce employees* may benefit from access to cloud hosted applications, shared data, dashboards, and virtual workspaces. CSPs can offer and support various connectivity methods and security protocols to facilitate these solutions. Hosting shared information in the cloud may provide for faster response and access for those on limited bandwidth connections while reducing corporate Internet bandwidth consumption.
- *Authentication schema support*, such as LDAP and Active Directory, can be provided by CSPs to host or extend authentication to cloud infrastructure to provide redundancy or facilitate single-sign on and other benefits.
- *Training* is a key element for registered entities that are looking to integrate cloud infrastructures, software and services into their environment. CSPs that offer online or in-classroom training and comprehensive support programs may be better suited for new internal IT and OT teams looking to adopt their technologies.

Cloud Risk Assessments

Registered entities should conduct their own reliability risk assessments to determine whether BES reliability operating services and other services should be migrated to the cloud. As such services are commissioned, applicable risks would then move to the registered entity's ongoing risk management plan or process. Generic cloud service risk assessment frameworks and guidance for entities to consider are presently available from sources such as the National Institute of Standards and Technology (NIST). Where applications and services support BES operations, risk management plans for cloud adoption should be expanded to include risk items for grid reliability and compliance management. Other risk factors may include the diversification of service providers or service technologies, integrations between applications hosted in different cloud environments, as well as significant reliance on a single

CSP. Finally, as new cloud-based technologies and services emerge these risk profiles may change and ongoing monitoring of evolving risks will be needed at regular intervals.

A risk management structure that appropriately segments and clearly demarks risk ownership between registered entities and cloud service provider is critical to success. Responsibility matrices are one tool to assign responsibilities. Enforcement of ownership can be achieved via contractual agreements and possibly monitored using technical or administrative methods. NIST discussed the key provisions for a framework for [5]Managing Risk the Cloud.

---

[5] Chapter 7: Managing Risk in the Cloud (nist.gov)

Chapter 3: Examining Use Cases in the Electricity Sector

This section elaborates on possible use cases of cloud technology in different environments used by various NERC registered entities. This list is not intended to be comprehensive nor is it intended to provide all operational challenges or risks associated with each use case. It is, however, intended to illustrate the many different ways in which cloud computing *could* be used moving forward.

Long-Term Planning Applications

The primary benefits of leveraging cloud technology in the long-term planning horizon include increasing study workloads and reducing costs. With the increasing complexity and rapid integration of new BES resources, transmission planners are faced with performing increasing number and complexities of studies in a shorter timeframe. Cloud technology can help support reduced costs of executing those studies by leveraging shared computational resources off-site rather than the entity maintaining sufficient on-premises resources to meet peak demand in a timely fashion. This is particularly important during the interconnection study process where very short timelines are allotted to execute these types of studies. Examples of workloads in the long-term planning horizon (both planning assessments and interconnection studies) where cloud technology may provide benefits include:

- Improving development, maintenance, and utilization of network models and updates to those models
- Reducing equipment overhead costs by leveraging shared cloud resources for storage and computation of study work
- Increasing the number of base cases and operating conditions studied
- Increasing the number of sensitivity cases performed
- Increasing the number and depth of contingencies applied (e.g., N-1-1 analysis)
- Performing electromagnetic transient (EMT) studies during interconnection studies
- Performing EMT studies during annual planning assessments
- Increasing the number of EMT studies executed for any given project or network being studied
- Enabling the executive or monitoring of reliability studies from anywhere at any time

Other types of functions performed by planners and associated departments could include:

- Storage and management of drawings, procedures, calculations, and relay/PLC configuration files
- Effective development and deployment of asset management plans
- Coordination and collaboration between engineering, technician, construction and field support staffs

The NERC CIP Standards are generally not applicable to the long-term planning horizon since these activities do not have an operational impact within a 15-minute time horizon. Furthermore, planning studies generally do not include data that would be considered BCSI, although each entity would need to determine this for their organization.[6] Other designations such as Critical Energy Infrastructure Information (CEII) may impose additional confidentiality requirements to this type of information that would need to be handled accordingly. Therefore, entities need to ensure an adequate security posture in the cloud environment that meets any applicable regulations.

---

[6] Entities should apply security best practices to protect planning information such as models, study cases, simulation results, etc.

Operations Planning Applications

Cloud technology in the operations planning horizon centers primarily on the ability to do more in a short time constraint. While not as time-constrained as real-time applications, operation planning requires quick, accurate, and trustworthy results to ensure the grid maintains reliable operation. Leveraging cloud computing can not only reduce costs, but can likely allow operations planning to explore more thoroughly the impact of potential decisions as well as the impact of many combinations of potential operator actions. Examples where cloud computing may provide benefits include:

- Expansion of available data for use in operational planning analysis
- Increasing the maximum PMU data streams able to feed operational tools
- Running off-line analysis in tandem with real-time analysis for comparison
- Offloading of expensive desktop equipment and setups to support operational tools
- Coordination of planned and maintenance outages
- Capability to perform more detailed and shorter time step simulations (e.g., three phase root-mean-square (RMS) and EMT) for use in operational planning assessments
- Determination with more accuracy any system operating limit (SOL) or interconnection reliability operating limit (IROL)
- Interaction with energy management system (EMS) applications for a wider variety of users and ease of sharing EMS data to a variety of end users (e.g., real-time contingency analysis users)
- Improvement of forecasting fidelity in day ahead time frames
- Calculation of available transfer capabilities (ATCs) through increasingly constrained transmission systems
- Alignment and data quality checks of the model information in the operational tools for matching current day, next day, weekly, and seasonal models as well as alignment in various software platforms
- Customer management systems (CMS) and outage management systems (OMS) interfaces integrated with geographical information systems (GIS) to allow for public to see local outages without overloading operator telephones
- Predictive equipment maintenance and failure predictions of transformers

Real-Time Field Applications

Many of the core reliability and safety functions performed by relays, remote terminal units, sensors, and other devices in a substation rely on very fast actions (microseconds to milliseconds) and require very low latency and very high availability. Devices communicate with the other field devices or with the control center through unidirectional or bidirectional data exchange. However, some devices may store information locally and the data is typically stored within the device itself for a period of time or on another local storage device. This type of data storage configuration is typically used for either: 1) data that is made available for analysis, or 2) very high sampling rates of relatively rare events (e.g., digital fault recorder data). This data can generally be retrieved either locally or remotely, when necessary. Due to the strict operational requirements, making use of regional cloud data center technology may have limited value on its own. However, there are opportunities to utilize cloud-based devices that reside on-premises to support real-time field applications. In these designs, the cloud technology may not be performing the real-time function itself. Hardened, ruggedized, cloud-built industrial internet of things (IIoT) edge devices and on-premises hybrid cloud servers may be viable architectures to complement substations and other distributed or remote sites in support of real-time field applications.

Note that there may be applications that rely on field data that is sent and stored in a central repository (e.g., vegetation management data, drone footage, PMU data, etc.) but the team has categorized this as an off-line application rather than a field application since the data would be used in a centralized location rather than in the field directly.

Real-Time Operations Applications

Real-time operations applications are vital for situational awareness as well as making and implementing well-informed operating decisions. One of the primary benefits of leveraging cloud technology in real-time operation applications includes faster, more efficient disaster recovery. The nearly limitless compute resource available in the cloud provides the benefits of superior processing speed. Complex workloads (like transient security assessment calculations) that can take up to 30 minutes to process on-premises are completed in a couple of minutes in the cloud. Unexpected outages of real-time operations applications can leave system operators with impaired visibility. Having previous versions of software stored in the cloud and having production instances running on multiple cloud availability zones or regions allows faster recovery from disasters. For example, suppose an application is deployed in various regions, and one region goes down for some reason. In that case, the traffic can automatically failover to the working regions without any interruptions to the end-users. In other cases where there is a major bug in the software release, a quick rollback can be initiated to restore a previously released, more stable version to minimize impact. The fact that data can be stored in the cloud without capacity constraints also helps with backup and restore purposes. Example workloads in real-time operations applications where cloud technology may provide benefits include:

- Providing a fast scan on system conditions with a shorter cycle for state estimator and/or real-time contingency analysis
- Increasing the number of base cases and operating conditions studied
- Expansion of scenario studies for real-time stability analysis
- Capability to consider more constraints in real-time optimal applications
- Capability to run real-time multiple time-point look-ahead study that assembles the current base case with planning outages and performs thermal/voltage/transient assessment for near future intervals
- Improving efficiency of data exchange between real-time operations applications
- Improving interactions between real-time operations applications and distribution/market applications
- Increasing collaboration between RCs and TOPs. They can view and share information easily and securely across a cloud-based platform.

There may be cloud use cases to be found if historically monolithic applications such as EMS and supervisory control and data acquisition (SCADA) are broken down to their logical service components. The use of microservices and containerization technology create opportunities to develop new architectures hosted in cloud environments for these applications. The typical dependency between main EMS/SCADA applications is illustrated in **Figure 3.1**.

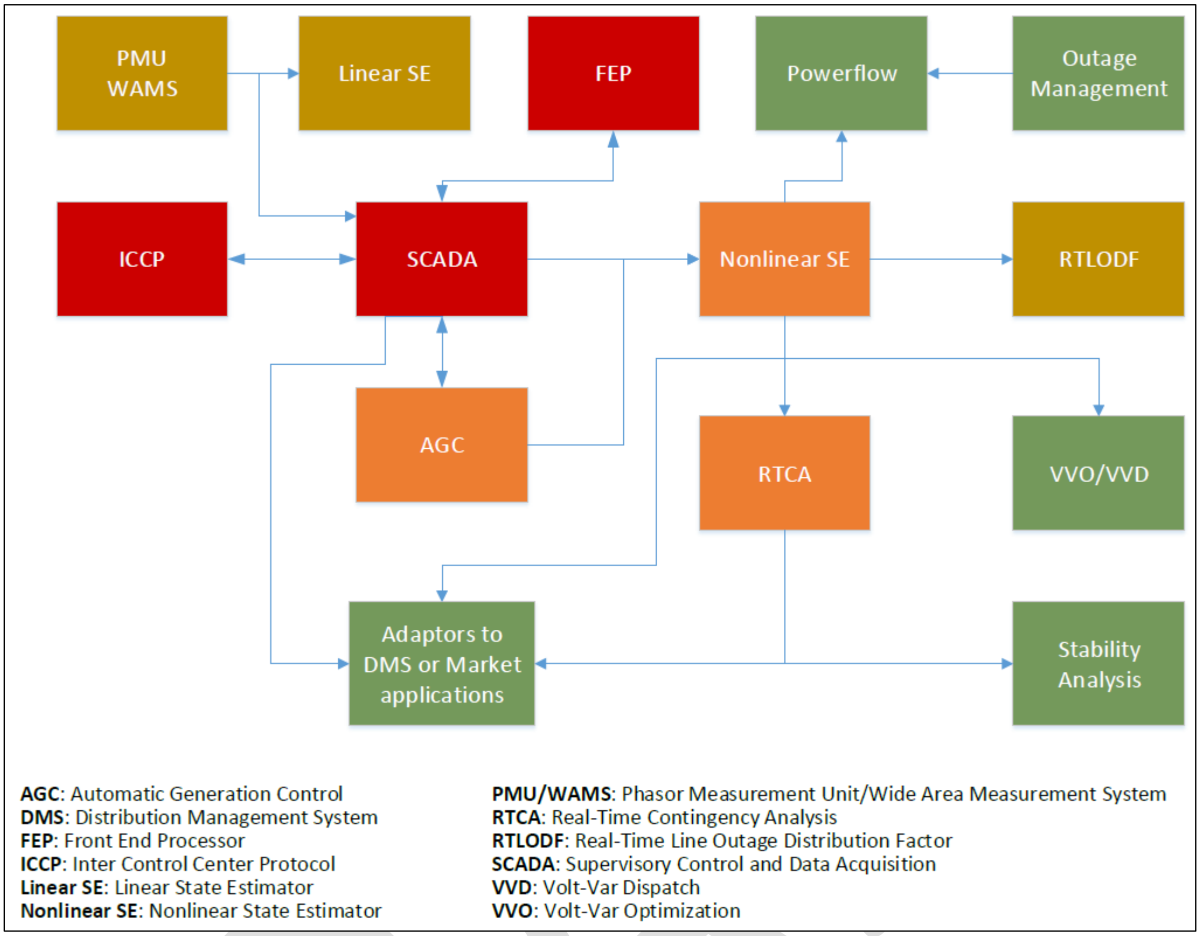


Figure 3.1: Example Visualization of EMS/SCADA Applications

The real-time operations applications that comprise the EMS/SCADA system (shown in **Figure 3.1**) can be categorized in the following risk levels.

- **Critical:** FEP, ICCP, and SCADA
- **High:** AGC, Nonlinear SE, and RTCA
- **Medium:** Linear SE, PMU/WAMS, and RTLODF
- **Low:** Adaptors to DMS or Market applications, Outage Management, Power Flow, Stability Analysis, and VVO/VVD

This categorization is based on the following questions intended to help entities evaluate operational restrictions and potential risks of placing real-time applications in the cloud:

- **How is the current real-time application deployed in the EMS and can it be migrated to a cloud solution?** Some applications are more suited for on-premises solutions while others may be migrated to the cloud. Software vendors may even offer cloud-based products today and in the near future, so ensuring the organization fully understands what the migration entails, how it will affect critical business functions, and whether cloud solutions are even an option or priority for applicable vendors will be key. The criticality (i.e., consequences of failure, unavailability, or compromise) of each service or application is key to informing business decisions in this area.
- **What type of cloud deployment models is being used?**

NIST SP 800-145[7] defines four deployment models: private cloud, community cloud, public cloud, and hybrid cloud. Public cloud is provisioned for public use and exists on the CSP's premises whereas private cloud is provisioned for exclusive use by a single organization and may exist on or off premises of the organization. On-premises private cloud options, and/or dedicated connections to a secure cloud environment at the CSP present lower risk for possible real-time applications. Hybrid cloud options may also help ensure security requirements are met while leveraging availability and uptime benefits of cloud-based technology.

- **Is the real-time operation application essential for entities to implement their reliability functions?** Entities use various EMS/SCADA applications based on their reliability functions. For example, AGC and SCADA are critical for Balancing Authorities (BAs) to monitor and control generation output and to calculate area control error. A Transmission Operator (TOP) may use SCADA, SE, and RTCA to monitor and control the transmission network to keep the system in a reliable operating state. FEP and ICCP may be required by both the BA and TOP. Placing non-essential real-time operations applications in the cloud is likely a lower risk than those applications essential to core reliability functions. Some situational awareness tools, advanced monitoring systems, or other tools may be more suitable for initial cloud adoption in real-time.
- **Will the failure of the real-time operation application cause a complete loss of monitoring and/or control capability, and what does the fail-over state look like?** Monitoring[8] and control[9] capabilities are essential for real-time operations. If the failure of the real-time operation application could cause a complete loss of monitoring or control capability, a higher risk should be considered to place this application in the cloud. For example, loss of SCADA would likely be the most impactful EMS failure. System operators would not have indication of the status of devices or key data points such as MW, MVar, current, voltage, or frequency from RTUs. Furthermore, system operators would not be able to open and close breakers or switches remotely from the control center. Fully understanding the operational impacts for any failure or unavailability of the service is critical. The type of cloud model implemented may impact these considerations.

Security Service Applications

Cloud technology for security service applications centers on the ability to visualize, process, assess, and quickly react to anomalies in a protected environment to mitigate the impact of security events on reliability. Leveraging cloud computing can reduce costs and also allow security operations centers (SOCs) or security teams to more quickly assess and analyze potential threat and the impact of a cyber event within their environment. Examples where cloud computing may provide benefits include:

- Expansion of available data for use in security analysis
- Offloading of desktop equipment and set up to support security tools
- Increased storage capacity to retain security and operational log data for extended timeframes
- Enhanced data analytics and machine learning services that support cyber security incident response and forensic analysis
- Cloud-based single platform tools that increase visibility into IT and OT networks to support situational awareness and threat detection (e.g., next generation antivirus)
- Cloud-based single platform tools that coordinate security maintenance across cloud and on-premises implementations (e.g., patching)

Examples of these types of systems or applications may include the following:

---

[7] https://csrc.nist.gov/publications/detail/sp/800-145/final

[8] Monitoring capability is the ability to accurately receive relevant information about the BES in real-time and evaluate system conditions using real-time data to assess existing (pre-contingency) and potential (post-contingency) operating conditions to maintain reliability of the BES.

[9] Control capability is the ability to take and/or direct actions to maintain the reliability of the BES in real-time via entity actions or by issuing operating instructions.

- **Electronic Access Control or Monitoring Systems (EACMS):**
    - **Security Information and Event Management (SIEM):**
        - Reduced infrastructure maintenance, enabling more focus on high-value security tasks instead of regular maintenance, monitoring SIEM health, and troubleshooting
        - Increased elasticity to scale the capacity of SIEM compared with capacity-constrained on-premises solutions (e.g., scaling storage for irregular increases in log volume versus losing logs)
        - Advanced analytics and machine learning that allow utilities to mature their security monitoring program through data correlation, behavioral analytics and/or anomaly detection
    - **Next-generation antivirus (NGAV):**
        - Reduce time to identify malware using advanced endpoint protection technologies involving AI and machine learning to identify new malware by examining more elements such as file hashes, URLs, and IP addresses
        - Endpoint security software protects endpoints from being breached including those that are physical or virtual, on- or off-premise, in data centers or in the cloud. It is installed on laptops, desktops, servers, virtual machines, as well as remote endpoints themselves.
        - Administrators can remotely monitor and manage endpoints through a centralized management console that lives in the cloud and connects to devices remotely through an agent on the endpoint.
        - These solutions leverage cloud controls and policies to maximize security performance beyond the traditional perimeter removing silos and expanding administrator reach.
    - **Automated patch management solutions**:
        - Cloud-native automated patch management solutions centralize patching into a single console that can patch hybrid infrastructure and remote environments.
        - IT administrators can set specific rules for new updates including rules for testing new code updates before deployment. This gives IT departments the oversight they need to help with compliance requirements and security maintenance.
- **Physical Access Control System (PACS):**
    - Cloud-based offerings are scalable and allow customers to adapt to the security needs of any number of remote sites, buildings, or doors without limits on controls or logging. They easily integrate with other systems like communications or electronic security systems. The integrations help offer context to physical or cyber monitoring of security standards and employee policies.

Use Cases for Smaller Entities

Cloud technology, particularly when shared across multiple entities at relatively low cost, may provide specific benefits to smaller entities. The cost of standalone products (e.g., SCADA systems, advanced applications, data historians) can be relatively steep for smaller entities, making tools significantly limited. Smaller entities are not able to staff IT and OT resources to properly maintain and secure these systems and applications. Larger entities will often use custom tools, applications, or programs for operational tools whereas smaller entities need off-the-shelf applications. In many cases, information sharing and shared use of common applications provides tangible benefits for smaller entities. Examples may include:

- **Secure Access to EMS:** Smaller entities may remotely access EMS systems and applications of neighboring TOPs and RCs for situational awareness. In many cases, these entities have read-only privilege for viewing analysis results. The ability to streamline and secure this access across a single platform could provide significant value to these entities.

- **Off-The-Shelf SCADA:** The ability to extend or offer mainstream off-the-shelf SCADA tools to smaller entities (and smaller systems), such as through a joint purchase, could provide additional value for these entities. For small organizations, SCADA solutions are often custom-built or ad-hoc, if they exist at all. Enabling more streamlined off-the-shelf solutions that minimize costs for custom solutions could be beneficial.
- **Customer and Outage Management:** Cloud-based customer management systems and outage management systems with a customer interface and geographic information system integration is another area of focus for smaller entities. This solution could greatly improve customer service during times of customer impact due to outages and overloading of resources (phones, staff, computational power, etc.).
- **Equipment Maintenance and Asset Management – Industry Sharing:** Cloud-based tools that share critical information (e.g., equipment failure data) from a centralized and secure database could streamline asset management and maintenance programs, and could enhance reliability through lessons learned and other information sharing.
- **Reliability Study Model Construction:** Software vendors and regional case building entities may be able to host cloud-based tools and products for the effective and efficient development of regional or interconnection-wide planning cases (steady-state, short-circuit, dynamic, etc.). This could help the ease of case creation as well as streamlining case updates and change management.
- **Engineering Drawing Management:** Cloud databases can be used to store engineering drawings, procedures, calculations, and configuration files. These databases can be tied to work order management systems such that relay techs are provided the most up-to-date database files from a master library database (which can be tied back to relay maintenance programs per PRC-005, etc.). Additionally, there are opportunities with collaborative modeling, tuning, and debugging in co-simulations.

Many of these solutions highlight the need for improved accessibility at a minimized cost. They also demonstrate the need to minimize potential errors throughout the planning, design, and real-time operations horizons that are often caused by disparate databases and/or tools rather than leveraging a centralized cloud-based tool. There are likely many more examples of opportunities for smaller entities; however, these provide some concrete examples from NERC engagement with smaller registered entities.

Chapter 4: NERC CIP Compliance Considerations

From a NERC CIP Standards compliance perspective, the most fundamental aspect of cloud technology is understanding what data is being put into the cloud and how that data is being secured. This requires a case-by-case assessment of cloud use cases to determine applicable security controls and how the implementation, and demonstration, of those controls align with the NERC CIP Standards. Once the "what" and the "how" are well understood, then Registered Entities, the Regional Entities, and NERC can delve into understanding how the controls are demonstrated and the role of contractual agreements with the CSP, separation of the underlay and the overlay, and the protections in place between the two layers, etc. A critical consideration for Registered Entities is assuring that sufficient documentation or demonstration in other forms is available both from the entity and the CSP to demonstrate compliance with all applicable requirements.

Cloud service providers architect security differently than traditional on-premises security architectures. These differences may include identity and access management to their underlay environments. For example, some CSP's purposely design their systems to prevent CSP personnel from accessing customer environments and data through strict physical and logical separation controls. These implementations may be supported by logging capabilities that offer customers the ability to see every API call made to and within their environment. Other CSPs may offer specific solutions to control access to a customer environment that offers the entity visibility and requires entity authorization each time CSP personnel needs access. Demonstrating that these controls are in place and meet the NERC CIP requirements necessitates collaboration, agreement and guidance to be developed by entities, the ERO Enterprise and CSPs. Future compliance demonstration may require consideration of the acceptance of third-party audit records such as SOC reports, or third-party certifications such as FedRAMP as components of compliance demonstration which are typically not necessary in an on-premises environment.

Acceptance of third-party audit reports and third-party certifications is a topic central to enabling cloud adoption. From a compliance assurance and auditing perspective, the Government Auditing Standards (known as the Yellow Book)[10] include requirements pertaining to accepting the work of others. In particular, Section 8.81 states the following:

> ***8.81*** *If auditors use the work of other auditors, they should perform procedures that provide a sufficient basis for using that work. Auditors should obtain evidence concerning the other auditors' qualifications and independence and should determine whether the scope, quality, and timing of the audit work performed by the other auditors can be relied on in the context of the current audit objectives.*

The footnote on section 8.81 references Section 5.80, which states:

> ***5.80*** *Auditors who are using another audit organization's work should request a copy of that organization's most recent peer review report, and the organization should provide this document when it is requested.*

NERC uses these Government Auditing Standards as the foundation of NERC Audits. Further analysis into ways that third-party audit reports and third-party certifications can be used in alignment with this guidance is necessary.

Registered entities adopting cloud technology will also need to consider the security controls available to prevent unauthorized access to their overlay environment, and how to demonstrate that they are implemented. Those controls may include, but are not limited to, encrypting the cloud overlay environment, managing access to the encryption keys, implementing and managing identity and access management controls that include authorization,

---

[10] Government Auditing Standards, 2018 Revision. Technical Update April 2021: https://www.gao.gov/assets/720/713761.pdf

development and use of discrete access roles, and log collection and retention. Some of these controls are likely to require additional and / or different audit evidence than an entity has needed to produce for on-premises environments.

An example of where these parties have come together in support of cloud adoption successfully is the NERC published *ERO Enterprise CMEP Practice Guide: BES Cyber System Information*.[11] The Practice Guide opened the door for Registered Entities to move BCSI data into the cloud, breaking down the tie to specific physical assets and data repositories, and included guidance that NERC Regional Auditors should consider access to include any instance or event during which a user obtains and uses BCSI. This clarity enabled utilities wanting to use third-parties such as CSPs to understand the controls necessary to implement a secure and compliant program. This also led to the formation of Project 2019-02 to revise the NERC CIP Standards, which will provide clearer guidance for allowing Registered Entities to utilize cloud technology for sensitive data storage.

Beyond CIP-004 and CIP-011 challenges, there are additional obstacles with other NERC CIP standards that would need to be addressed once access requirements between the overlay and underlay are addressed. These include, but are not limited to, the following:

- CIP-005 utilization of External Routable Connectivity
- CIP-006 how cloud-based PACs are deployed, logged and monitored
- CIP-007 logging of events and how event log reviews occur

These issues will need to be addressed by stakeholders including industry, NERC and registered entities working collaboratively through future standards revisions, development of compliance guidance and other mechanisms. Given the expected timetables for CIP standards revision and development of this magnitude, however, it may serve industry well to make additional efforts towards cloud adoption that build consensus on a more optimistic timeline.

---

[11] https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/ERO%20Enterprise%20CMEP%20Practice%20Guide%20_%20BCSI%20-%20v0.2%20CLEAN.pdf

Chapter 5: Recommended Industry Actions Moving Forward

The following are recommended actions that NERC and its stakeholders should take to remove barriers of adoption and promote the secure and reliable use of BES operations within CSP hosted clouds:

Long Term:

- **Recommendation L1:** SITES recommends industry submit a SAR to develop a new NERC CIP standard for cloud security which consolidates security control objectives for BES cyber system hosted in CSP cloud environments. This new standard should accommodate various cloud service models and cloud architectures, and provide clear expectations for evidencing controls within the cloud underlay and cloud overlay.
  - The SAR should aim to complement, and not impede, the efforts of Project 2019-02 for BCSI in the cloud.
  - The SITES team is aware of an industry group currently drafting a SAR to meet recommendation #1. As well, other groups have expressed interest in developing a SAR.

Short Term:

- **Recommendation S1:** SITES recommends industry perform NERC CIP audit tabletops covering CSP cloud-hosted BES cyber system use cases to identify compliance and security risks in order to continue building knowledge for industry and subsequently informing the development of CMEP Practice Guides when assessing registered entities in similar audit scenarios.
  - Intended to identify further problems to be solved including needs to modify evidence request tools, RSAWs, and specific security, compliance, implementation, CMEP guidelines, etc.
- **Recommendation S2:** SITES recommends NERC and the Regional Entities consider how to review and accept (as reasonable assurance of compliance) the following sources if provided as evidence of compliance with applicable Reliability Standards: accredited third party auditors providing cloud-based security framework certification for CSPs and independent cloud risk assessments of CSPs performed by registered entities. The intention is for NERC and the Regional Entities to consider relying on these measures as evidence for the security of a CSP underlay environment in an assessment of a registered entity utilizing BCS in a CSP cloud. SITES recommends NERC and the Regional Entities further consider the following:
  - Where a SaaS provider utilizes a separate IaaS provider, the SaaS provider would use third-party audit evidence provided by CSP/IaaS provider for the security of the underlay, and documentation/third-party audit evidence for the security of the overlay they are providing to the registered entity.
  - The registered entity would then be responsible for evidencing security objectives for the overlay and/or underlay depending upon the shared responsibility model.
- **Recommendation S3:** SITES recommends industry endeavor to map NERC CIP standards and requirements equitably to prominent cloud-based security control frameworks, providing a foundation for the potential use of accredited third-party auditor reports and certification of CSP products and services to be utilized as accepted work of others by ERO Enterprise auditors within audits of registered entities as part of a shared responsibility model between the CSP and registered entity for BES cyber system hosted in the cloud. E.g. ISO/IEC 27017
- **Recommendation S4:** SITES recommends vendors with cloud-based products and services for the electric sector take a pro-active approach to seek accredited third-party certification to cloud-based security frameworks which encompass the NERC CIP requirements, and to furnish both audit reports associated to such certifications, and CIP implementation guidance or controls documentation for their cloud products.

    - SITES recommends cloud security frameworks where consensus on equitable mapping to NERC CIP is building, such as with FedRAMP Moderate.

- **Recommendation S5:** SITES recommends the ERO Enterprise develop compliance implementation guidance for registered entities to evidence control ownership within a shared responsibility model for their cloud-hosted BES cyber system.
- **Recommendation S6:** SITES recommends industry develop and standardize use of a CIP-tailored cloud risk assessment framework for independent use by registered entities during evaluation and selection of CSPs for cloud hosted BES cyber system . The risk assessment framework should likewise be tied to a standardized cloud security framework (e.g., Cloud Security Alliance's Cloud Controls Matrix). Furthermore, CSPs may limit their participation in the risk assessments by pro-actively furnishing the necessary input to the risk assessment through controls implementation and management documentation. SITES recognizes that smaller CSPs and SaaS vendors may find the process for third-party certification too substantial or costly, potentially creating a gap that may be filled by independent cloud risk assessments performed by registered entities.

Appendix A: A Look at EMS Cloud Deployment

Table A.1 illustrates a deconstructed view of the elements of an EMS and the top two business drivers for possible adoption of cloud technology. For each element of the EMS, the frequency execution and the required roundtrip execution time are also specified (for a general understanding of operational requirements). Next, each element is assigned a risk factor, in particular the overall response time of each application as well as its criticality to real-time operations are defined. High risk applications are defined here as those applications that the operators rely heavily upon that if rendered unavailable could have a significantly adverse impact to BPS reliability in a short period of time. With these two indicators, the team determined which elements could possibly be moved to the cloud and whether that would be a local, hybrid or full cloud implementation. This table is intended as a high-level illustration for entities to consider based on their own risk tolerance.

Table A.1: Deconstructing EMS for Cloud Evaluation

Deconstructed View of the Solution Area	Top Two Business Drivers				Frequency of Execution	Required Roundtrip Execution Time[12]	High Risk Application[13]	Cloud vs. Hybrid vs. Local
	Agility/CTI	Cost Savings	Resilience	Scalability				
Front End Processor					millisecond	millisecond	Yes	Local
SCADA					millisecond	1 second	Yes	Local
ICCP					millisecond	millisecond	Yes	Local
Automatic Generation Control (AGC)					2 seconds	< 1 second	Yes	Local
Nonlinear State Estimation (SE)					1 to 5 minutes	< 30 seconds	Yes	Hybrid
Real-Time Contingency Analysis (RTCA)					1 to 5 minutes	< 60 seconds	Yes	Hybrid
RTLODF (Real-Time Line Outage Distribution Factor)			Y	Y	1 to 5 minutes	< 5 seconds	No	Cloud
Adapters to DMS or Market applications			Y	Y	1 to 5 minutes	< 5 seconds	No	Cloud
Outage Management			Y	Y	By request	< 5 seconds	No	Cloud
Power flow			Y	Y	By request	< 10 seconds	No	Cloud
Stability Analysis (voltage and transient)		Y		Y	5 minutes for voltage 15 minutes for transient	< 5 minutes for voltage < 15 minutes for transient	No	Cloud

---

[12] This is the roundtrip time for the application to execute completely including data input, computation, and results output, with all delays and communications.

[13] High risk applications are defined here as those applications that the operators rely heavily upon that if rendered unavailable could have a significantly adverse impact to BPS reliability in a short period of time.

Table A.1: Deconstructing EMS for Cloud Evaluation

Deconstructed View of the Solution Area	Top Two Business Drivers				Frequency of Execution	Required Roundtrip Execution Time[12]	High Risk Application[13]	Cloud vs. Hybrid vs. Local
	Agility/CTI	Cost Savings	Resilience	Scalability				
Volt-VAR Optimization/Dispatch		Y		Y	10 minutes	< 5 minutes	No	Cloud
Dashboard Visualization						<1 second		
Linear SE			Y	Y	60 seconds	< 10 seconds	No	Cloud
PMU/Wide Area Monitoring System (WAMS)			Y	Y	5 seconds	< 1 second		Cloud

Key Takeaways of Table Exercise

The table above shows that once an EMS is deconstructed, its functions do not all have the same critical requirements of speed/performance and nor do they share the same risk. Traditionally an EMS is a monolithic application responsible for executing all functions. The performance requirements and risk of an EMS as a monolithic application comes from its most demanding functions such as SCADA, AGC and ICCP, etc. However, if an EMS was designed and built as a collection of microservices where each EMS function was represented by its own highly scalable microservice then a utility can decide where each function runs based on its individual risk and speed/performance requirement. This approach opens the door to the use of virtualization, containers, distributed processing, and cloud technology without putting to risk critical operations. Figure A.1 shows an example of a potential EMS application architecture between a CSP cloud environment and on-premises.

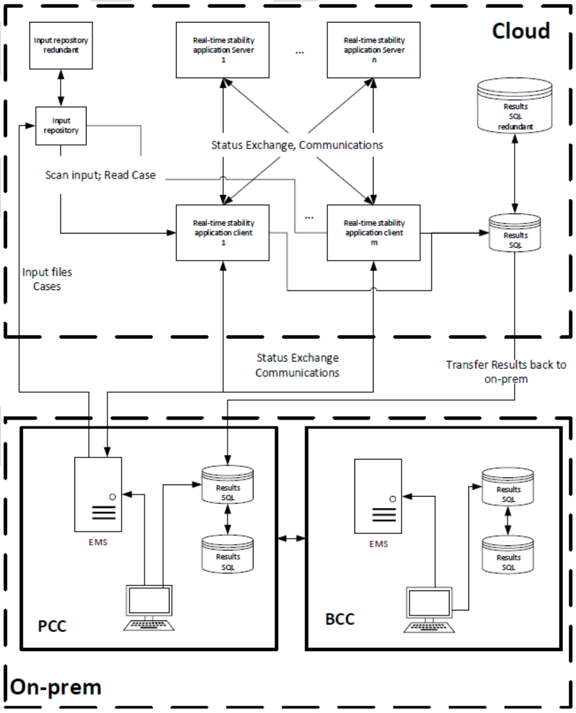


Figure A.1: System Architecture for Cloud Technology for Stability Study Applications

Appendix B: Explanation of BROS and CIP-002-5.1a

The scope of the CIP Cyber Security Reliability Standards is restricted to BES cyber systems that would impact the reliable operation of the BES. In order to identify BES cyber systems, Responsible Entities determine whether the BES cyber systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the initial scope for consideration includes only those BES cyber systems and their associated BES cyber assets that perform or support the reliable operation of the BES. The definition of BES cyber asset provides the basis for this scoping.

CIP-002-5.1a requires that applicable Responsible Entities categorize their BES cyber systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES." Responsibility for the reliable operation of the BES is spread across all Regional Entity registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES cyber systems that would be in scope. Responsible Entities use Table B.1 from CIP-002-5.1a to determine applicable BES reliability operations services (BROS) according to their Function Registration type.

Table B.1: Entity Registration and the BROS

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Appendix C: References

This document is not intended to serve as a detailed and technical reference for cloud technology; rather, it is intended to provide guidance and considerations for industry adopting cloud technology moving forward in a secure and reliable manner. A key goal of this document is to help bridge the gap between engineering and security considerations, and better integrate these concepts holistically. The following are links to reference documents that provide more detailed information related to the concepts described in this document:

- *NERC Security Guideline for the Electricity Sector - Supply Chain Risks Related to Cloud Service Providers*

  https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Cloud_Computing.pdf

- *NERC Security Guideline for Electricity Sector Primer for Cloud Solutions and Encrypting BCSI*

  https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline_BCSI_Cloud_Encryption.pdf

- NATF Energy Sector Supply Chain Risk Questionnaire:

  https://www.natf.net/industry-initiatives/supply-chain-industry-coordination

- AWS *The Utility Executive's Guide to Cloud Security*

  https://d2908q01vomqb2.cloudfront.net/c5b76da3e608d34edb07244cd9b875ee86906328/2020/08/10/AWS-Utility-Executive-Guide-to-Cloud-Security-1.pdf

- AWS *Power & Utility Path to Production in the Cloud*

  https://d2908q01vomqb2.cloudfront.net/c5b76da3e608d34edb07244cd9b875ee86906328/2021/01/04/AWS-Power-and-Utility-Path-to-Production-in-the-Cloud-1.pdf

- IEEE Report on Practical Adoption of Cloud Computing in Power Systems

  https://resourcecenter.ieee-pes.org/publications/technical-reports/PES_TP_TR92_AMPS_012822.html

- NATF Supply Chain Security Assessment Model

  https://www.natf.net/industry-initiatives/supply-chain-industry-coordination

- MITRE ATT&CK® Matrix for cloud-based techniques, and industrial control systems (ICS)

  https://attack.mitre.org/matrices/enterprise/cloud/

  https://attack.mitre.org/matrices/ics/

Appendix D: Contributors

Contributors to this whitepaper include members of NERC, the Regional Entities, SITES, and other industry stakeholders. Contributions include research, discussion, writing, and editing. A special thank you goes to AWS staff for their significant collaborative efforts and contributions to this whitepaper. In alphabetical order, the list of contributors include the following individuals:

Whitepaper Contributors			
Name	**Name**	**Name**	**Name**
Abhineet Parchure	David Hartley	Karl Perman	Ryan Carlson
Alejandro Gonzalez	David Metheny	Katherine Street	Ryan Quint
Andrea Koch	Doug Peterchuck	Kristine Martz	Sean Crimmins
Anthony Pearce	Eric Carriere	Larry Collier	Scott Pelfrey
Ashwini Paranjape	Eric Chen	Maggy Powell	Sean Randles
Barry Jones	Ian King	Manu Parashar	Song Zhang
Barry Kuehnle	James Ball	Marc Child	Stan Hoptroff
Benny Naas	Jay Cribb	Marisa Hecht	Stephanie Lawrence
Brenda Davis	Jay Moser	Michael Cloud	Steven Dougherty
Brent Sessions	Jeffrey Sykes	Michael Sanders	Suzanne Black
Brian Hogue	Jeremiah Miller	Mike Unum	Thomas Peterson
Casey Werth	Jerrod Montoya	Morgan King	Thomas Standifur
Chris Holmquest	Jerry Reed	Muralidhar Cheruvu	Tom Hofstetter
Curtis Dorcheus	John Biasi	Philippe Comperon	Tracey Stewart
Dan Goodlett	John Lemmon	Pierre Janse van Rensburg	Wally Magda
Dan Goyne	John Porter	Ranjan Banerji	Wei Qiu
Dan Grundman	Joseph Baugh	Ravi Pradhan	Xiaochuan Luo
Danny Johnson	Joseph Januszewski	Roger Hales	Xing Wang
Dave Sopata	Joyce Harris	Ron Ross	Zach Trublood

White Paper Bulk Electric System Operations in Cloud

Larry Collier, SITES Secretary, NERC
Marc Child, RSTC Sponsor
Reliability and Security Technical Committee Meeting
September 20, 2023

RELIABILITY | RESILIENCE | SECURITY

Purpose

- This whitepaper informs on:
  - Cloud Concepts – IaaS/PaaS/SaaS, Overlay vs Underlay, and Geographic Region Data Availability
  - Viable Bulk Electric System (BES) Operations use cases for cloud technologies through both cloud service providers (CSPs) and independent software vendors
  - Considerations for technology requirements, including cloud security through concepts of shared security responsibility models and shared security assurance
  - Software and communication architecture resiliency challenges
  - Challenges with current NERC Critical Infrastructure Protection (CIP) standards, ability to facilitate compliance evidence for audits,
  - Evaluation of third party certification and accreditations to cloud security frameworks for CSPs and explores viability of use for NERC CIP audits.
- The collaboration and content of this paper has inspired one or more industry SARs both currently submitted and upcoming

Background

- Drivers
  - Digitalization bringing large amounts of data. Cloud offers scalable compute and storage to enable advanced analytics
  - Technology and security industry moving towards cloud in solutions and training/skillsets
  - Enabling innovation to drive a more resilient energy infrastructure with highly redundant multi-region compute and storage
  - Due to infrastructure and software trends, costs are expected to rise for on-premises deployments
  - On-premises software may see less support as vendors move onto more popular cloud products
  - Use of cloud infrastructure, services, and expertise enables utilities to focus on core business activities
  - Emerging grid technologies already integrating with cloud (Virtual Power Plant (VPP), DER Aggregators, EV Charging and Vehicle-To-Grid (V2G)

Approach

- This white paper serves to:
  - Educate on cloud fundamental concepts
  - Dispel misconceptions
  - Spread awareness of use cases
  - Emphasize a safe and secure approach to adopting cloud for BES Operations
  - Build off "BCSI in the Cloud" and evaluate the next level of regulatory compliance challenges
  - Provide industry recommendations to address CSP-based cloud technology use under NERC CIP
  - Provoke additional thought leadership

Restatement of Request

SITES requests the RTSC to **approve** this whitepaper for publishing.

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

2023 Frequency Response Annual Analysis

TBD 2023

This report was approved by the Resources Subcommittee on XX- XX, 2023.

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

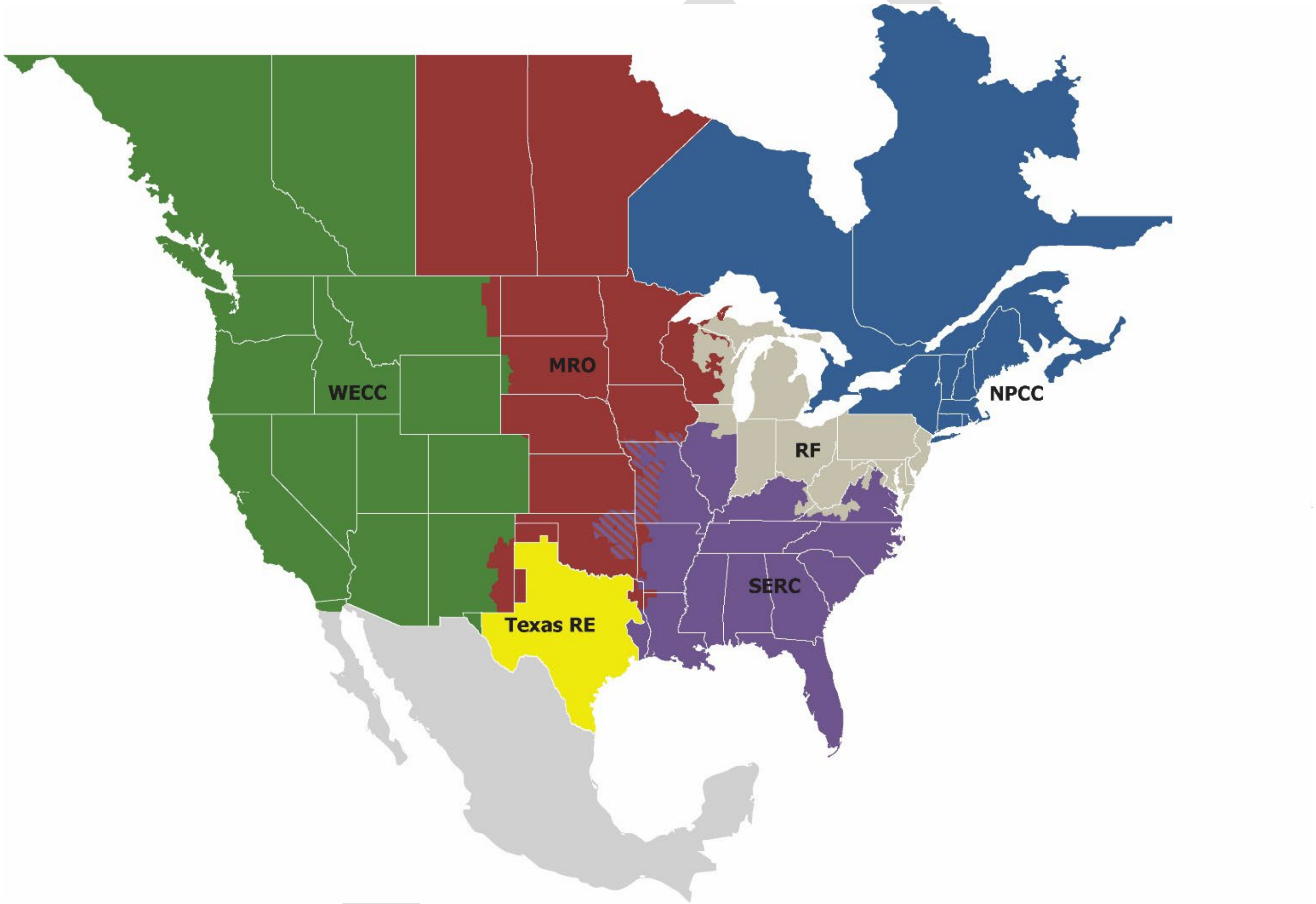
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of NERC and the six Regional Entities, is a highly reliable, resilient, and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six Regional Entities as shown on the map and in the corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Executive Summary

This report is the 2023 annual analysis of frequency response performance for the administration and support of *NERC Reliability Standard BAL-003-2 – Frequency Response and Frequency Bias Setting,*[1] effective December 1, 2020. It provides an update to the statistical analyses and calculations contained in the *2012 Frequency Response Initiative Report*[2] that was approved by the NERC Resources Subcommittee (RS) and the technical committee, which predated the Reliability and Security Technical Committee (RSTC) and was accepted by the NERC Board of Trustees (Board).

This report is prepared by NERC staff[3] and contains the annual analysis, calculation, and recommendations for the interconnection frequency response obligation (IFRO) for each of the four electrical Interconnections of North America for the operating year (OY) 2024 (December 2023 through November 2024). Below are the key findings and recommendations contained in this report.

Key Findings

Starting Frequency

The starting frequency for the calculation of IFROs, shown in **Table 1.1**, is the fifth percentile of the 5-year probability distribution of the respective interconnection frequency, representing a 95% chance that frequencies will be at or above that value at the start of any frequency event. The starting frequency remained the same for the Eastern Interconnection (EI) at 59.971 Hz, increased slightly for the Western Interconnection (WI) from 59.969 Hz to 59.970 Hz, remained the same for the Texas Interconnection (TI) at 59.970 Hz and Québec Interconnection (QI) at 59.965 Hz.

Frequency Probability Density Functions

The standard deviation is a measure of the dispersal of frequency values around the mean value; a smaller standard deviation indicates tighter concentration around the mean value and more stable performance of Interconnection frequency. Analysis of the frequency probability density functions shows that in the EI the standard deviation consistently increased from 2018 to 2021 and decreased from 2021 to 2022 but still remained higher than in 2018-2020. In the other Interconnections, standard deviations have been flat (Texas) or decreasing (Western and Québec). Comparisons of annual frequency profiles for each Interconnection are shown in **Figures 1.6–1.9**.

Interconnection Performance and the Comparison of Mean Value A, B, and Point C

Table 2.6 shows a comparison of mean Value A, mean Value B, and mean Point C that is illustrative of Interconnection performance during low frequency events over the previous OY and as compared to the 2016 OY in which the IFRO values were frozen. Loss of load events have been excluded from the data in **Table 2.6**. All four Interconnections show an increase in mean Value B and a decrease in the mean (A-B), indicating improved performance during the stabilizing period of frequency events. All four Interconnections show either an increase or no change in mean Point C as well as a decrease or no change in mean (A–C), indicating improved performance during the arresting period of frequency events. This performance data demonstrates that the higher calculated IFROs are due to improved stabilizing period performance and not due to a decline in the performance of the Point C nadir.

---

[1] http://www.nerc.com/pa/Stand/Reliability%20Standards/BAL-003-2.pdf

[2] http://www.nerc.com/docs/pc/FRI_Report_10-30-12_Master_w-appendices.pdf

[3] Prepared by the NERC Standards and Engineering organization.

Recommendations

NERC provides the following recommendation for the administration of *Standard BAL-003-2*[1] for OY 2024 (December 1, 2023, through November 30, 2024):

- The IFRO value for the TI will change by -68 MW/0.1 Hz due to an increase in Credit for Load Resources (CLR). Therefore, the recommended IFRO for TI is -395 MW/ .1 Hz.
- NERC requests that the Recommended IFRO values calculated in this report in accordance with BAL-003-2 and shown in Table **ES.1** be approved for implementation in OY 2023. NERC, in collaboration with the RS, shall continue to monitor and evaluate the impacts on BPS reliability as a result of changes in IFRO values.

Table ES.1: Recommended IFROs for OY 2024

	Eastern (EI)	Western (WI)	Texas (TI)	Québec (QI)	Units
MDF[4]	0.420	0.280	0.405	0.947	Hz
RLPC[5]	3,875	2,918	2,805	2,000	MW
CLR	N/A	N/A	1,204	N/A	MW
Calculated IFRO	-923	-1,042	-395	-211	MW/0.1 Hz
Recommended IFROs[6]	**-923**	**-1,042**	**-395**	**-211**	**MW/0.1 Hz**

---

[4] The Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard, Version II, provided in the approved ballot for BAL-003-2, specifies that, "MDF is the Maximum Delta Frequency for the specific interconnection as determined in the 2017 Frequency Response Annual Analysis (FRAA)."

[5] BAL-003-2, Attachment A specifies that Resource Loss Protection Criteria (RLPC) be based on the two largest potential resource losses in an interconnection. This value is required to be evaluated annually.

[6] BAL-003-2 requires that the EI IFRO will be stepped down to its calculated value over three years. The maximum reduction is limited to 100 MW/0.10 Hz annually.

Introduction

This report, prepared by NERC staff,[7] contains the annual analysis, calculation, and recommendations for the IFRO for each of the four Interconnections of North America for the OY 2024 (December 2023 through November 2024). This analysis includes the following information:

- Statistical analysis of Interconnection frequency characteristics for the OYs 2018 through 2022 (December 1, 2017, through November 30, 2022)
- Analysis of frequency profiles for each Interconnection
- Calculation of adjustment factors from BAL-003-2 frequency response events

This year's frequency response analysis builds upon the work and experience from performing such analyses since 2013. As such, there are several important things that should be noted about this report:

- The University of Tennessee–Knoxville FNET[8] data used in the analysis has seen significant improvement in data quality, simplifying and improving annual analysis of frequency performance and ongoing tracking of frequency response events. In addition, NERC uses data quality checks to flag additional bad one-second data, including bandwidth filtering, least squares fit, and derivative checking.
- As with the previous year's analysis, all frequency event analysis uses subsecond data from the FNET system frequency data recorders (FDRs). This eliminates the need for the CC_{ADJ} factor originally prescribed in the *2012 Frequency Response Initiative Report*[9] because the actual frequency nadir was accurately captured.
- The Frequency Response Analysis Tool[10] is being used by the NERC Power System Analysis group for frequency event tracking in support of the NERC Frequency Working Group and RS. The tool has streamlined interconnection frequency response analysis. The tool provides an effective means of determining frequency event performance parameters and generating a database of values necessary for calculation of adjustment factors.

This report contains numerous references to Value A, Value B, and Point C, which are defined in NERC *BAL-003-2.*[1] As such, it is important to understand the relationship between these variables and the basic tenants of primary and secondary frequency control.

The Arresting, Rebound, Stabilizing, and Recovery Periods of a frequency event following the loss of a large generation resource are shown in Figure I.1. Value A and Value B are average frequencies from t-16 to t-2 seconds and t+20 to t+52 seconds, respectively, as defined in NERC *BAL-003-2*. Point C is the lowest frequency experienced within the first 20 seconds following the start of a frequency event. A Point C' value may exist if frequency falls below the original Point C nadir or Value B after the end of the 20–52 second Stabilizing Period.

---

[7] Prepared by the Power System Analysis and Advanced System Analytics & Modeling departments.

[8] Operated by the Power Information Technology Laboratory at the University of Tennessee, FNET is a low-cost, quickly deployable GPS-synchronized wide-area frequency measurement network. High-dynamic accuracy FDRs are used to measure the frequency, phase angle, and voltage of the power system at ordinary 120 V outlets. The measurement data are continuously transmitted via the Internet to the FNET servers hosted at the University of Tennessee and Virginia Tech.

[9] http://www.nerc.com/docs/pc/FRI_Report_10-30-12_Master_w-appendices.pdf

[10] Developed by Pacific Northwest National Laboratory

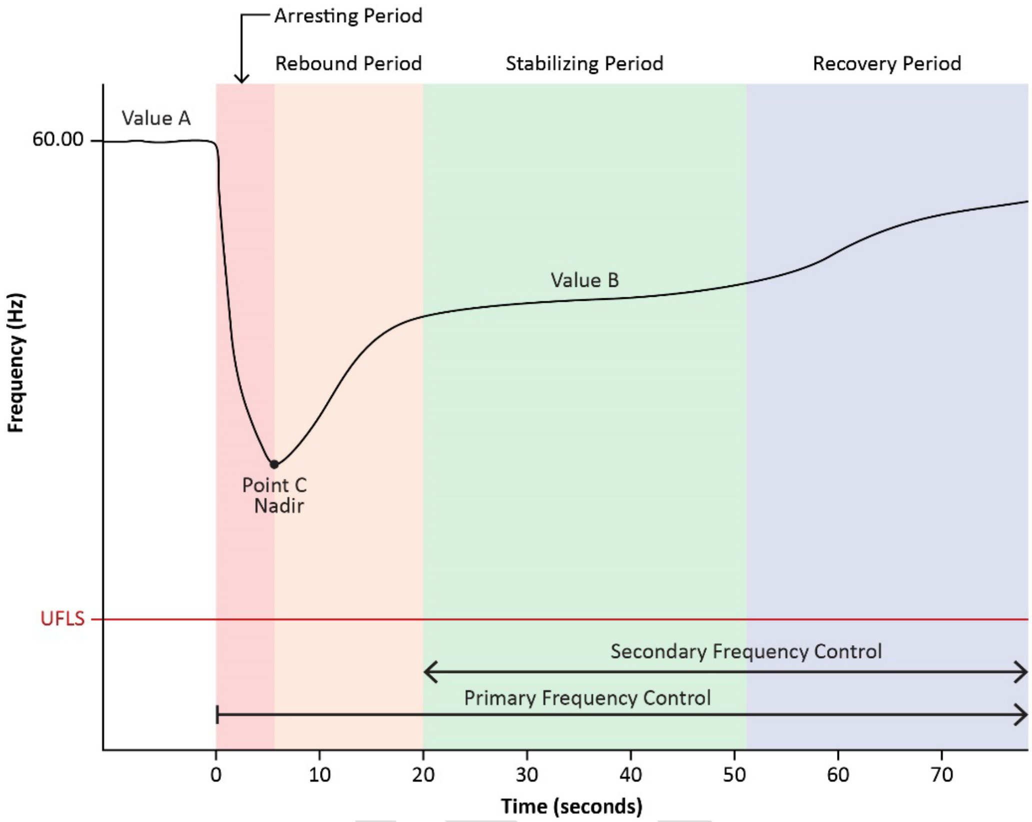


Figure I.1: Primary and Secondary Frequency Control

Primary Frequency Control: This is the action by the Interconnection to arrest and stabilize frequency in response to frequency deviations and has three-time components: the Arresting Period, Rebound Period, and Stabilizing Period. These terms are defined below:

- **Arresting Period:** This is the time from time zero (Value A) to the time of the nadir (Point C) and is the combination of system inertia, load damping, and the initial primary control response of resources acting together to limit the duration and magnitude of frequency change. It is essential that the decline in frequency is arrested during this period to prevent activation of automatic under-frequency load shedding (UFLS) schemes in the Interconnection.
- **Rebound Period:** This includes the effects of governor response in sensing the change in turbine speed as frequency increases or declines, causing an adjustment to the energy input of the turbine's prime mover. This can also be impacted by end-user customers or other loads that are capable of self-curtailment due to local frequency sensing and control during frequency deviations.
- **Stabilizing Period:** This is the third component of primary frequency control following a disturbance when the frequency stabilizes following a frequency excursion. Value B represents the interconnected system frequency at the point immediately after the frequency stabilizes primarily due to governor action but before the contingent control area takes corrective automatic generation control action.

Chapter 1: Interconnection Frequency Characteristic Analysis

Annually, NERC staff performs a statistical analysis, as detailed in the *2012 Frequency Response Initiative Report,*[11] of the frequency characteristics for each of the four Interconnections. That analysis is performed to monitor the changing frequency characteristics of the Interconnections and to statistically determine each Interconnection's starting frequency for the respective IFRO calculations. For this report's analysis, one-second frequency data[12] from OYs 2018–2022 (December 1, 2017, through November 30, 2022) was used.

Frequency Variation Statistical Analysis

The 2023 frequency variation analysis was performed on one-second frequency data for 2018–2022 and is summarized in **Table 1.1**. This variability accounts for items like time-error correction (TEC), variability of load, interchange, and frequency over the course of a normal day. It also accounts for all frequency excursion events.

The starting frequency is calculated and published in this report for comparison and informational purposes. Starting frequencies are evaluated annually and indicate no need to change the Maximum Delta Frequency for OY 2024.

Table 1.1: Interconnection Frequency Variation Analysis 2018-2022

Value	Eastern	Western	Texas	Québec
Number of Samples	157,099,132	157,065,244	156,955,420	132,125,710
Filtered Samples (% of total)	99.58	99.56	99.49	83.75
Expected Value (Hz)	59.999	59.999	59.999	60.000
Variance of Frequency (σ^2)	0.00026	0.00030	0.00029	0.00043
Standard Deviation (σ)	0.01627	0.01744	0.01691	0.02077
50% percentile (median)[13]	59.999	59.999	60.004	59.998
Starting Frequency (F_{START}) (Hz)	**59.971**	**59.97**	**59.97**	**59.965**

The starting frequency is the fifth percentile of the 5-year probability distribution of the respective interconnection frequency based on the statistical analysis, representing a 95% chance that frequencies will be at or above that value at the start of any frequency event. Since the starting frequencies encompass all variations in frequency, including changes to the target frequency during TECs, the need to expressly evaluate TEC as a variable in the IFRO calculation is eliminated.

Figures 1.1–1.4 show the probability density function (PDF) of frequency for each Interconnection. The vertical black line indicates the fifth-percentile frequency; the interconnection frequency will statistically be greater than that value 95% of the time; this value is used as the starting frequency.

---

[11] https://www.nerc.com/docs/pc/FRI_Report_10-30-12_Master_w-appendices.pdf

[12] One-second frequency data for the frequency variation analysis is provided by UTK. The data is sourced from FDRs in each Interconnection. The median value among the higher-resolution FDRs is down-sampled to one sample per second, and filters are applied to ensure data quality.

[13] Note regarding the EI median frequency that: with fast time error corrections the median value is around but slightly below 60 Hz. Without these corrections the median would be above 60 Hz.

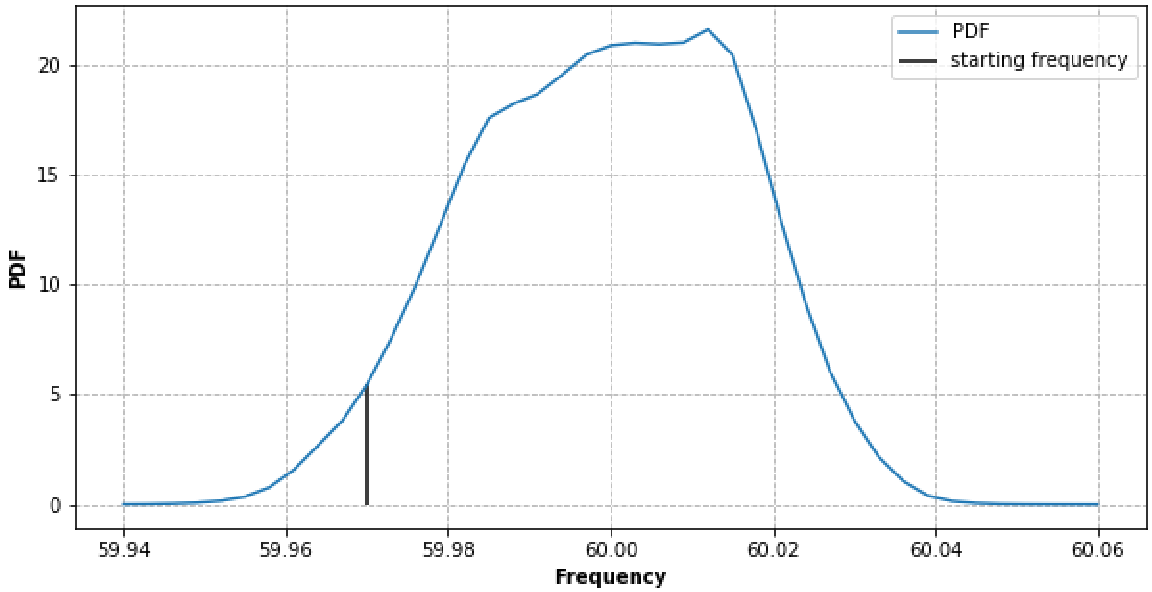


Figure 1.1: Eastern Interconnection 2018–2022 Probability Density Function of Frequency

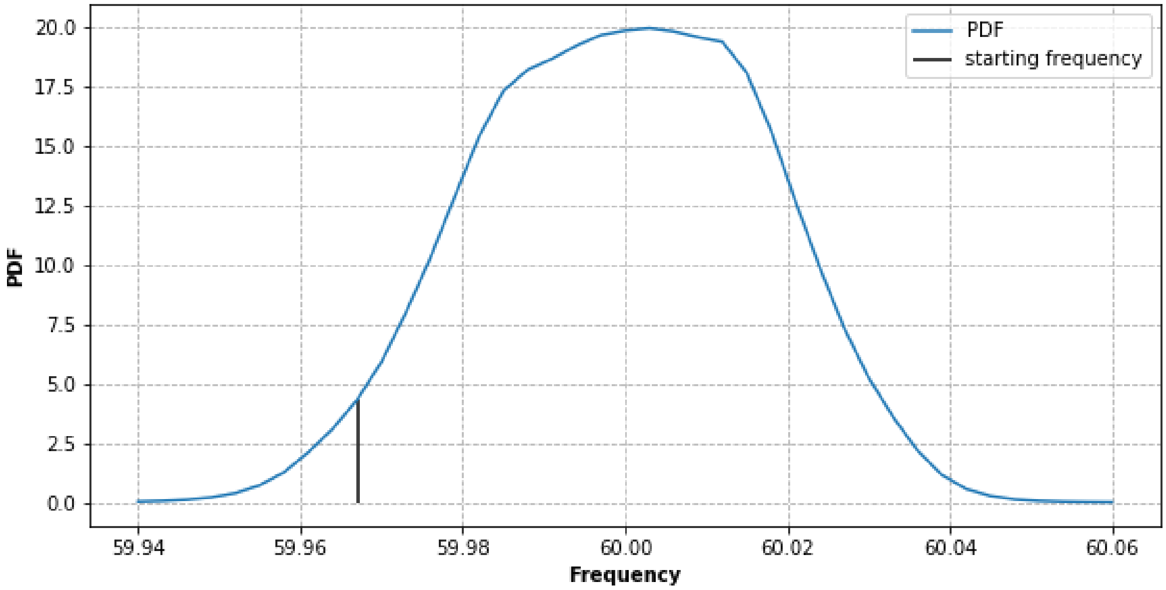


Figure 1.2: Western Interconnection 2018–2022 Probability Density Function of Frequency

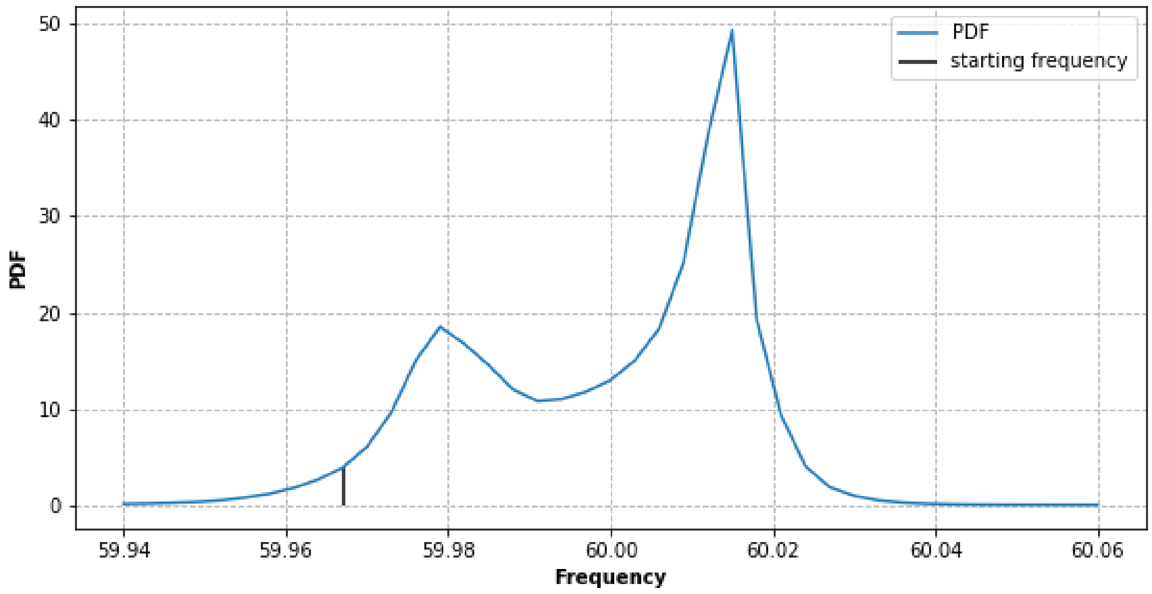


Figure 1.3: Texas Interconnection 2018–2022 Probability Density Function of Frequency

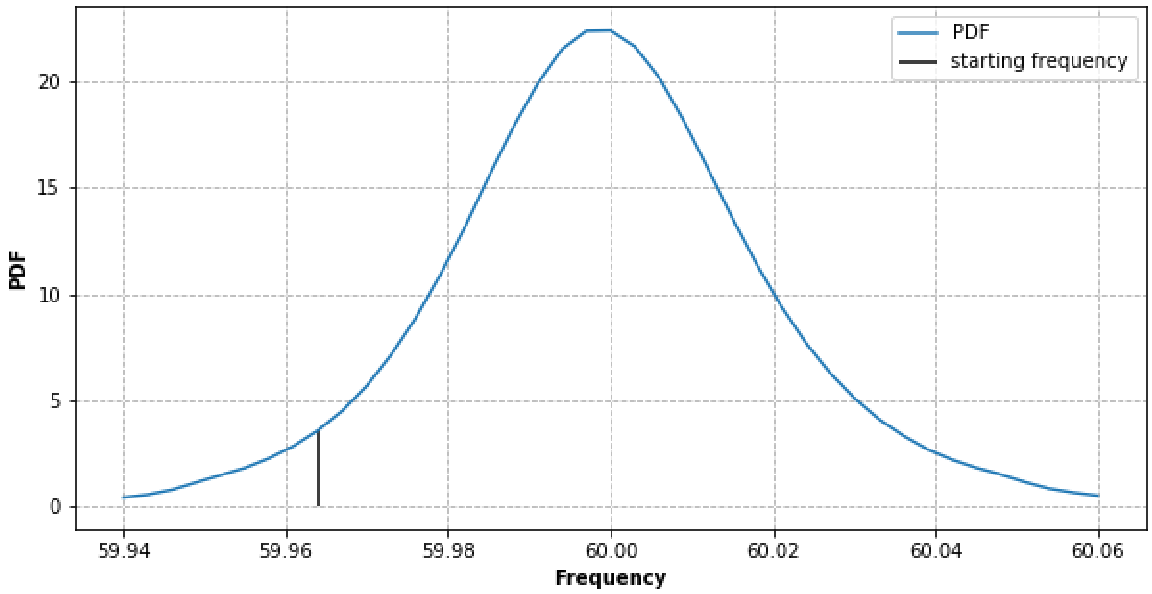


Figure 1.4: Québec Interconnection 2018–2022 Probability Density Function of Frequency

Figures 1.1–1.4 show the PDF of frequency for each Interconnection. The Interconnection frequency will statistically be greater than that value 95% of the time; this value is used as the starting frequency. Figure 1.5 shows a comparison of the PDF for all Interconnections.

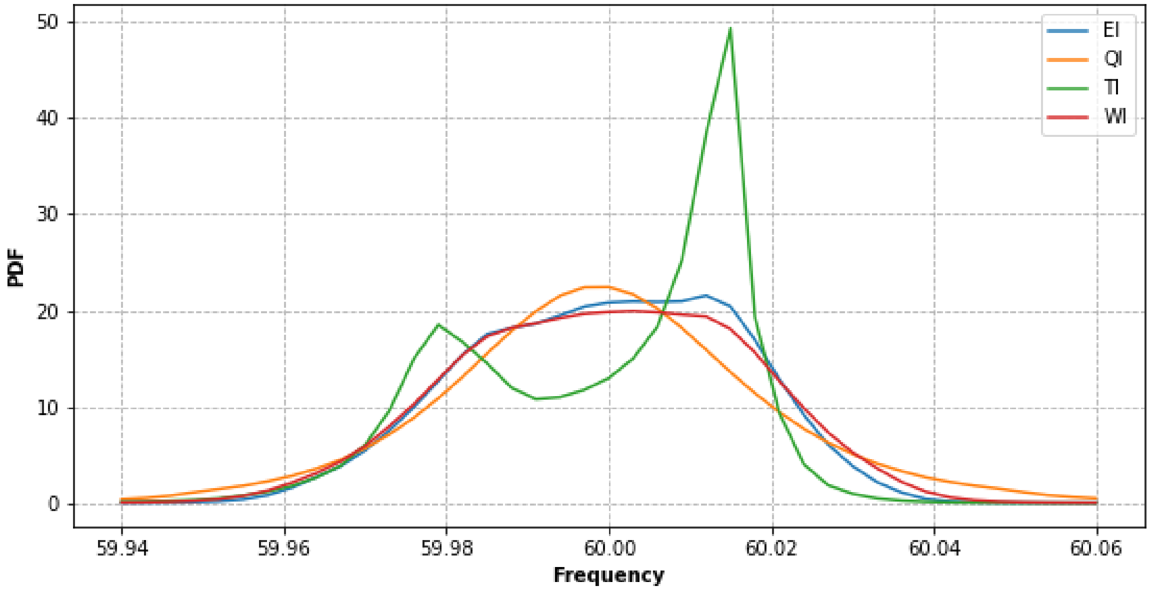


Figure 1.5: Comparison of 2018–2022 Interconnection Frequency PDFs

Variations in Probability Density Functions

The following is an analysis of the variations in probability density functions of the annual distributions of Interconnection frequency for years 2018–2022. **Table 1.2** lists the standard deviation of the annual Interconnection frequencies.

Table 1.2: Interconnection Standard Deviation by Year

Interconnection	2018	2019	2020	2021	2022
Eastern	0.0161	0.0162	0.0163	0.0164	0.0164
Western	0.0186	0.0174	0.0176	0.0174	0.0172
Texas	0.0162	0.0165	0.0174	0.0176	0.0169
Québec	0.0203	0.0204	0.0208	0.0223	0.0187

In the EI, the standard deviation continued to increase in 2022 compared to 2018–2020. The standard deviation decreased in the QI, the TI, and the WI in 2022 compared to 2021. As standard deviation is a measure of dispersion of values around the mean value, the increasing standard deviations indicate reduced concentration around the mean value and less stable performance of the interconnection frequency. Comparisons of annual frequency profiles for each Interconnection are shown in **Figures 1.6–1.9.**

Eastern Interconnection Frequency Characteristic Changes

The increase in standard deviation for the EI frequency characteristic in 2022 is shown in **Figure 1.6**. Statistical skewness (S)[14] decreased in 2022 (S = -0.15) as compared to 2020 and 2021 (S = -0.17 and -0.16, respectively). NERC,

---

[14] The skewness (S) is a measure of asymmetry of a distribution. A perfectly symmetric distribution has S=0. The sign indicates where a longer tail of the distribution is. The negatively-skewed distribution has a longer left tail, and its curve leans to the opposite direction (to the right).

in coordination with its technical committees, continues to evaluate this phenomenon and its impact, if any, on BPS reliability.

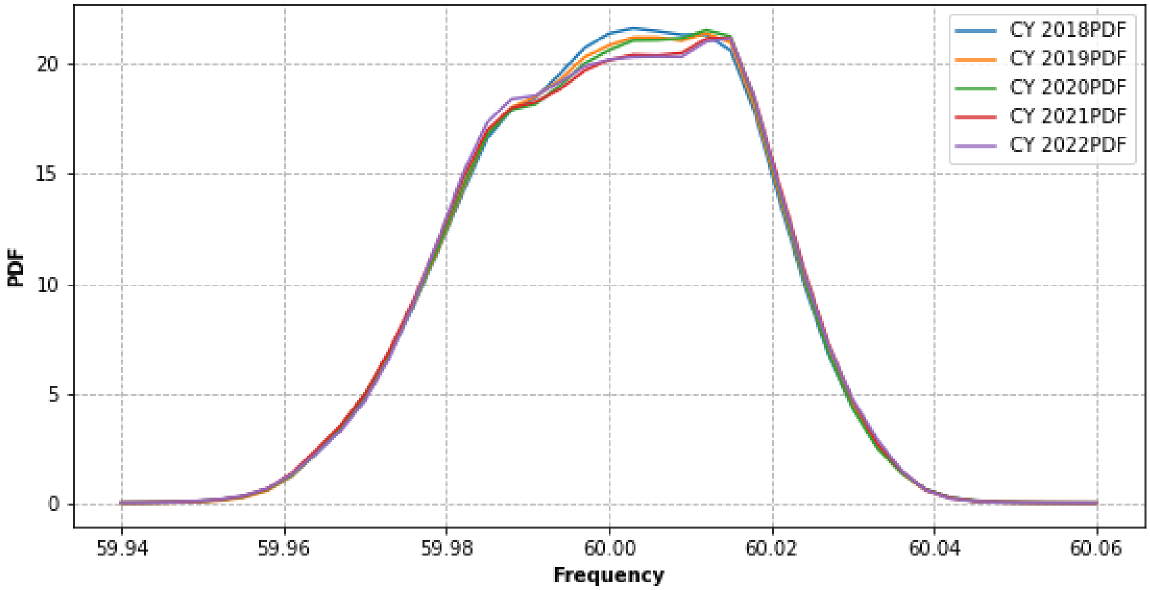


Figure 1.6: Eastern Interconnection Frequency Probability Density Function by Year

---

Algebraically, it means that the frequency values that are smaller than its mean are spread farther from the mean than the values greater than the mean or that there is more variability in lower values of the frequency than in higher values of the frequency.

Western Interconnection Frequency Characteristic Changes

There was an observable change in the frequency distribution for the WI in 2021 that includes some skewness as shown in **Figure 1.7**.

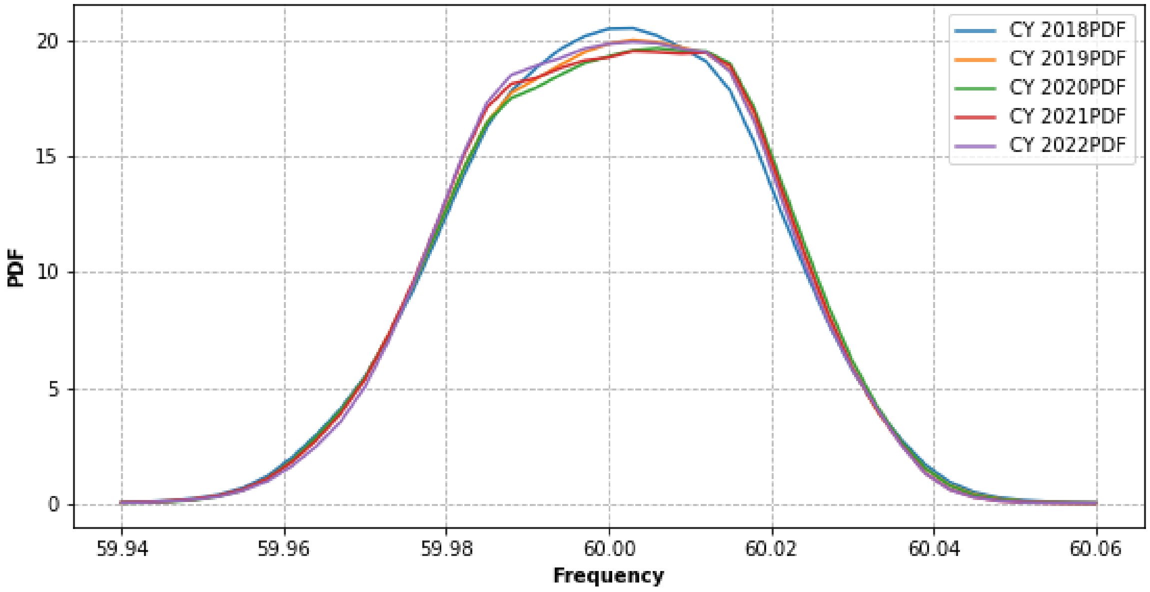


Figure 1.7: Western Interconnection Frequency Probability Density Function by Year

Texas Interconnection Frequency Characteristic Changes

Standard TRE BAL-001[15] went into full effect in April 2015 and caused a dramatic change in the probability density function of frequency for Texas Interconnection in 2015 and 2016. This standard requires all resources in Texas Interconnection to provide proportional, nonstep primary frequency response with a ±17 mHz dead-band. As a result, any time frequency exceeds 60.017 Hz, resources automatically curtail themselves. That has resulted in far less operation in frequencies above the dead-band since all resources, including wind and solar, are backing down. It is exhibited in **Figure 1.8** as a probability concentration around 60.015 Hz. Similar behavior is not exhibited at the low dead-band of 59.983 Hz because most wind and solar resources are operated at maximum output and cannot increase output when frequency falls below the dead-band.

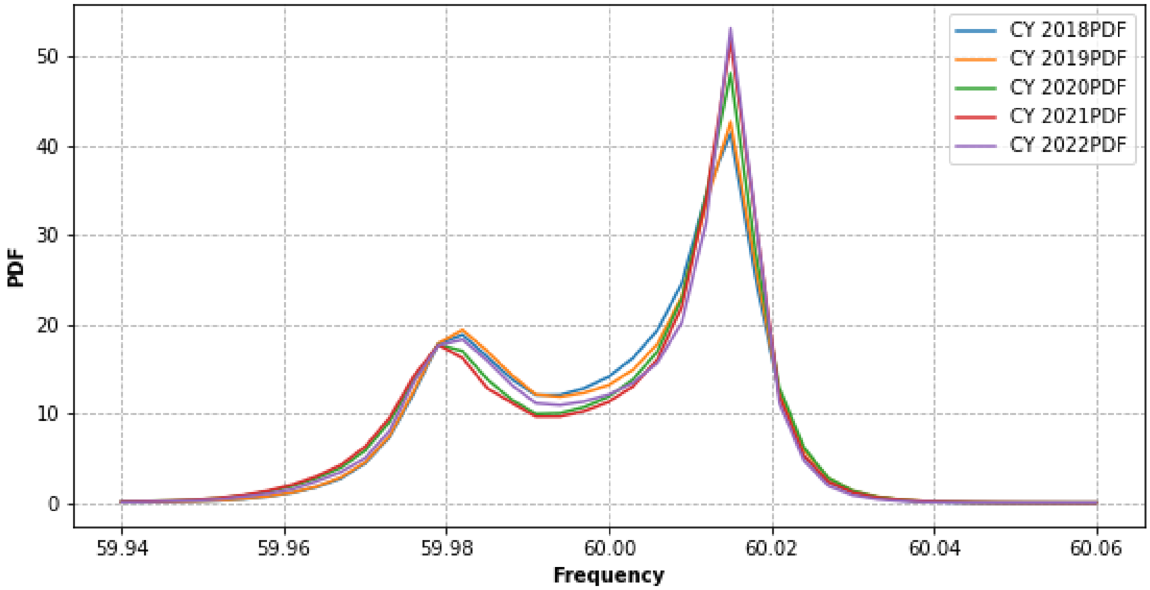


Figure 1.8: Texas Interconnection Frequency Probability Density Function by Year

---

[15] http://www.nerc.com/pa/Stand/Reliability%20Standards/BAL-001-TRE-1.pdf

Quebec Interconnection Frequency Characteristic Changes

There were no observable changes in the shape of the distribution for the QI as shown in **Figure 1.9**.

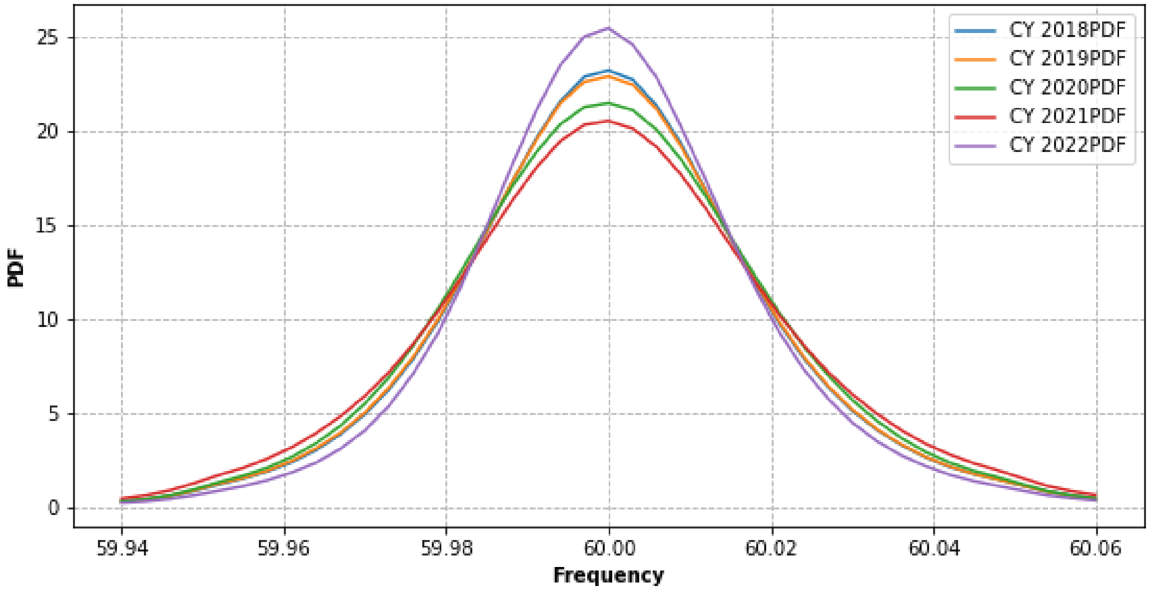


Figure 1.9: Québec Interconnection Frequency Probability Density Function by Year

Chapter 2: Determination of Interconnection Frequency Response Obligations

With this report the calculation of the IFROs is determined by recently approved BAL-003-2. Previously, the calculation involved a multifaceted process that employed statistical analysis of past performance; analysis of the relationships between measurements of Value A, Point C, and Value B; and other adjustments to the allowable frequency deviations and resource losses used to determine the recommended IFROs. Refer to the *2012 Frequency Response Initiative Report* for additional details on the development of the IFRO and the adjustment calculation methods.[16] This report includes information that serves to transition from the old to the new method.

Tenets of IFRO

The IFRO is the minimum amount of frequency response that must be maintained by an Interconnection. Each Balancing Authority (BA) in the Interconnection is allocated a portion of the IFRO that represents its minimum annual median performance responsibility. To be sustainable, BAs susceptible to islanding may need to carry additional frequency-responsive reserves to coordinate with their UFLS plans for islanded operation.

A number of methods to assign the frequency response targets for each Interconnection can be considered. Initially, the following tenets should be applied:

- A frequency event should not activate the first stage of regionally approved UFLS systems within the Interconnection.
- Local activation of first-stage UFLS systems for severe frequency excursions, particularly those associated with delayed fault-clearing or in systems on the edge of an Interconnection, may be unavoidable.
- Other frequency-sensitive loads or electronically coupled resources may trip during such frequency events as is the case for photovoltaic (PV) inverters.
- It may be necessary in the future to consider other susceptible frequency sensitivities (e.g., electronically coupled load common-mode sensitivities).

UFLS is intended to be a safety net to prevent system collapse due to severe contingencies. Conceptually, that safety net should not be utilized for frequency events that are expected to happen on a relatively regular basis. As such, the resource loss protection criteria were selected in accordance with BAL-003-2 to avoid violating regionally approved UFLS settings.

Interconnection Resource Loss Protection Criteria (RLPC)

BAL-003-2 introduced the Interconnection Resource Loss Protection Criteria (RLPC) to replace the Resource Contingency Protection Criteria used previously. It is based on resource loss in accordance with the following process:

NERC will request BAs to provide their two largest resource loss values and largest resource loss due to an N-1 or N-2 remedial action scheme (RAS) event or largest resource as described above. This will facilitate comparison between the existing Interconnection RLPC values and the RLPC values in use. This data submission will be needed to complete the calculation of the RLPC and IFRO.

BAs determine the two largest resource losses for the next OY based on a review of the following items:

---

[16] https://www.nerc.com/comm/OC/BAL0031_Supporting_Documents_2017_DL/FRI_Report_10-30-12_Master_w-appendices.pdf#search=Frequency%20Response%20Initiative%20Report

- The two largest balancing contingency events due to a single contingency identified using system models in terms of loss measured by megawatt loss in a normal system configuration (N-0) (An abnormal system configuration is not used to determine the RLPC).
- The two largest units in the BA area, regardless of shared ownership/responsibility
- The two largest RAS resource losses (if any) that are initiated by single (N-1) contingency events.

The BA provides these two numbers determined above as Resource Loss A and Resource Loss B in the FR Form 1.

The BA should then provide the largest resource loss due to RAS operations (if any) that are initiated by a multiple contingency (N-2) event (RLPC cannot be lower than this value). If this RAS impacts more than a single BA, one BA is asked to take the lead and sum all resources lost due to the RAS event and provide that information.

The calculated RLPC should meet or exceed any credible N-2 resource loss event.

The host BA (or planned host BA) where jointly owned resources are physically located should be the only BA to report that resource. The full ratings of the resource, not the fractional shares, should be reported.

Direct current (dc) ties to asynchronous resources (such as dc ties between Interconnections, or the Manitoba Hydro Dorsey bi-pole ties to their northern asynchronous generation) should be considered as resource losses. DC lines such as the Pacific DC Intertie, which ties two sections of the same synchronous Interconnection together, should not be reported. A single pole block with normal clearing in a monopole or bi-pole high-voltage direct current system is a single contingency.

Calculation of IFRO Values

The IFRO is calculated using the RLPC above (Table 1 from BAL-003-2).

$$IFRO = \frac{RLPC - CLR}{MDF * 10}\ \mathrm{MW/0.1Hz}$$

As specified in the Procedure for ERO Support of Frequency Response and Frequency Bias Setting standard, “MDF is the Maximum Delta Frequency for the specific interconnection as determined in the 2017 Frequency Response Annual Analysis (FRAA).” The BAL-003-2 revision alleviated the adverse impacts of an improving CB_R.

The IFRO for each Interconnection is calculated in this report in **Table 2.5**; note that the calculated value for the EI IFRO is estimated by BAL-003-2 to be stepped down over three years with a reduction of IFRO not to exceed -100 MW/0.10 Hz per year in accordance with BAL-003-2. Collected RLPC data exceeded the estimate at the time BAL-003-2 balloted, and EI IFRO should meet the actual calculated value in only two OYs as a result. That determines the difference between the calculated EI IFRO in **Table 2.5** and the recommended IFRO shown in **Table ES-1** and **Table 2.9**.

Determination of Adjustment Factors

The C-to-B ratio (CB_R) is no longer used in the IFRO method and has been eliminated.

Adjustment for Primary Frequency Response Withdrawal (BC'_{ADJ})

Point C is normally the frequency nadir during the event; however, point C and the nadir may differ if the nadir occurs more than 20 seconds after the start of the event[17]. This lower nadir is symptomatic of primary frequency response withdrawal or squelching by unit-level or plant-level outer loop control systems. Withdrawal is most prevalent in the EI.

To track frequency response withdrawal in this report, the later-occurring nadir is termed Point C,' which is defined as occurring after the Value B averaging period and must be lower than either Point C or Value B.

Primary frequency response withdrawal is important depending on the type and characteristics of the generators in the resource dispatch, especially during light-load periods. Therefore, an additional adjustment to the maximum allowable delta frequency for calculating the IFROs was statistically developed. This adjustment is used whenever withdrawal is a prevalent feature of frequency events.

The statistical analysis is performed on the events with C' value lower than Value B to determine the adjustment factor BC'_{ADJ} to account for the statistically expected Point C' value of a frequency event. These results correct for the influence of frequency response withdrawal on setting the IFRO. Table 2.1 shows a summary of the events for each Interconnection where the C' value was lower than Value B (averaged from T+20 through T+52 seconds) and those where C' was below Point C for OYs 2017 through 2021 (December 1, 2016, through November 30, 2021).

Table 2.1: Statistical Analysis of the Adjustment for C' Nadir (BC'_{adj})

Interconnection	Number of Events Analyzed	C' Lower than B	C' Lower than C	Mean Difference	Standard Deviation	BC'ADJ (95% Quantile)
EI	104	11	5	0.007	0.005	0.015
WI	107	66	1	N/A	N/A	N/A
TI	80	45	5	N/A	N/A	N/A
QI	160	15	8	-0.014	0.010	-0.007

The 15 events detected for QI are for load-loss events; this is indicated by the negative values for the mean difference and the BC'_{ADJ}. The adjustment is not intended to be used for load-loss events.

Although one event with C' lower than Point C was identified in the WI, an adjustment factor is not warranted; only the adjustment factor of 15 mHz for the EI is necessary. Of the 104 frequency events analyzed in the EI, there were 11 events that exhibited a secondary nadir where Point C' was below Value B and 5 events where Point C' was lower than the initial frequency nadir (Point C). These secondary nadirs occur beyond 52 seconds after the start of the event,[18] which is the time frame for calculating Value B.

Therefore, a BC'_{ADJ} is only needed for the EI; no BC'_{ADJ} is needed for the other three Interconnections. This will continue to be monitored moving forward to track these trends in C' performance.

---

[17] The "*Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard*" defines Point C to occur within T+20 seconds.

[18] The timing of the C' occurrence is consistent with outer-loop plant and unit controls, causing withdrawal of inverter-based resource frequency response.

Low-Frequency Limit

The low-frequency limits to be used for the IFRO calculations (**Table 2.2**) should be the highest step in the Interconnection for regionally approved UFLS systems. These values have remained unchanged since the *2012 Frequency Response Initiative Report*.

Table 2.2: Low-Frequency Limits (Hz)

Interconnection	Highest UFLS Trip Frequency
EI	59.5
WI	59.5
TI	59.3
QI	58.5

The highest UFLS set point in the EI is 59.7 Hz in SERC-Florida Peninsula (FP), which was previously FRCC, while the highest set point in the rest of the Interconnection is 59.5 Hz. The SERC-FP 59.7 Hz first UFLS step is based on internal stability concerns and is meant to prevent the separation of the FP from the rest of the Interconnection. SERC-FP concluded that the IFRO starting point of 59.5 Hz for the EI is acceptable in that it imposes no greater risk of UFLS operation for an Interconnection resource loss event than for an internal SERC-FP event.

Protection against tripping the highest step of UFLS does not ensure generation that has frequency-sensitive boiler or turbine control systems will not trip, especially in electrical proximity to faults or the loss of resources. Severe system conditions might drive the combination of frequency and voltage to levels that present some generator and turbine control systems to trip the generator. Similarly, severe rates-of-change occurring in voltage or frequency might actuate volts-per-hertz relays; this would also trip some generators, and some combustion turbines may not be able to sustain operation at frequencies below 59.5 Hz.

Inverter-based resources may also be susceptible to extremes in frequency. Laboratory testing by Southern California Edison of inverters used on residential and commercial scale PV systems revealed a propensity to trip at about 59.4 Hz, about 200 mHz above the expected 59.2 Hz prescribed in IEEE Standard 1547 for distribution-connected PV systems rated at or below 30 kW (57.0 Hz for larger installations). This could become problematic in the future in areas with a high penetration of inverter-based resources.

Credit for Load Resources

The TI depends on contractually interruptible (an ancillary service) demand response that automatically trips at 59.7 Hz by under-frequency relays to help arrest frequency declines. A CLR is made for the resource contingency for the TI.

The amount of CLR available at any given time varies by different factors, including its usage in the immediate past. NERC performed statistical analysis on hourly available CLR over a two-year period from December 2021 through November 2022, like the approach used in the *2015 FRAA* and in the *2016 FRAA*. Statistical analysis indicated that 1204 MW of CLR is available 95% of the time. Therefore, a CLR adjustment of 1204 MW is applied in the calculation of the TI IFRO as a reduction to the RLPC.

TI Credit for Load Resources

Prior to April 2012, the TI was procuring 2,300 MW of responsive reserve service, of which up to 50% could be provided by the load resources with under-frequency relays set at 59.70 Hz. Beginning April 2012, due to a change in market rules, the responsive reserve service requirement was increased from 2,300 MW to 2,800 MW for each hour, meaning load resources could potentially provide up to 1,400 MW of automatic primary frequency response.

Determination of Maximum Allowable Delta Frequencies

Because of the measurement limitation[19] of the BA-level frequency response performance, IFROs must be calculated in "Value B space." Protection from tripping UFLS for the Interconnections based on Point C, Value B, or any nadir occurring after Point C, within Value B, or after T+52 seconds must be reflected in the maximum allowable delta frequency for IFRO calculations expressed in terms comparable to Value B.

Table 2.3 shows the calculation of the maximum allowable delta frequencies for each of the Interconnections. All adjustments to the maximum allowable change in frequency are made to include the following:

- Adjustments for the differences between Point C and Value B
- Adjustments for the event nadir being below Value B or Point C due to primary frequency response withdrawal measured by Point C'

Table 2.3: Determination of Maximum Allowable Delta Frequencies

	EI	WI	TI	QI	Units
Starting Frequency	59.971	59.970	59.970	59.965	Hz
Minimum Frequency Limit	59.500	59.500	59.300	58.500	Hz
Base Delta Frequency	0.471	0.470	0.670	1.465	Hz
BC'$_{ADJ}$[20]	0.015	N/A	N/A	-0.007	-
Calculated Max. Allowable Delta Frequency	0.367	0.204	0.322	0.952	Hz
Max. Delta Frequency Per Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard	0.420	0.280	0.405	0.947	Hz

---

[19] Due to the use of 1–6 second scan-rate data in BA's EMS systems to calculate the BA's Frequency Response Measures for frequency events under BAL-003-1

[20] Adjustment for the event nadir being below the Value B (EI only) due to primary frequency response withdrawal.

Calculated IFROs

Table 2.4 shows the determination of IFROs for OY 2024 (December 2023 through November 2024) under standard BAL-003-2 based on a resource loss equivalent to the recommended criteria in each Interconnection. The maximum allowable delta frequency values have already been modified to include the adjustments for the differences between Value B and Point C (CB_R), the differences in measurement of Point C using one-second and subsecond data (CC_{ADJ}), and the event nadir being below the Value B (BC'_{ADJ}).

Table 2.4: Initial Calculation of OY 2024 IFROs

	Eastern	Western	Texas	Québec	Units
Starting Frequency	59.971	59.970	59.970	59.965	Hz
Max. Delta Frequency Per Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard	0.420	0.280	0.405	0.947	Hz
Resource Loss Protection Criteria	3,875	2,918	2,805	2,000	MW
Credit for Load Resources	N/A	N/A	1204	N/A	MW
Calculated IFRO using 2017 MDF	-923	-1042	-395	-211	MW/0.1 Hz
Recommended IFRO					
IFRO per Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard	-923[21]	-1042	-395	-211	MW/0.10 Hz

---

[21] BAL-003-2 requires that the EI IFRO will be stepped down to its calculated value over three years. The maximum reduction is limited to 100 MW/0.10 Hz annually.

Comparison to Previous IFRO Values

The IFROs were first calculated and presented in the *2012 Frequency Response Initiative Report*. **Table 2.5** compares the current IFROs and their key component values to those presented in the *2016 FRAA* report.

Table 2.5: Interconnection IFRO Comparison

	OY 2016 Calc[22]	OY 2023 In Use.[23]	OY 2024 Calc.[24]	2023 Calc. to 2024 Calc. Change	OY 2023 In Use to 2024 Calc. Change	Units
Eastern Interconnection						
Starting Frequency	59.974	59.971	59.971	0.000	-0.003	Hz
Max. Allowable Delta Frequency	0.443	0.420	0.420	0.000	-0.023	Hz
Resource Contingency Protection Criteria	4500	3740	3,875	135	-625	MW
Credit for Load Resources	0	0	0	0.000	0.000	MW
Absolute Value of IFRO	**1015**	**890**	**923**	33	-92	MW/0.1 Hz
Western Interconnection						
Starting Frequency	59.967	59.969	59.970	0.001	0.003	Hz
Max. Allowable Delta Frequency	0.292	0.280	0.280	0	-0.012	Hz
Resource Loss Protection Criteria	2626	3068.5	2918	-151	292	MW
Credit for Load Resources	0	0	0.000	0	0	MW
Absolute Value of IFRO	**858**	**1096**	**1042**	-54	184	MW/0.1 Hz
Texas Interconnection						
Starting Frequency	59.971	59.971	59.970	-0.001	-0.001	Hz
Max. Allowable Delta Frequency	0.405	0.405	0.405	0.000	0.000	Hz
Resource Loss Protection Criteria	2805	2805	2805	0.000	0.000	MW
Credit for Load Resources	1136	931	1204	273	68	MW
Absolute Value of IFRO	**412**	**463**	**395**	-68	-17	MW/0.1 Hz
Québec Interconnection						
Starting Frequency	59.969	59.965	59.965	0.000	-0.004	Hz
Max. Allowable Delta Frequency	0.948	0.947	0.947	0.000	-0.001	Hz
Resource Loss Protection Criteria	1700	2000	2000	0.000	300	MW
Credit for Load Resources	0	0	0.000	0.000	0.000	MW

---

[22] Calculated in the 2015 FRAA report. Average frequency values were for OYs 2012–2014.

[23] Calculated in the 2022 FRAA report. Average frequency values were for OYs 2017–2021.

[24] Calculated in the 2023 FRAA report. Average frequency values were for OYs 2018–2022.

Table 2.5: Interconnection IFRO Comparison

	OY 2016 Calc[22]	OY 2023 In Use.[23]	OY 2024 Calc.[24]	2023 Calc. to 2024 Calc. Change	OY 2023 In Use to 2024 Calc. Change	Units
Absolute Value of IFRO	**179**	**211**	**211**	0	32	MW/0.1 Hz

Key Findings

Table 2.6 shows a comparison of mean Value A, mean Value B, and mean Point C that is illustrative of Interconnection performance over the previous OY and as compared to the 2016 OY in which the IFRO values were frozen. Loss of load events have been excluded from the data in Table 2.6. The EI and WI maintained the trend of an increase in mean Value B and a decrease in the mean (A–B), indicating improved performance during the Stabilizing Period of frequency events. The TI maintained the trend of an increase in mean Value B and a decrease in mean (A-B), indicating improved performance during the Arresting Period of frequency events. QI had a decrease in mean Value B and decrease in mean (A–B). The EI and WI show an increase or no change in mean Point C as well as an increase or no change in mean (A–C), indicating improved performance during the Arresting Period of frequency events. This performance data demonstrates that the increases in year-over-year CB_R that result in higher calculated IFROs are due to improved Stabilizing Period performance and not due to a decline in the performance of the Point C nadir. TI showed an increase or no change in the mean Point C as well as a decrease or no change in mean (A-C), indicating improved performance during the Arresting Period of frequency events. QI showed decreasing mean Point C and increasing mean (A-C).

Table 2.6: Year over Year Comparison Value A, Value B, and Point C (Loss of Load Events Excluded)

	OY2016	OY2023	OY2024	Difference OY 2023–2016	Difference OY 2024–2023
Eastern Interconnection					
Mean Value A (Hz)	59.998	60.000	60.000	0.002	0.000
Mean Value B (Hz)	59.947	59.955	59.956	0.008	0.001
Mean Point C (Hz)	59.947	59.949	59.948	0.002	0.000
Mean A – B (Hz)	0.051	0.045	0.045	-0.006	-0.001
Mean A – C (Hz)	0.051	0.052	0.052	0.001	0.000
Western Interconnection					
Mean Value A (Hz)	60	59.995	59.996	-0.0053	0.002
Mean Value B (Hz)	59.923	59.941	59.949	0.0180	0.008
Mean Point C (Hz)	59.887	59.888	59.898	0.0006	0.011
Mean A – B (Hz)	0.076	0.053	0.047	-0.0228	-0.006
Mean A – C (Hz)	0.112	0.107	0.098	-0.0054	-0.009
Texas Interconnection					
Mean Value A (Hz)	59.996	59.998	59.999	0.0023	0.000
Mean Value B (Hz)	59.889	59.921	59.924	0.0321	0.003
Mean Point C (Hz)	59.84	59.859	59.858	0.0191	-0.002
Mean A – B (Hz)	0.107	0.077	0.074	-0.0298	-0.003
Mean A – C (Hz)	0.156	0.139	0.141	-0.0167	0.002

Table 2.6: Year over Year Comparison Value A, Value B, and Point C (Loss of Load Events Excluded)

	OY2016	OY2023	OY2024	Difference OY 2023–2016	Difference OY 2024–2023
Québec Interconnection					
Mean Value A (Hz)	60.003	60.005	60.005	0.0017	0.000
Mean Value B (Hz)	59.843	59.874	59.876	0.0315	0.001
Mean Point C (Hz)	59.433	59.519	59.515	0.0856	-0.004
Mean A – B (Hz)	0.16	0.130	0.129	-0.0298	-0.001
Mean A – C (Hz)	0.57	0.486	0.490	-0.0840	0.004

Recommended IFROs for OY 2024

Consistent with the requirements of BAL-003-2, the IFRO values shown in Table 2.7 for OY 2024 (December 2023 through November 2024) are recommended as follows:

Table 2.7: Recommended IFROs for OY 2024

	EI	WI	TI	QI	Units
MDF[25]	0.42	0.28	0.405	0.947	Hz
RLPC[26]	3875	2918	2805	2000	MW
CLR	0	0	1204	0	MW
Calculated IFRO	-923	-1042	-395	-211	MW/0.1 Hz
Recommended IFRO[27]	**-923**	**-1042**	**-395**	**-211**	MW/0.1 Hz

---

[25] The Procedure for ERO Support of Frequency Response and Frequency Bias Setting Standard, Version II, provided in the approved ballot for BAL-003-2, specifies that, "MDF is the Maximum Delta Frequency for the specific interconnection as determined in the 2017 Frequency Response Annual Analysis (FRAA).

[26] BAL-003-2, Attachment A specifies that Resource Loss Protection Criteria (RLPC) be based on the two largest potential resource losses in an interconnection. This value is required to be evaluated annually.

[27] BAL-003-2 requires that the EI IFRO will be stepped down to its calculated value over three years. The maximum reduction is limited to 100 MW/0.10 Hz annually.

Chapter 3: Dynamics Analysis of Recommended IFROs

Because the IFROs for the EI, WI, and TI have only upon issue of this report been changed as governed by BAL-003-2, additional dynamic validation analyses were not done for this report.

Refer to the dynamics validation in the *2017 FRAA*[28] report for details. No analysis was performed for the QI.

Further supporting dynamic studies accompanied the development and filing of BAL-003-2.

---

[28] https://www.nerc.com/comm/OC/Documents/2017_FRAA_Final_20171113.pdf

2023 Frequency Response Annual Analysis (FRAA)

Action

Accept

Summary

The FRAA report is published annually and includes the annual analysis of frequency response performance for the administration and support of *NERC Reliability Standard BAL-003-2 – Frequency Response and Frequency Bias Setting,*[1], effective December 1, 2020. It provides an update to the statistical analyses and calculations contained in the 2012 Frequency Response Initiative Report that was approved by the NERC Resources Subcommittee and the technical committee, which predated the Reliability and Security Technical Committee (RSTC) and was accepted by the NERC Board of Trustees.

This report is prepared by NERC staff[2] and contains the annual analysis, calculation, and recommendations for the interconnection frequency response obligation (IFRO) for each of the four electrical Interconnections of North America for the operating year (OY) 2024 (December 2023 through November 2024).

We are seeking acceptance from the RSTC at this time.

---

[1] http://www.nerc.com/pa/Stand/Reliability%20Standards/BAL-003-2.pdf

[2] Prepared by the NERC Standards and Engineering organization.

Primary Frequency Control Reliability Guideline

Action:
Approve

Purpose:

The Guideline "Frequency Response Guideline" has had its triennial review by the NERC Resources Subcommittee. This reliability guideline provides recommendations to the industry for frequency control, covering governor deadband and governor droop settings that can enable generating resources (synchronous, inverter-based, and other technologies) to provide needed primary frequency response (PFR) to the Interconnection.

While the incorporation of guideline practices is strictly voluntary there are a couple of exceptions. NERC Regional Reliability Standard BAL-001-TRE-1 Primary Frequency Response in the ERCOT area establishes required governor settings for generating resources operating in the Texas Interconnection. Similarly, WECC has a regional criterion (PRC-001-WECC-CRT-2) that establishes a range of acceptable governor droop settings for generators operating in their footprint.

Background:

NERC recommends that all generating resources be equipped with a functioning governor. FERC Order 842[1] requires any new synchronous and nonsynchronous generators to install, maintain, and operate equipment capable of providing PFR as a condition of interconnection. Primary frequency control is the first active response of resources to arrest the locally measured or sensed changes in speed/frequency. Governors are continuously active, automatic, not driven by a centralized system, and respond instantaneously to frequency deviations exceeding its governor deadband limits. Governor action is delivered proportionally on the droop curve for excursions of frequency beyond the governor deadband limits.

The Reference Document:

The NERC Resources SubCommittee reviewed the Primary Frequency Control to insure continued relevance. Changes to the guideline include:

- Updated document to include references to Inverter-Based Resource Task Force
- Addition of metrics to support evaluation during triennial review, consistent with the RSTC Charter.
- Formatted to new NERC format
- Additionally, many links were updated as outlined by commentors
- Finally, several errata changes were made to correct grammar and typographical errors.

This guideline has been posted for 45-day industry comment and includes the response to those comments.

---

[1] https://www.ferc.gov/whats-new/comm-meet/2018/021518/E-2.pdf

Reliability Guideline	Primary Frequency Response				
Organization(s)	**Page #**	**Line / Paragraph**	**Comment**	**Proposed Change**	**NERC Response**
American Electric Power	Entire Document	N/A	Please note, all page numbers noted in our comments are those shown in the page footers of the redlined draft.	N/A	
American Electric Power	Page 18 and 23	N/A	Pages 18 and 23 both have broken links to Appendix B and display the message "Error! Reference source not found."	Correct links as appropriate.	Thank you for your comment. The link has been fixed.
Edison Electric Institute	N/A	N/A	General Comment: EEI supports the revised version of the Reliability Guideline titled Primary Frequency Control dated January 24, 2023 but offer some non-substantive comments for NERC consideration. Many of the following comments involve broken links to documents. NERC might want to consider referencing documents by name, number, author and avoid the hyperlinks.	Suggest correcting various broken links in this Guideline.	Thank you for you comment. The links has been addresed.
Edison Electric Institute	10	188	Footnote 2 link appears to be broken, however, EEI suggests deleting the footnote. Access to FERC Orders do not need to be footnoted because they are easily and readily available on the FERC website and the files tend to move over time. If NERC believes that a footnote is needed, they should consider identifying the FERC Order number, name and date and avoid using the links (see our general comment above).	EEI suggests deleting the footnote for the reasons provided.	Thank you for you comment. The link has been addresed.
Edison Electric Institute	10	209	EEI suggests removing the reference to the NERC OC in this sentence because the OC is no longer a NERC operating group. We additionally suggest footnote 3 be deleted because it is no longer working. NERC Reliability Guideline are found on the NERC webpage. To resolve these issues, we suggest changing this sentence as follows: The NERC OC-approved Reliability Guideline titled Operating Reserve Management guideline provides additional details on the recommended methods to determine FRR needs.	Suggest deleting Footnote 3 and adjusting the identified sentence (see bold and strick through changes).	Thank you for your comment. We have updated to the RSTC and updated the link.
Edison Electric Institute	15	308 - 309	Figure 2.5 and Footnote 5: should include a reference to the Lawrence Berkley National Laboratory Report titled Primary Frequency Response and Control of Power System Frequency, because the graph was directly taken from that document, albeit titles modified for the bottom diagram. See Figure 19 (page 30) from the above referenced report.	EEI suggests that the Footnote 5 provide a clearer reference to the LBNL report.	Thank you for comment. There is a reference labeled "Source."
Edison Electric Institute	15	320	Footnotes 6 should provide a clearer reference from the technical document that is referenced with attribution given to both NREL and the identified authors. (See https://www.nrel.gov/docs/fy17osti/67799.pdf). EEI suggests similar adjustments to Footnote 7. Alternatively, NERC could use endnotes to more clearly link the document references in Appendix D to the referenced section of this Guideline.	EEI suggests making clearer attribution for Footnotes 6 & & as indicated in our comments. Hyperlinks often change over time and may not be the best method of footnoting supporting materials.	Thank you for comment. We updated footnote 6 wuth the following link. https://www.nrel.gov/docs/fy17osti/67799.pdf
Edison Electric Institute	15	326	Footnote 8 – Suggest deleting the footnote to the Reliability Guideline titled Power Plant Model	Suggest removing the hyperlink for the reasons provided in our comments.	Thank you for comment. We updated the footnote link.
Edison Electric Institute	17	360	Footnote 9: The hyperlink to the GE Energy Consulting report does not work. Suggest identifying the	The hyperlink to the GE Energy Consulting report no longer works. Suggest the link provided in our	Thank you for comment

Edison Electric Institute	18	375	Line 375; Footnote 11 does not appear to be working. Suggest removing the hyperlinks and identifying the document. Alternatively, we offer the following: https://www.nerc.com/pa/Stand/Project%20200712%20Frequency%20Response%20DL/FRI_Report_10-30-12_Master_w-appendices.pdf	Footnote 11 does not appear to be working. Suggest the link provided in our comment or simply referencing the report title, author, etc.	Thank you for comment we have updated the link.
Edison Electric Institute	34	630 - 664	Appendix D: Related Document –Suggests identifying all of the identified document by document, name, date, author, etc. and removing the hyperlinks (See our general comment above). Alternative we note the following: • FERC Order 842 – Broken Link • Reliability Guideline: Operating Reserve Management – Version 23 – Broken Link & Wrong Version • Primary Frequency Response and Control of Power System Frequency – Broken Link • NERC Inverter-Based Resource Performance Task Force Inverter Based Resource Guideline – Broken Link • Technology Capabilities for Fast Frequency Response – Broken Link • WECC Criterion: PRC-001-WECC-CRT-1.2 – Correct title of Document	Suggest avoiding hyperlinks in Appendix D. More traditional document references to Title, Document Number, Author, etc. are generally more reliable over time than hyperlinks.	Thank you for your comment.
Manitoba Hydro	iv	65	Should WECC be defined in the second column of the table?	Write "WECC" as "Western Electricity Coordinating Council"	Thank you for comment. We will share your comment to NERC staff.
Manitoba Hydro	7	101	"grid event" is referenced, but what consitutes a "grid event"?	Consider adding a footnote to define "grid event"	Thank you for your comment. The term is meant to be generic in nature and was not intended to be defined.
Manitoba Hydro	7	108, 101	"major grid events" is referenced here, but the purpose section (line 101) only indicates "grid event"	For conformity, update to "major grid event" in the purpose statement	Thank you for your comment. The term is meant to be generic in nature and was not intended to be defined.
Manitoba Hydro	9	157	"NERC BAL-003-1.1" should be referenced as "NERC Reliability Standard BAL-003-1.1" for conformity with the rest of the document	Consider replacing "NERC BAL-003-1.1" with "NERC Reliability Standard BAL-003-1.1"	Thank you for your comment. We modified the references to "NERC Reliability Standard".
Manitoba Hydro	11	242	Can a footnote be added to define "squelched responses." for clarity	Add a footnote to define "squelched responses"	Thank you for your comment. We believe the paragraph defines "Squelched Responses"
Manitoba Hydro	22	442	"NERC Regional Standard" should be referenced as "NERC Regional Reliability Standard" for conformity with the rest of the document	Consider replacing "NERC Regional Standard" with "NERC Regional Reliability Standard"	Thank you for your comment. We modified the references to "NERC Regional Reliability Standard".
Manitoba Hydro	30	507 - 518	Punctuation - missing periods at th end of each sentence	Add periods following each sentence	Thank you for your comment. We agree add period.
Manitoba Hydro	33	626	"frequency control" should be capitalized in the definition	Write "Tertiary frequency control" as "Tertiary Frequency C	_
Manitoba Hydro	37	687-689, 694, 695	Punctuation - missing periods at th end of each sentence	Add periods following each sentence	Thank you for your comment. We agreed to add periods.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Guideline

Primary Frequency Control

January 24, 2023

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Formatted: Font: Calibri

Formatted: Font: Calibri

Formatted: Font: Calibri

Formatted: Font: Calibri

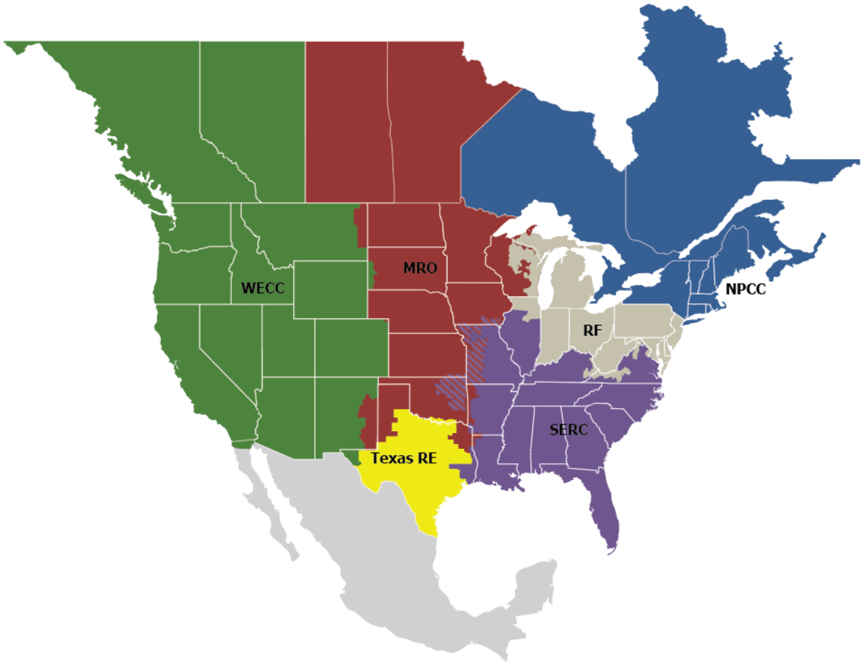
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the NERC and the six Regional Entities, is a highly reliable, resilient, and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six Regional Entity boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners /Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Preamble

The NERC Reliability and Security Technical Committee (RSTC), through its subcommittees and working groups, develops and triennially reviews reliability guidelines in accordance with the procedures set forth in the RSTC Charter. Reliability guidelines include the collective experience, expertise, and judgment of the industry on matters that impact BPS operations, planning, and security. Reliability guidelines provide key practices, guidance, and information on specific issues critical to promote and maintain a highly reliable and secure BPS.

Each entity registered in the NERC compliance registry is responsible and accountable for maintaining reliability and compliance with applicable mandatory Reliability Standards. Reliability guidelines are not binding norms or parameters nor are they Reliability Standards; however, NERC encourages entities to review, validate, adjust, and/or develop a program with the practices set forth in this guideline. Entities should review this guideline in detail and in conjunction with evaluations of their internal processes and procedures; these reviews could highlight that appropriate changes are needed, and these changes should be done with consideration of system design, configuration, and business practices.

Executive Summary

This reliability guideline provides recommendations to the industry for frequency control, covering governor deadband and governor droop settings that can enable generating resources (synchronous, inverter-based, and other technologies) to provide needed primary frequency response (PFR) to the Interconnection.

NERC Regional Reliability Standard BAL-001-TRE-1 Primary Frequency Response in the ERCOT area establishes required governor settings for generating resources operating in the Texas Interconnection. Similarly, WECC has a regional criterion (PRC-001-WECC-CRT-2) that establishes a range of acceptable governor droop settings for generators operating in their footprint.

This Guideline does not create binding norms, does not establish mandatory Reliability Standards and does not create parameters by which compliance with Reliability Standards are monitored or enforced. In addition, this Reliability Guideline is not intended to take precedence over any Regional procedure.

Introduction

Purpose

This Reliability Guideline outlines a coordinated operations strategy for resources to stabilize system frequency when frequency deviates due to a grid event. It is designed to keep frequency within allowable limits while maintaining acceptable frequency control.

Applicability

This reliability guideline is intended to assist Balancing Authorities (BAs), Generator Operators (GOPs), Generator Owners (GOs), Transmission Operators (TOPs), and Transmission Owners (TOs) in understanding the fundamentals of frequency control, the recommended governor deadband and governor droop settings (so as to provide more effective frequency response during major grid events), and the techniques of measuring frequency response at a resource level. It is offered as information to other functional model entities. It outlines a coordinated operations strategy to restore system frequency after frequency has deviated due to a BES disturbance.

The primary focus of this guideline is the PFR provided by generating resources during loss of generation scenarios. Other forms of resources providing frequency response should have similar response characteristics described herein for governors.

Chapter 1: Frequency Control – Fundamentals

The instantaneous balance between generation and load is directly reflected in an interconnected electric power system's frequency. Reliable power system operation depends on controlling frequency within predetermined boundaries above and below a nominal value. In North America, this value is 60 cycles per second (or 60 Hertz (Hz)). These concepts unambiguously apply to other Interconnections with different nominal frequencies.

BAs are responsible to dispatch generation and manage their area control error (ACE) in a manner that maintains frequency at the scheduled value using automatic generation control (AGC) on a continuous basis. NERC BAL standards establish the frequency control performance requirements for BAs.

Resilient interconnection frequency response to a sudden loss of generation or load depends upon the coordinated interplay of inertia, load damping, and defined control actions.

Figure 1.1~~Figure 1.1~~ shows a simplified illustration of frequency and power trends that would be seen in a properly functioning power system in response to a sudden loss of generation. The event has been segmented into three periods to aid in the discussion of frequency control actions. Frequency is managed by the combined actions of primary, secondary, and tertiary controls.

Formatted: Font: Not Bold, Font color: Auto

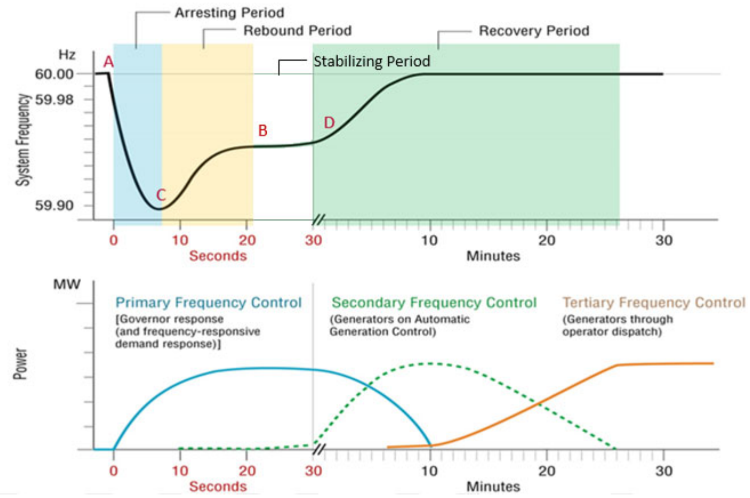


Figure 1.1: The Sequential Actions and Impacts on System Frequency of Primary, Secondary, and Tertiary Frequency Control

Source: Eto, et al. LBNL: Use of a Frequency Response Metric to Assess the Planning and Operating Requirements for Reliable Integration of Variable Renewable Generation

Arresting Period

As shown in the top trace (Figure 1.1), the "A Point" is defined as the predisturbance frequency. The time period beginning with a generation loss at T_0 and ending at the lowest frequency deviation, frequency nadir or C-Point, is

Formatted: Font: Not Bold

labeled the “Arresting Period.” Primary control action, indicated by the solid blue line in the bottom part of the figure, starts to engage immediately once frequency falls outside the deadband. In this period, the decay of frequency must be arrested to avoid triggering under frequency load shedding (UFLS). The decline of frequency is arrested only when the combined response from load changes, load damping, demand response, and PFR responsive equals the size of generator loss. Inertia plays a critical role in determining the timing with which frequency response must be delivered to arrest the decline of frequency. The behavior of frequency after the arrest depends on the effect of primary and secondary control action and load changes.

Recovery Period

The recovery period can be divided into three sub-periods referred to as rebound, stabilizing, and recovery. In the example event referenced earlier in Figure **1.1**~~Figure **1.1**~~, the rebound period is defined by the sharp recovery of frequency between the C Point and T+20 seconds. Early withdrawal of primary response, as indicated by the dashed blue line, dampens the rebound and slows the recovery of frequency. The stabilizing period is defined as the window between T+20 to T+60 seconds when frequency has leveled out after the rebound period. During the stabilizing period, the collective PFR establishes a new balance between load and generation at a frequency called the settling frequency. In NERC BAL-003-1.1, the frequency defined by the period extending from T_{+20} to T_{+52} seconds is averaged and identified as the “B-Point” or the value at which frequency has been stabilized by PFR.

Formatted: Font: Bold, Font color: Accent 1

As mentioned above, frequency is stabilized at a value lower than the original scheduled frequency. This is an expected and necessary consequence of PFR delivered via droop control with a defined deadband. Governor droop changes resource output in proportion to the deviation of frequency once frequency has exceeded the deadband limit. PFR alone does not restore frequency to the original scheduled value primarily because governor-directed changes only occur when frequency is beyond the governor deadband.

Application of secondary control action begins when deviations of frequency and power flows are detected and continues until scheduled values have been restored. The action of automatic generation controls may be augmented or modified by manual control actions directed by system operators—such as deploying contingency reserves, demand response, or establishing emergency interchange schedules. Secondary frequency control action takes place more slowly than primary frequency control actions. For example, in the case of AGC, secondary frequency control is initiated by external automated commands sent every two to six seconds. Resources typically employ a rate-of-change limit on the AGC input to the unit control system. This results in a ramp response of a resource to secondary control action.

Secondary response may require 5 to 15 minutes (and sometimes more) to complete the restoration of frequency to the scheduled value. It is therefore critical to recognize that the sustained delivery of PFR is essential for stabilizing frequency throughout the recovery period to ensure system reliability.

Post Recovery Period

In the third stage, frequency has been restored to its scheduled value, and the reserves held to provide primary and secondary frequency control are restored by tertiary control. The goal of tertiary control actions is to restore the reserves that were used to deliver PFR and secondary frequency response during the recovery period. Reserves may be restored using redispatch, commitment of resources, or establishing new interchange schedules. Restoring these reserves completes the repositioning of the power system so that it is prepared to respond to a future loss-of-generation event.

Chapter 2: Primary Frequency Control

NERC recommends that all generating resources be equipped with a functioning governor. FERC Order 842[1] requires any new synchronous and nonsynchronous generators to install, maintain, and operate equipment capable of providing PFR as a condition of interconnection. Primary frequency control is the first active response of resources to arrest the locally measured or sensed changes in speed/frequency. Governors are continuously active, automatic, not driven by a centralized system, and respond instantaneously to frequency deviations exceeding its governor deadband limits. Governor action is delivered proportionally on the droop curve for excursions of frequency beyond the governor deadband limits. Examples of PFR to high and low frequency events by generation type can be found in **Appendix A:~~Appendix A:Appendix A~~**.

Allocation and Distribution of Frequency Responsive Reserve for Sustained Primary Frequency Response

The sudden loss of a generating resource will cause frequency to decline. Loss of generation events are fairly common. For this reason, each Interconnection should be designed and operated to withstand the sudden loss of a certain amount of generation without jeopardizing reliability. BAs are required to meet a frequency response obligation for their areas. Providing frequency response in such events is accomplished by maintaining frequency responsive reserve (FRR) capacity that is adequate to arrest and stabilize the decline in frequency and to reserve additional headroom that is adequate to restore frequency to its scheduled value. In a scenario where the reserved capacity of generation providing frequency response and secondary response is lower than the loss of generation, frequency would continue to decline and could potentially lead to the loss of load through the triggering of UFLS. The aggregate performance of the units supplying the reserve capacities can vary based on the number of generators and the generation mix of the fleet. Overall, the expectation is that the reserved capacity exceeds its largest expected generation loss with margin in order to account for uncertainty in the actual performance of the fleet. The NERC RSTC~~OC~~ approved O~~o~~perating R~~r~~eserve M~~m~~anagement G~~g~~uideline[2] provides additional details on the recommended methods to determine FRR needs.

The frequency response expected of generators should not exceed the amount they can produce before the declining frequency triggers UFLS. It is highly recommended that FRR be distributed among many generators rather than a select few in order to limit the response each unit individually needs to contribute; additionally, distributed FRR facilitates the mitigation of and recovery from wide scale events. Drawing frequency response from a large pool of geographically diverse resources makes frequency response faster, more reliable, and more effective than drawing from select isolated resources. That, in turn, helps arrest frequency earlier resulting in a higher frequency nadir and reduces the risk that some units may not provide the expected response.

The responses to generation loss from two sets of reserves are compared in Figure 2.1~~Figure 2.1~~. One (blue trace) is composed of resources that sustain PFR throughout the event in aggregate, and the other (red trace) is composed of resources that respond initially but do not sustain PFR throughout the event in aggregate. PFR is withdrawn from the set of reserves represented by the red trace before secondary frequency response is applied. In the initial phase of the event, the frequency trends for the two simulations are nearly identical because the same amount of PFR has been delivered. However, even as the nadir is reached, the effect of a lower amount of sustaining PFR of the reserves represented by the red trace can be observed; this leads to a lower apparent settling frequency. As the event progresses, the nonsustaining portion of the reserves represented by the red trace continues to reduce the PFR delivered. During the stabilizing period, frequency begins to decline again as there continues to be an imbalance of load and resource due to nonsustained PFR. This increases the risk of load being shed due to UFLS action.

Formatted: Font: Not Bold, Font color: Auto

---

[1] https://www.ferc.gov/whats-new/comm-meet/2018/021518/E-2.pdf

[2] https://www.nerc.com/comm/OC_Reliability_Guidelines_DL/Operating_Reserve_Management_Guideline_V2_20171213.pdf

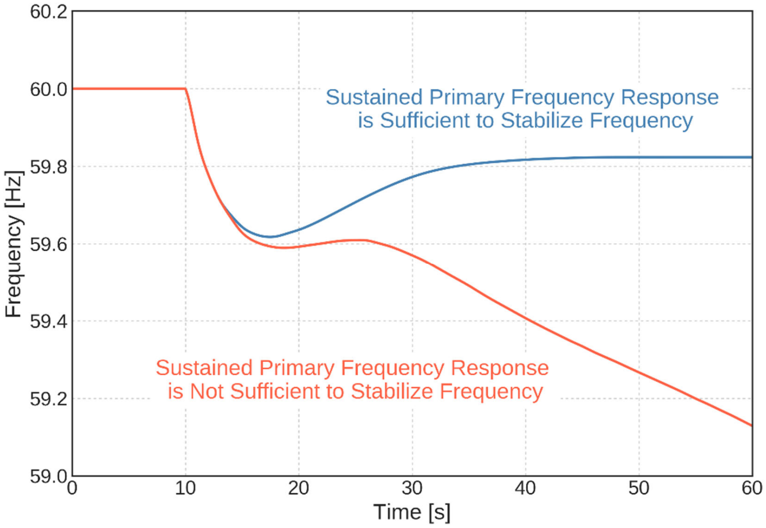


Figure 2.1: Sustaining vs Nonsustaining Primary Frequency Response Effect on System Frequency

Source: Developed by LBNL from Undrill (2018): Primary Frequency Response and Control of Power System Frequency

There are several reasons why PFR may not be sustained: The first is through withdrawal of PFR by the actions of plant-level or unit-level control of net resource output overriding and resetting the actions of the governor response to frequency deviations; the second is through actions stemming from inherent physical characteristics and limit actions of a generating resource. One example is the exhaust gas temperature limiter on certain types of combustion turbine/generators. These protective systems are intrinsic to the design of combustion turbine/generators and unlike plant-level controllers; these actions cannot be overridden or corrected. All generating resource types exhibit similar responses by equipment protection systems. These types of responses are also known as “squelched responses.”

These factors also reinforce the need to distribute reserves to numerous generators of different generation types in order to provide reliable sustained PFR. Each generating resource’s capability for providing a sustained response must be considered when accounting for expected PFR until it is replaced by response to secondary frequency control action.

Coordination between a Resource’s Governors and Output Controls

Modern generating resource control systems generally incorporate a form of plant or unit load control. These load control systems can be applied within the turbine control system, the plant or unit control system, or remotely from a central dispatch center. Regardless of their location or method of implementation, the design of secondary controls must be coordinated with that of the governor to ensure that PFR can be sustained.

Closed loop load control can exist at a minimum in one or possibly both load control loops based on operator selection. Proper coordination of control actions can be accomplished in several ways, including the following:

- Use of a frequency bias in the plant level load controller would allow it to adjust individual load targets in harmony with the governor response.

1. Use of a frequency bias in the turbine level load controls in conjunction with open loop load control at the plant level would allow the turbine control panel to adjust its internal load control target in harmony with the governor response.

   In both case one and case two the plant level load controls can adjust targets in response to external input, (e.g., a revised AGC target). Plant and turbine controls must be coordinated with governor settings.

- Operation of the generating resource in pure governor control mode with manual adjustments to the speed governor target, such as analog or mechanical control systems. Some early digital controllers in use on generating resources may not be capable of operation in any form of megawatt (MW) target control.

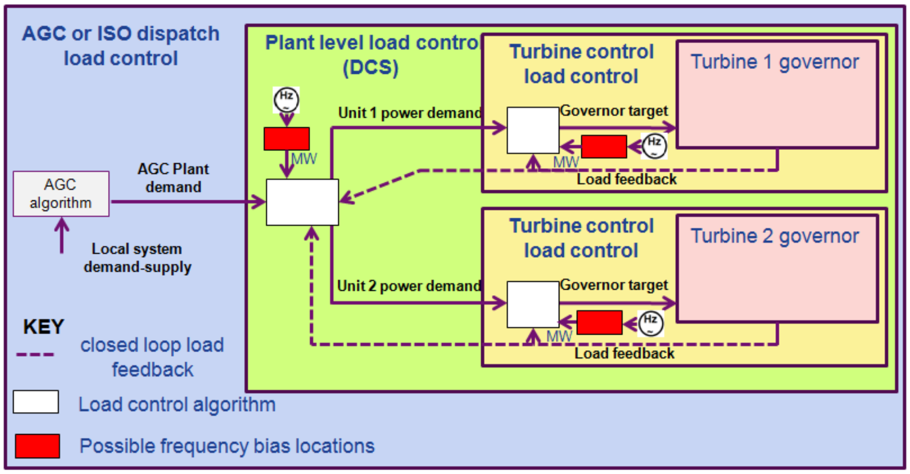
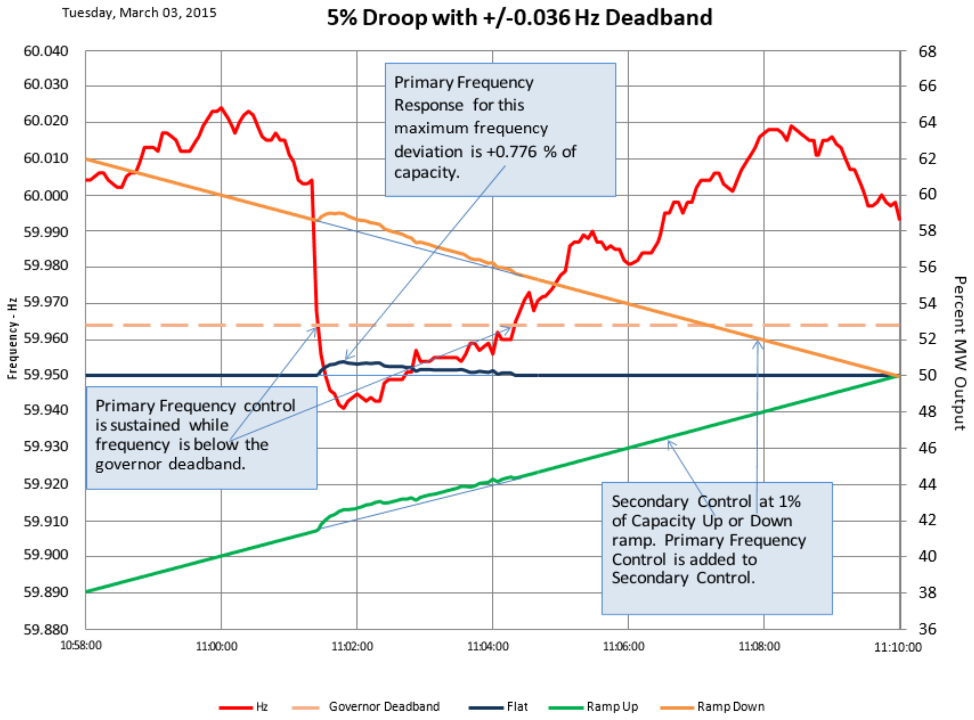


Figure 2.2: Typical High Level Generating Resource Control System

Frequency bias should be applied at all levels of closed loop MW output control for a coordinated generating resource response. See Figure 2.3~~Figure 2.3~~ and Figure 2.4~~Figure 2.4~~ for illustrations of expected frequency response from a generating resource that is properly coordinated to provide sustained PFR following loss of generation or loss of load when at steady output, ramping up, or ramping down.

Formatted: Font: Not Bold, Font color: Auto

Formatted: Font: Not Bold, Font color: Auto



Tuesday, March 03, 2015

5% Droop with +/-0.036 Hz Deadband

Primary Frequency Response for this maximum frequency deviation is +0.776 % of capacity.

Primary Frequency control is sustained while frequency is below the governor deadband.

Secondary Control at 1% of Capacity Up or Down ramp. Primary Frequency Control is added to Secondary Control.

Figure 2.3: Example of Properly Coordinated Primary Frequency Control while Ramping MW Up or Down via Local or Remote Control or While Operating at a Fixed MW Output (Deadband = 36 mHz)

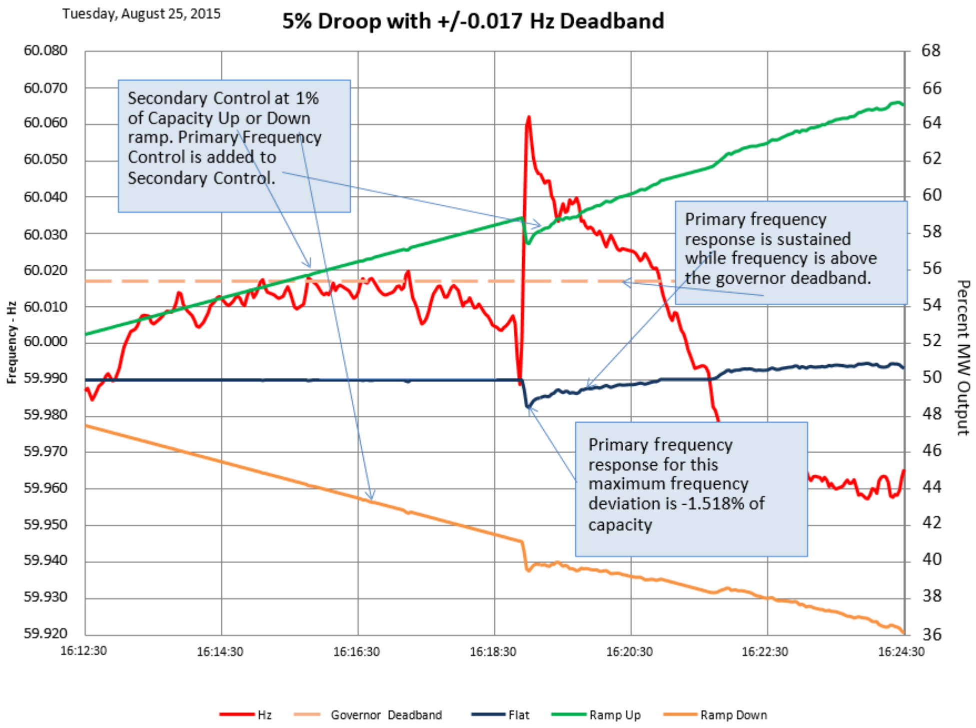


Figure 2.4: Example of Properly Coordinated Primary Frequency Control while Ramping MW Up or Down Via Local or Remote Control or while Operating at a Fixed MW Output in the Graph Above - High Frequency Excursion with a Lower Deadband (Deadband = 17 mHz)

Ability of Natural Gas Turbines to Sustain Primary Frequency Response Following Large Loss-of-Generation Events

Combustion turbine/generators are important contributors to arrest system frequency following a sudden loss of generation. However, if an under-frequency event calls for maximum output from a combustion turbine/generator, this output may not be sustainable due to reduced air flow, the working fluid of these engines, and the actions of the exhaust temperature limit protection system of the turbine. At less than nominal frequency, the combustion turbine/generator rotates more slowly and moves less air into/through the combustion process. Burning the same or greater amount of fuel with less air results in higher exhaust gas temperature. If exhaust gas temperatures exceed a preset limit, the combustion turbine/generator will reduce output automatically to protect the turbine from damage. Unlike the withdrawal of response by plant load-controls, reduction of output by this means cannot be deactivated at the discretion of the plant operator.

Moreover, there is linkage between the exhaust gas temperature protection system and system frequency that can be detrimental to reliable interconnection frequency response. If system frequency continues to be depressed or decline as the exhaust gas temperature controls reduce turbine output, then the temperature limit controls will further reduce turbine output.

Figure 2.5~~Figure 2.5~~ illustrates this effect. The lower panel shows the control actions directed by the turbine-governor (red) and the exhaust gas temperature protection system (blue). Initially, the turbine-governor, responding to the decline in interconnection frequency, directs increased fuel flow to the turbine thus increasing the combustion rate and MW output. Once the turbine exhaust has reached its temperature limit, the protection system overrides the turbine-governor and directs lower levels of fuel flow until the exhaust temperature is below the limit. The top panel illustrates the impact these control actions could have on interconnection frequency when combustion turbine/generators predominate the generation mix in an interconnection and are operated near the exhaust temperature limit.

Formatted: Font: Not Bold, Font color: Auto

Formatted: Font: Not Bold, Font color: Auto

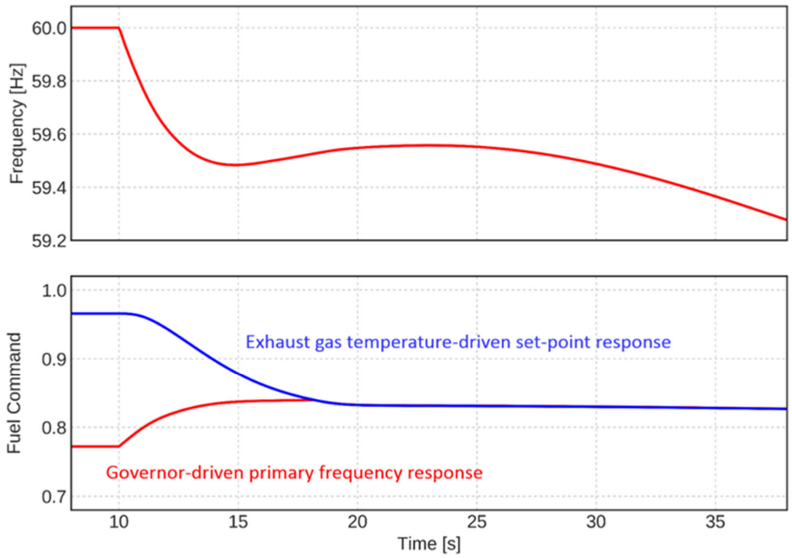


Figure 2.5: Exhaust Gas Temperature Controls on Gas Turbines Will Decrease Primary Frequency Response if Frequency Remains Depressed

Source: Developed by LBNL from Undrill (2018): Primary Frequency Response and Control of Power System Frequency

As noted, the effect of these controls cannot be overridden; they are intrinsic to the design of protection for the turbine. This reduction is better thought of as a reduction in the headroom or PFR capability of the natural gas turbine, rather than a form of withdrawal of PFR.

Primary Frequency Response from Inverter-Based Resources

Inverter-based resources (IBR) are capable of providing primary response in accordance with the common droop rule of the grid. IBRs have demonstrated their ability to respond to frequency deviation events in various Interconnections,[3] including ERCOT,[4] where it is a requirement. Most IBRs operate at maximum available output based on the availability of solar irradiance or wind speed. As a result, IBRs normally do not have headroom to provide PFR to low frequency events, but IBRs can provide very effective PFR to high frequency events. There are instances, however, where the resource may be curtailed; in these cases, IBRs would have the ability to provide PFR to frequency dips. IBRs normally have enough "down headroom" to provide PFR to high frequency events. More detailed guidance

---

[3] Demonstration of Essential Reliability Services by a 300-MW Solar Photovoltaic Power Plant

[4] Advanced Grid-Friendly Controls Demonstration Project for Utility-Scale PV Power Plants

on effective control settings, frequency measurement resolution, and speed of PFR delivery for IBRs is available in the *Power Plant Model Verification for Inverter-Based Resources Reliability Guideline.*[5]

Fast Frequency Controls on Electronically Coupled Wind Generation and Sustained Primary Frequency Response

Most modern wind turbines are Type 3 (doubly fed induction generator) or Type 4 (full-scale converter generator) and are designed to allow operation at variable speed to achieve greater efficiency. However, variable speed operation requires generator speed and system frequency to be decoupled from each other via use of power electronic converters. As a result, even though kinetic energy is stored in the rotating mass of a wind turbine, variable speed wind turbines do not inherently provide inertial response to grid disturbances. Inertia itself is not a substitute for primary frequency control because inertia, whether synthetic or real, is not a sustained source of energy injection; however, it continues to oppose frequency change in real time.

Fast frequency control systems have been developed by several wind turbine manufacturers to allow the kinetic energy stored in the rotating mass of a wind turbine to be extracted and provide temporary active power to the grid in response to a frequency trigger during low frequency events. Such fast response is not considered to be PFR because it cannot be sustained unless the resource is operating under a curtailment.

Figure **2.6**~~Figure **2.6**~~ shows the actual performance of a specific Type 3, 1.5 MW wind turbine equipped with "rotor inertia-based Fast Frequency Response" functionality for varied wind speeds. At 14 m/s (above nominal wind speed) there is no recovery phase. At 11.5 m/s, just below nominal wind speed, the recovery phase is the most demanding. Fast frequency control response decreases drastically at 50 percent of rated power and drops to zero at 20 percent of rated power, this is illustrated by 5 m/s (blue) trace below. This response is not proportional to frequency change and the same response will be provided for the same wind conditions for all frequency events.

Formatted: Font color: Auto

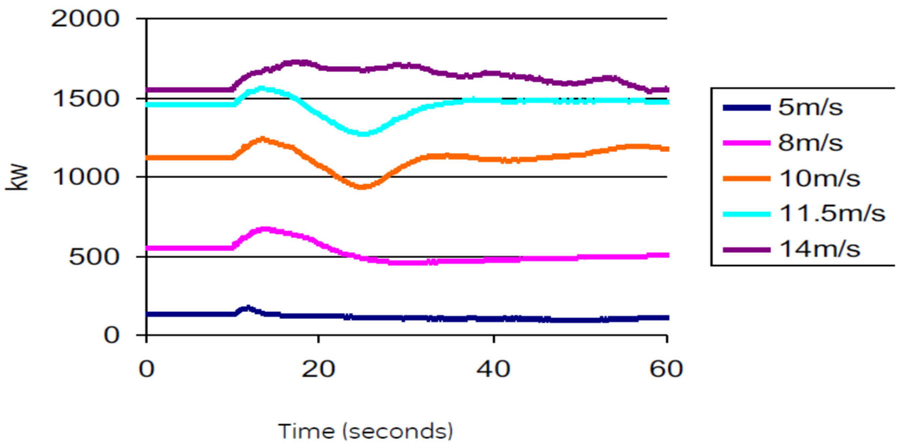


Figure 2.6: Fast Frequency Control Response of Wind Turbine at Different Wind Speed Conditions

It is important to recognize that the value of fast frequency control response is in energy being delivered during the arresting period to "buy" time for conventional PFR to act. Failing to sustain fast frequency response beyond the

---

[5] https://www.nerc.com/comm/RSTC_Reliability_Guidelines/PPMV_for_Inverter-Based_Resources.pdf

frequency nadir may lead to a prolonged recovery period. With that in mind, PFR coupled with fast frequency response from energy storage resources (activated only when headroom is allocated) and faster frequency response from IBRs with stored energy that can be tapped can help in the arresting period and is also sustained. To be beneficial to the power system, fast frequency control settings must be tuned to specific systems needs and various operating conditions. Additional details about fast frequency controls can be found in *Technology Capabilities for Fast Frequency Response,*[6] which was published by GE Energy Consulting in March 2017.

---

[6] https://www.nrel.gov/docs/fy17osti/67799.pdf

Chapter 3: Governor Deadband and Governor Droop Settings

This guideline proposes maximum governor deadband and governor droop settings to achieve desired frequency response for each of the Interconnections while subject to other technical, operational, or regulatory considerations that would prevent governors from achieving the particular governor settings. Although there are recommended governor deadband maximums for two of the Interconnections at 36 mHz, it should be noted that deadbands of 0 and 17 mHz have been successfully implemented for several generating resource types. Governor deadbands are recommended to be implemented without a step into the droop curve. A step in the droop curve exposes the generator to excessive cycling when frequency dithers about the deadband limit. An example of each scenario can be seen in Figure 3.1~~Figure 3.1~~ (recommended) and Figure 3.2~~Figure 3.2~~ (not recommended). A more detailed discussion of the two methods (step and no-step) can be found in Appendix B ~~**Appendix B**~~ of *Dynamic Models for Turbine-Governors in Power System Studies,*[7] which was published by the IEEE PES in January 2013. A larger percent droop value is less responsive to frequency deviations (e.g., a five percent droop is less responsive than a three percent droop).

Formatted: Font: Not Bold, Font color: Auto

Formatted: Font: Not Bold, Font color: Auto

Formatted: Font color: Auto

Formatted: Font: Not Bold, Font color: Auto

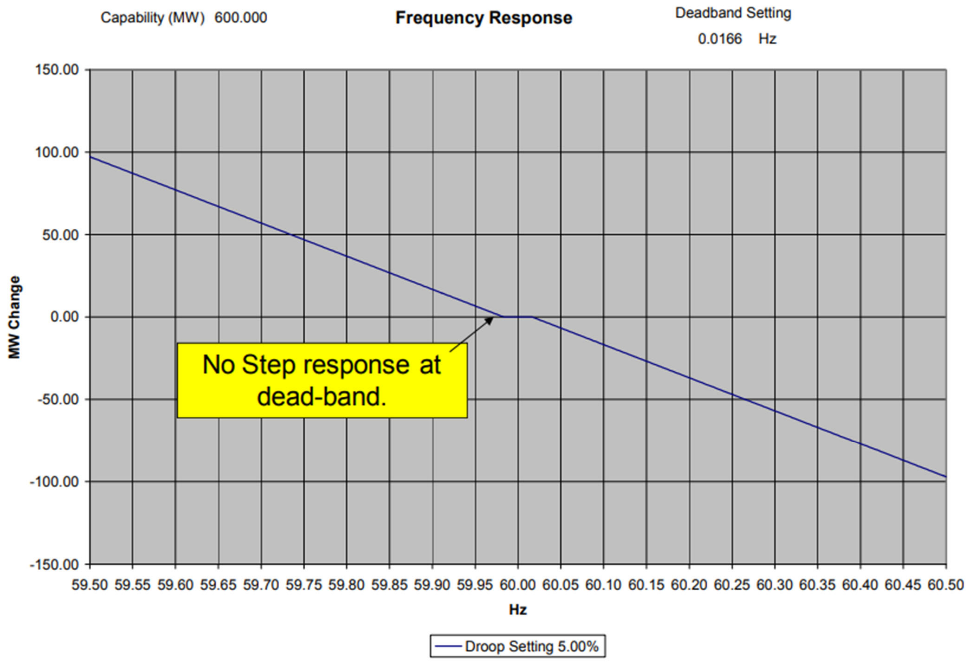


Figure 3.1: Governor Deadband Setting without Step Implementation
Source: NERC Frequency Response Initiative Report 2012[8]

---

[7] http://sites.ieee.org/fw-pes/files/2013/01/PES_TR1.pdf

[8] https://www.nerc.com/docs/pc/FRI_Report_10-30-12_Master_w-appendices.pdf Frequency Response Initiative Report 2012

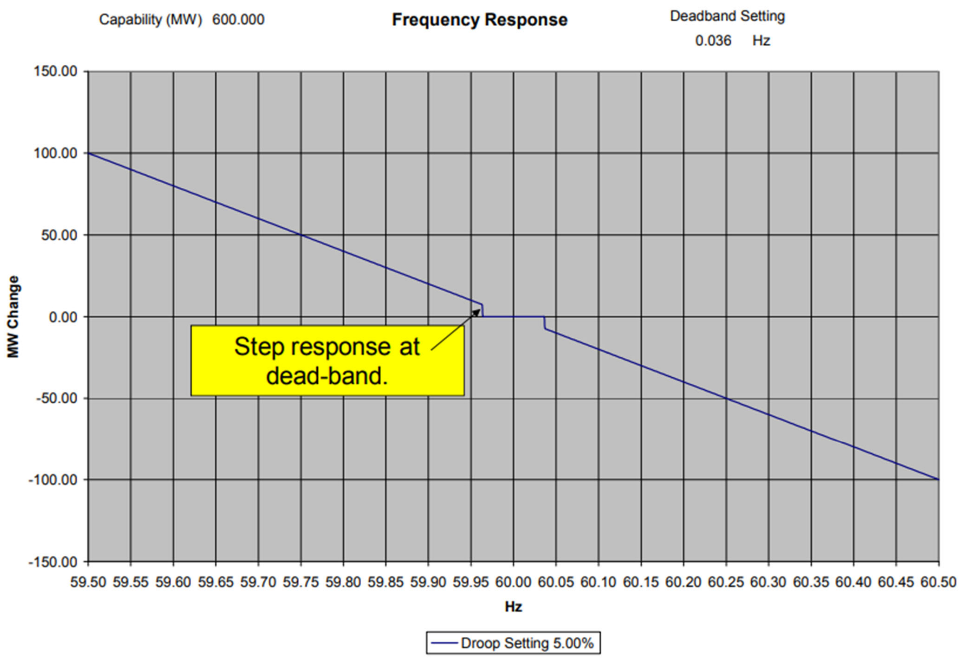


Figure 3.2: Governor Deadband Setting with Step Implementation

Source: NERC Frequency Response Initiative Report 2012

The recommended maximum governor deadband and governor droop settings for each Interconnection are as follows in this section.

Eastern Interconnection

The recommended governor deadband setting should not exceed the value stated in Table 3.1.

Formatted: Font: Not Bold, Font color: Auto

Table 3.1: Eastern Interconnection Deadband Settings	
Generator Type	**Maximum Deadband Setting**
All Generating Units	+/- 0.036 Hz

The maximum expected droop performance for the entire combined-cycle facility is six percent. The effective droop of a combined-cycle plant depends on the size of the steam turbine generator in proportion to the sum of the natural gas turbine generators. Many combustion turbines in a combined-cycle configuration have a four percent droop setting. The recommended governor droop settings should not exceed the values in Table 3.2 for each type of generator.

Formatted: Font: Not Bold, Font color: Auto

Table 3.2: Eastern Interconnection Droop Settings	
Generator Type	**Maximum ~~Deadband~~ Droop Setting**
Combustion Turbine (Combined Cycle)	4%

Table 3.2: Eastern Interconnection Droop Settings

Generator Type	Maximum ~~Deadband~~ Droop Setting
Steam Turbine (Combined Cycle)	5%
All Others	5%

ERCOT Interconnection

The required governor deadband setting shall not exceed the values in Table 3.3 from BAL-001-TRE.

Formatted: Font: Not Bold, Font color: Auto

Table 3.3: ERCOT Interconnection Dead Band Settings

Generator Type	Maximum Dead-Band Setting
Steam and Hydro Turbines with Mechanical Governors	+/- 0.034 Hz
All Other Generating Units/Generating Facilities	+/- 0.017 Hz

The required governor droop settings shall not exceed the values **in Table 3.4** for each respective type of generator from BAL-001-TRE.

Formatted: Font: Bold

Formatted: Font color: Auto

Formatted: Font: Bold

Table 3.4: ERCOT Interconnection Droop Settings

Generator Type	Maximum ~~Deadband~~ Droop Setting
Hydro	5%
Nuclear	5%
Coal and Lignite	5%
Combustion Turbine (Simple Cycle and Single-Shaft Combined Cycle)	5%
Combustion Turbine (Combined Cycle)	4%
Steam Turbine (Simple Cycle)	5%
Diesel	5%
Wind Powered Generator	5%
DC Tie Providing Ancillary Services	5%
Renewable (Non-Hydro)	5%

Western Interconnection

The recommended governor deadband setting should not exceed the value in Table 3.5.

Formatted: Font: Not Bold, Font color: Auto

Table 3.5: Western Interconnection Deadband Settings

Generator Type	Maximum Deadband Setting
All Generating Units	+/- 0.036 Hz

The governor droop settings shall not be less than three percent or greater than five percent. Many combustion turbines have a four percent droop setting. The droop settings should not exceed the values in Table 3.6 for each respective type of generator.

Formatted: Font: Not Bold, Font color: Auto

Table 3.6: Western Interconnection Droop Settings

Generator Type	Maximum ~~Deadband~~ Droop Setting
Combustion Turbine (Combined Cycle)	4%
Steam Turbine (Combined Cycle)	5%

Table 3.6: Western Interconnection Droop Settings	
Generator Type	**Maximum ~~Deadband~~ Droop Setting**
All Others	5%

Quebec Interconnection

There shall be no intentional governor deadband set on generators within the Quebec Interconnection by local requirement, shown in Table 3.7.

Formatted: Font: Not Bold, Font color: Auto

Table 3.7: Quebec Interconnection Deadband Settings

Generator Type	Maximum Deadband Setting
All Generation	N/A

The required governor droop settings shall not exceed five percent for all types (synchronous, inverter based and other technologies) of generation within the Quebec Interconnection by local requirement (see Table 3.8).

Formatted: Font: Not Bold, Font color: Auto

Table 3.8: Quebec Interconnection Droop Settings

Generator Type	Maximum ~~Deadband~~ Droop Setting
All Generation	5%

Chapter 4: Performance Assessment

Some BAs have developed methods for determining if governors are working properly by reviewing energy management system scan rate data (e.g., every four seconds) stored in their data historians (e.g., OSISoft, PI, AVEVA eDNA). Verification of proper governor function within a BA can be time consuming and requires specific expertise. BAs are strongly encouraged to evaluate the governor's responses being provided within their BA area to an adequate FRR is available in real time. To assist in this effort, methods used successfully by some BA to address this task are presented below and may be used as a starting point for similar efforts of other BAs, GOPs, and GOs.

The ERCOT Interconnection is a single BA Interconnection and has developed metrics to evaluate governor response performance. These metrics are included in the Regional Reliability Standard BAL-001-TRE-1, Attachment 2 "Primary Frequency Response Reference Document." BAL-001-TRE-1 Attachment A, provides performance metric calculations for initial PFR, sustained PFR, and limits on calculation of PFR performance. PFR uses a fixed time interval to determine initial governor response to a frequency event. Sustained PFR also establishes a fixed time interval; this time is used to determine if frequency response is being sustained through the stabilization period. High scores on both metrics indicate that frequency response is being sustained as desired. Low scores on both can indicate that frequency response is not being provided. Problems with outer loop control causing frequency response to be withdrawn (i.e., squelched response) can be indicated by a relatively high score in the initial PFR metric and a lower score in sustained PFR metric.

NERC also uses a similar tool to that of ERCOT, known as the Generator Resource Survey to calculate governor PFR by using historical data or manually calculated values. This tool, which uses the NERC Reliability~~Regional~~ Standard BAL-001-TRE-1 as a starting framework, evaluates an individual resource's ability to provide PFR during both the initial period and the sustained period. This tool is used for single event and unit evaluation and is intended to be used as a benchmarking tool for an individual resource as well as for the BA. It evaluates resources for their ability to provide PFR much like the BAL-001-TRE-1 except for a few notable differences. Those differences include the lack of consideration of certain aspects of conventional steam turbine operation and natural gas turbine and combined-cycle operation due to lack of data availability to many BAs and GOs. The survey is intended to be a starting point for the evaluation of resources and their ability to provide PFR through both the initial excursion of a frequency event as well as during the arresting/stabilization period during the recovery.

Several NPCC BAs within the NPCC Region have used a graphical approach to determining if generator governor response is being sustained. Two plots of generator output and frequency are reviewed in the evaluation of a generator's response along with some supplemental data. The first plot (starting five minutes before the decline in frequency and ending 15 minutes after the decline in frequency) is used to determine if other factors (e.g., such as unit ramping or AGC control) are occurring, which may invalidate the utility of the sample (i.e., it is not a "controlled" experiment). The second plot (starting one minute before the decline in frequency and ending two minutes after the decline in frequency) is used to determine the type of response observed and to calculate an observed droop if the response is being sustained. The analysis performed is a three-step process: sample validation, response type classification, and droop verification. The process is explained further in Appendix B ~~**Appendix B**~~. A fixed time window is not used in the response type classification and droop verification because Eastern Interconnection frequency deviations often persist for longer than one minute, and frequency response should be sustained until the frequency returns to a value within the governor deadband.

Appendix A: Typical Unit Response to Low and High Frequency Events by Unit Type

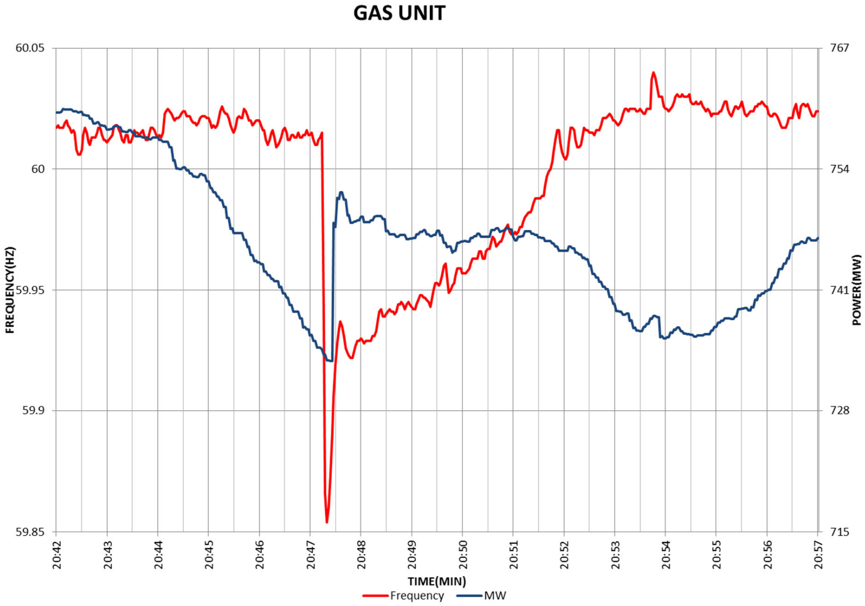


Figure A.1: Gas Unit Responding to Low Frequency Event at 17 mHz Deadband and Five Percent Droop

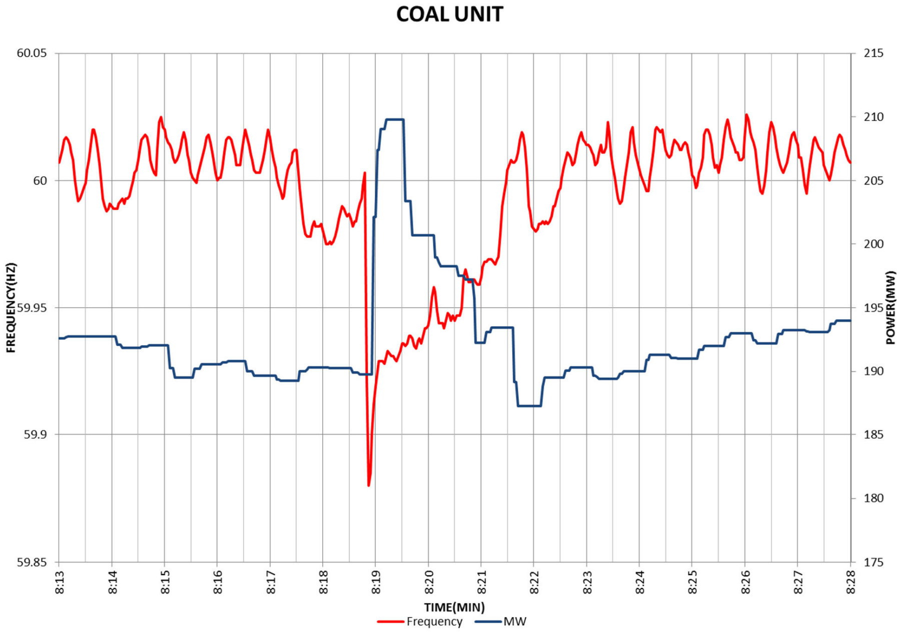


Figure A.2: Coal Unit Responding to Low Frequency Event at 17 mHz Deadband and Five Percent Droop

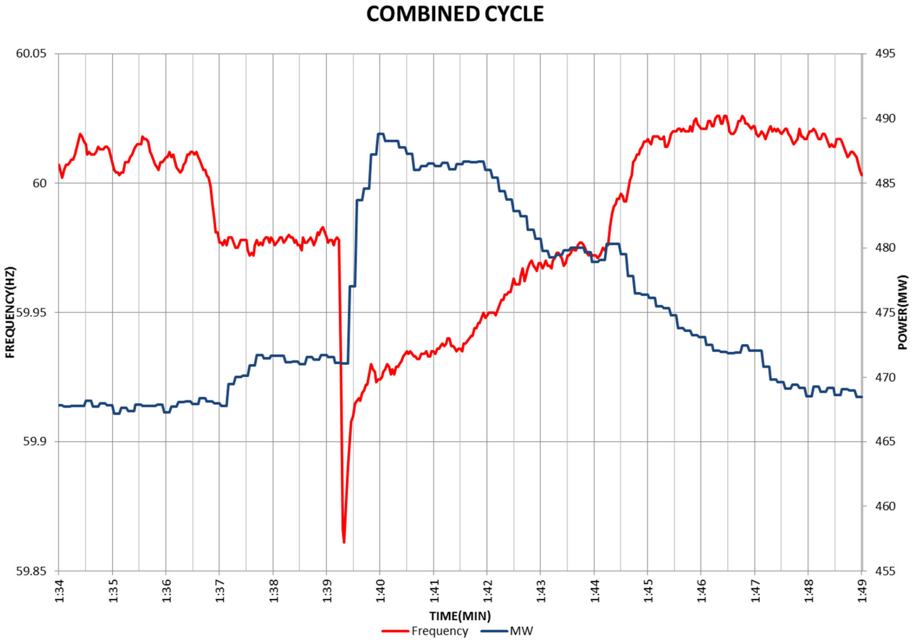


Figure A.3: Combined-Cycle Unit/Block Responding to Low Frequency Event at 17 mHz Deadband

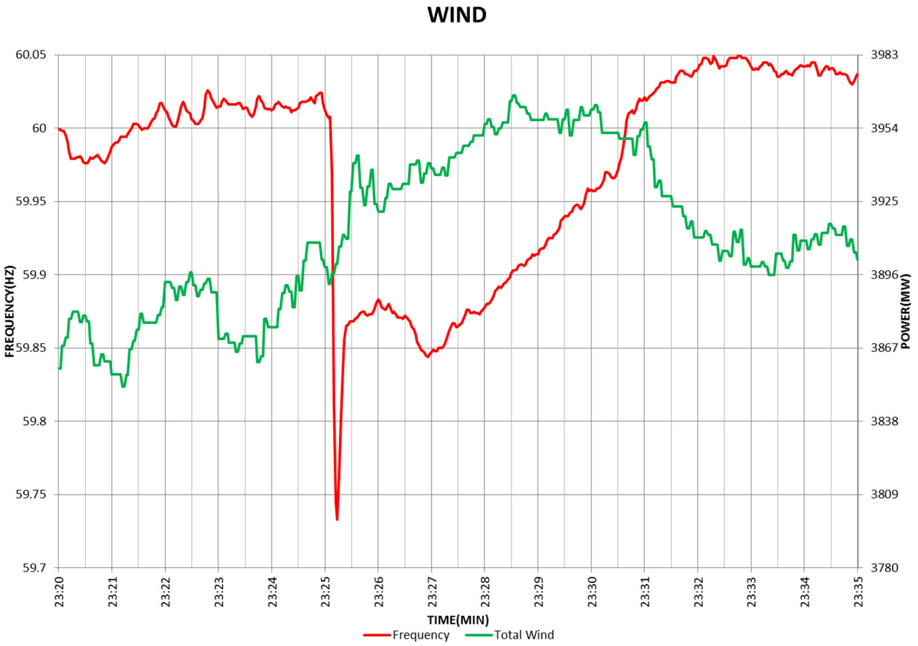


Figure A.4: Wind Resources Responding to Low Frequency Event at 17 mHz Deadband and Five Percent Droop

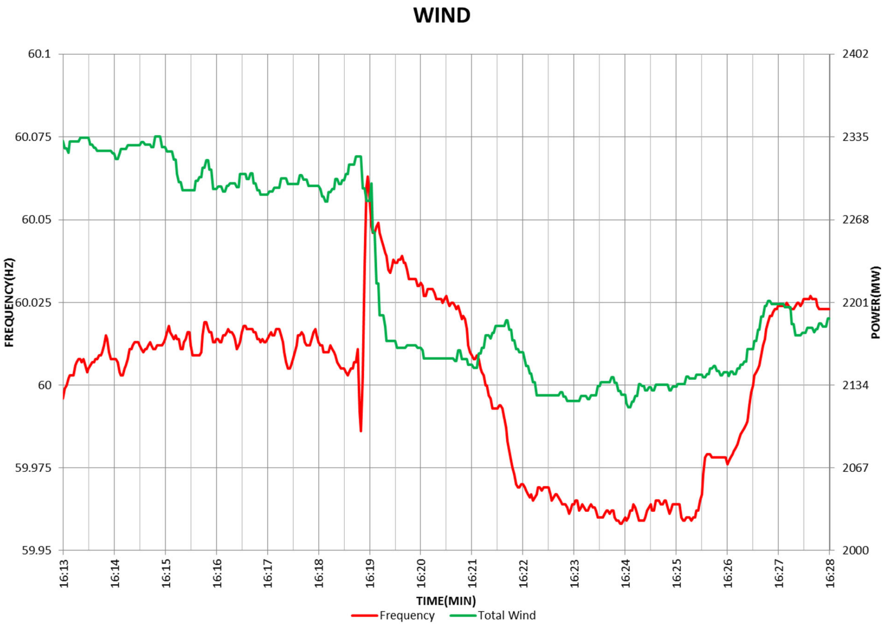


Figure A.5: Wind Resources Responding to High Frequency Event at 17 mHz Deadband and Five Percent Droop

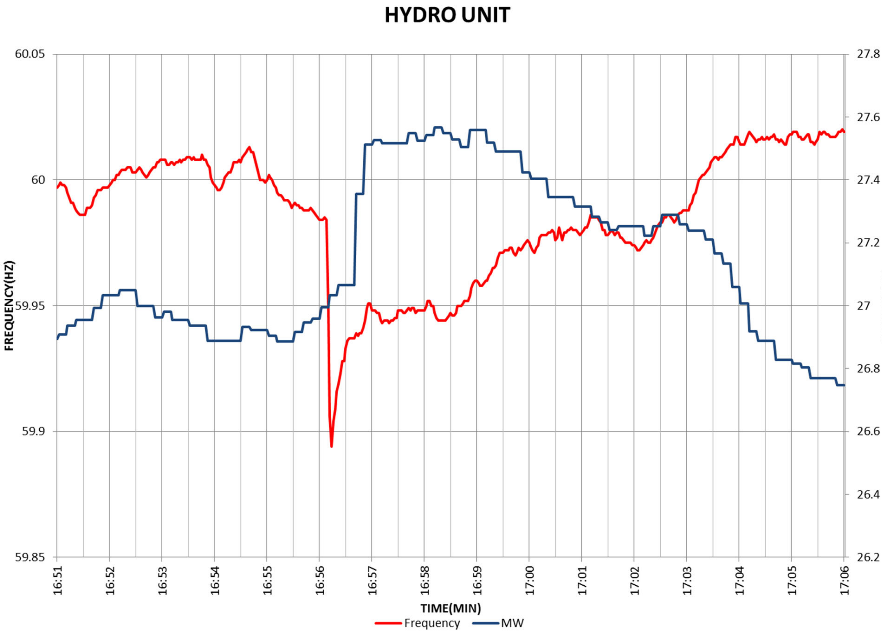


Figure A.6: Hydro Resource Responding to Low Frequency Event at 17 mHz Deadband and Five Percent Droop

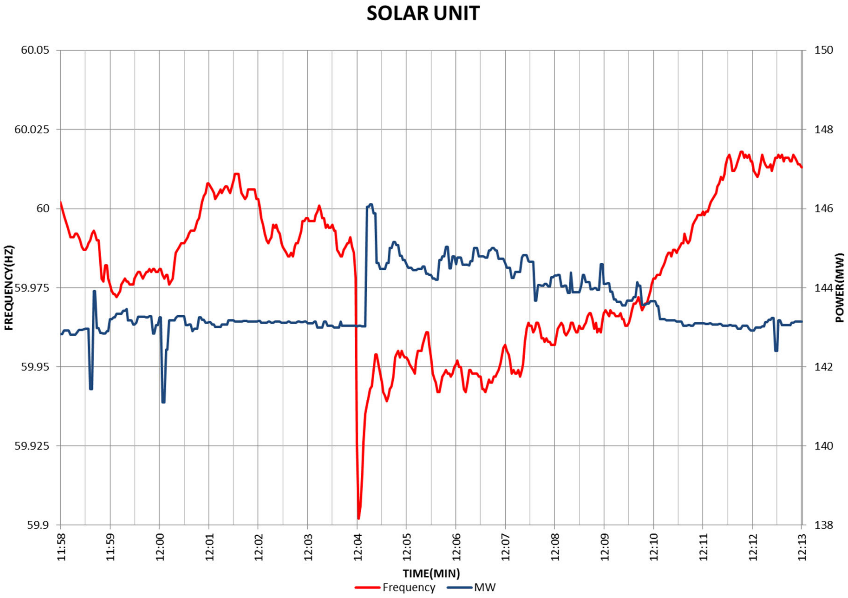


Figure A.7: Solar Resource Responding to Low Frequency Event at 17 mHz Deadband and Five Pecent Droop in ERCOT

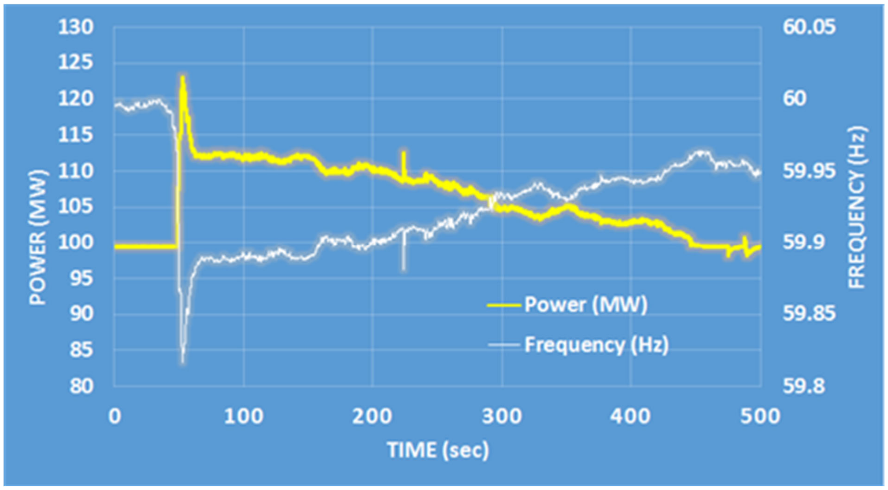


Figure A.8**: Solar Resource Responding to Low Frequency Event at 36 mHz Deadband and Three Percent Droop in WECC**

Appendix B: -Sample Validation, Response Type Classification, and Droop/Deadband Verification

Sample Validation

There are several factors to be considered in determining if a particular declining frequency event can provide useful information about the frequency response of a particular generator. Any one of the following factors can reduce the confidence in or totally invalidate the performance sample:

- Poor signal resolution from the plant historian.
- ~~2.~~ Historian compression techniques duration and extent of frequency excursion beyond the expected governor deadband limit.
- Oscillatory generator output due to plant control tuning problems.
- ~~3.~~ Generator is off-line, ramping up or down due to dispatch instructions, or on AGC.
- Output is at or near the generator high limit at the time of the frequency event.
- ~~4.~~ Insufficient accuracy of the data acquisition system to measure and record the measured parameters.
- Noisy telemetry of the output of the generator.
- ~~5.~~ Actual high limit's sensitivity to ambient temperature versus a high limit provided based on forecasted temperature.
- Higher levels of output provided by equipment that is not frequency responsive (e.g., duct burners, steam injection).

Formatted: Outline numbered + Level: 1 + Numbering Style: Bullet + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Outline numbered + Level: 1 + Numbering Style: Bullet + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Outline numbered + Level: 1 + Numbering Style: Bullet + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Outline numbered + Level: 1 + Numbering Style: Bullet + Aligned at: 0.25" + Indent at: 0.5"

Response Type Classification

Once a sample for a declining frequency event has been validated, an attempt is made to classify a sample as one of the following types based on a review of the plots of actual generation and frequency:

- Sustained: Output increases after the frequency deviates outside the governor deadband with frequency response that is proportional to the ongoing frequency deviation beyond the governor deadband continuing until the frequency returns to be within the governor deadband.
- ~~6.~~ Withdrawal/Squelched: Output increases after the frequency deviates outside the frequency deadband, but it decreases significantly in the direction of the output level that existed prior to the decline in frequency even though the frequency continues to be outside the governor deadband.
- No Response: Output is essentially unchanged when the frequency deviates outside the governor dead-band.
- ~~7.~~ Negative Response: Output declines as the frequency declines, possibly due to thermal limitations or improper configuration of plant controls.

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Outline numbered + Level: 1 + Numbering Style: Bullet + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Font: Not Bold

Formatted: Font: Not Bold

Formatted: Outline numbered + Level: 1 + Numbering Style: Bullet + Aligned at: 0.25" + Indent at: 0.5"

Individual samples are compared to determine an overall response type classification and repeatability among samples is a key factor in this determination. A high degree of confidence in the overall classification can be developed when five to 10 samples exhibit the same response type. However, an overall assessment of squelched response may require a greater number of samples as the relative values of actual generation versus the desired dispatch level and its surrounding megawatt control deadband can result in a mixture of response types among samples. For example, out of 20 samples, six may appear to be sustained, six may appear to be squelched, six may appear to have no response, and two may appear to be negative responses.

Governor Deadband and Droop Verification

For generators classified as having sustained response, the governor deadband and governor droop settings can be verified. An expected output change for a declining frequency event can be computed based on generator size, governor deadband expected governor settings, and the frequency observed when it is relatively stable prior to the event. The computed expected response can be compared with the actual observed change in output. Greater confidence in this verification can be achieved if the mean and median of about ten events are used in the comparison.

If the droop and deadband settings are not known, but there are about 10 samples of sustained response, trial droop and deadband values can be used to estimate an effective droop/deadband pair by matching the mean and median of the observations with those expected for candidate droop/deadband pairs.

The empirical/effective droop settings can vary substantially for some conventional thermal generators based on load levels. For some generators, it may be necessary to compute different effective droop values for different output ranges. The droop rating is applicable to the entire operating range while droop performance can vary depending on the initial load (and its corresponding governor valve position) when a frequency event occurs.

Formatted: Justified, Space After: 0 pt, Line spacing:

Appendix C: : Definitions and Terminology

Area Control Error (ACE): The instantaneous difference between a Balancing Authority's net actual and scheduled interchange, taking into account the effects of Frequency Bias, correction for meter error, and Automatic Time Error Correction (ATEC) if operating in the ATEC mode. ATEC is only applicable to BAs in the WI.

Arrested Frequency – Value C – Point C – Frequency Nadir: The point of maximum frequency excursion in the first swing of the frequency excursion between time zero (Point A) and time zero plus 20 seconds.

Arresting Period: The period of time from time zero (Point A) to the time of Point C.

Arresting Period Frequency Response: A combination of load damping and the initial Primary Control Response acting together to limit the duration and magnitude of frequency change during the Arresting Period.

Automatic Generation Control (AGC): Equipment that automatically adjusts generation in a Balancing Authority Area from a central location to maintain the BA's interchange schedule plus Frequency Bias. AGC may also accommodate automatic inadvertent payback and time error correction.

Balancing Authority (BA): The responsible entity that integrates resource plans ahead of time, maintains load-interchange-generation balance within a BA Area, and supports interconnection frequency in real time.

Frequency: The rate at which a period waveform repeats itself. Frequency is measured in cycles per second or in hertz (Hz). The symbol is "F."

Frequency Deviation: A difference between the interconnection frequency and the interconnection scheduled frequency.

Frequency Responsive Reserve: The capacity of Governor Response and/or Frequency-Responsive Demand Response that will be deployed for any frequency excursion.

Frequency-Responsive Demand Response: Voluntary load shedding that complements governor response. This load reduction is typically triggered by relays that are activated by frequency.

Headroom: The difference between the current operating point of a generator and its maximum operating capability.

Inertia: The property of an object that resists changes to the motion of an object. For example, the inertia of a rotating object resists changes to the object's speed of rotation. The inertia of a rotating object is a function of its mass, diameter, and speed of rotation.

Load Damping: The damping effect of the load to a change in frequency due to the physical aspects of the load such as the inertia of motors and the physical load to which they are connected.

Plant Secondary Control: Secondary control refers to controls affected through commands to a turbine controller issued by external entities not necessarily working in concert with frequency management objectives. It is common for a modern power plant to have several distinct modes of secondary control implemented within the plant and to be able to accept secondary control inputs from sources external to the plant.

Primary Control Response Withdrawal: The withdrawal of previously delivered Primary Control Response, through plant secondary controls.

Primary Frequency Control: Actions that deliver power to the interconnection in response to a frequency deviation through inertial response generator governor response, load response (typically from motors), demand response (designed to arrest frequency excursions), and other devices that provide an immediate response to frequency based on local (device-level) control systems, without human or remote intervention.

Recovery Period: The period of time from when Secondary Control Response are deployed (typically about zero plus 53 seconds) to the time of the return of frequency to within pre-established ranges of reliable continuous operation.

Settling Frequency: Refers to the third key event during a disturbance when the frequency stabilizes following a frequency excursion. Point B represents the interconnected system frequency at the point immediately after the frequency stabilizes due to governor action but before the contingent control area takes corrective AGC action.

Secondary Frequency Control: Actions provided by an individual BA or its Reserve Sharing Group intended to restore Primary Control Response and restore frequency from the Arrested Frequency back to Scheduled Frequency, or to maintain Scheduled Frequency deployed in the “minutes” time frame. Secondary Control comes from either manual or automated dispatch from a centralized control system. Secondary Control also includes initial reserve deployment for disturbances and maintains the minute-to-minute balance throughout the day and is used to restore frequency to normal following a disturbance and is provided by both spinning and non-spinning reserves.

Tertiary frequency control: Encompasses actions taken to get resources in place to handle current and future changes in load or contingencies. Reserve deployment and Reserve restoration following a disturbance is a common type of Tertiary frequency control.

Appendix D: Related Documents

Formatted: Justified, Space After: 0 pt, Line spacing:

Frequency Control Requirements for Reliable Interconnection Frequency Response – Lawrence Berkeley National Laboratory

FERC Order 842

Field Code Changed

Reliability Guideline: Operating Reserve Management – Version 23

~~Primary Frequency Response and Control of Power System Frequency~~

Demonstration of Essential Reliability Services by a 300-MW Solar Photovoltaic Power Plant

Advanced Grid-Friendly Controls Demonstration Project for Utility-Scale PV Power Plants

~~NERC Inverter-Based Resource Performance Task Force Inverter Based Resource Guideline~~

NERC Inverter-Based Resource Performance Task Force Fast Frequency Response Concepts and Bulk Power System Reliability Needs White Paper

~~Technology Capabilities for Fast Frequency Response~~

IEEE PES Appendix B of "Dynamic Models for Turbine-Governors in Power System Studies"

Frequency Response Initiative Report 2012

NERC Alert A-2015-02-05-01

BAL-001-TRE-1 Attachment A

Using Renewables to Operate a low-carbon Grid: Demonstration of Advanced Reliability Services from a Utility-Scale Solar PV Plant

PRC-001-WECC-CRT-2

Contributors

NERC gratefully acknowledges the contributions and assistance of the following industry experts in the preparation of this guideline.

Name	
Troy Blalock	Dominion Energy South Carolina
Nitika Mago	ERCOT
Greg Park	Northwest Power Pool
Sam Rugel	Tucson Electric Power Company
William Shultz	Southern Company Generation/ NAGF member
Terry Bilke	
Darrel Richardson	North American Electric Reliability Corporation
~~Levitra~~ Levetra Pitts	North American Electric Reliability Corporation

Guideline Information and Revision History

Guideline Information	
Category/Topic: [NERC use only]	**Reliability Guideline/Security Guideline/Hybrid:** Primary Frequency Control
Identification Number: [NERC use only]	**Subgroup:** NERC Resource Subcommittee

Revision History		
Version	**Comments**	**Approval Date**
1.0	Initial Version – *Reliability Guideline: Primary Frequency Response*	12/15/2015
2.0	Updated Document to include additional guidance for Primary Frequency Response	9/19/2018
3.0	Update document to include additional guidance for Primary Frequency Response	5/1/2019
4.0	Updated document to include references to IBRTF, added metrics and formatted to new guideline	

Metrics

Pursuant to the Commission's Order on January 19, 2021, *North American Electric Reliability Corporation*, 174 FERC ¶ 61,030 (2021), reliability guidelines shall now include metrics to support evaluation during triennial review consistent with the RSTC Charter.

Baseline Metrics

All NERC reliability guidelines include the following baseline metrics:

- BPS performance prior to and after a reliability guideline as reflected in NERC's State of Reliability Report and Long Term Reliability Assessments (e.g., Long Term Reliability Assessment and seasonal assessments).
- Use and effectiveness of a reliability guideline as reported by industry via survey.
- Industry assessment of the extent to which a reliability guideline is addressing risk as reported via survey.

Specific Metrics

The RSTC or any of its subcommittees can modify and propose metrics specific to the guideline in order to measure and evaluate its effectiveness, listed as follows:

- NERC M-4 Interconnection Frequency Response.
- NERC BAL- 003 compliance by BA or FRSG.

Effectiveness Survey

On January 19, 2021, FERC accepted the NERC proposed approach for evaluating Reliability Guidelines. This evaluation process takes place under the leadership of the RSTC and includes:

- industry survey on effectiveness of Reliability Guidelines;
- triennial review with a recommendation to NERC on the effectiveness of a Reliability Guideline and/or whether risks warrant additional measures; and
- NERC's determination whether additional action might be appropriate to address potential risks to reliability in light of the RSTC's recommendation and all other data within NERC's possession pertaining to the relevant issue.

~~NERC is asking entities who are users of Reliability and Security Guidelines to respond to the short survey provided in the link below.~~

~~Guideline Effectiveness Survey [insert hyperlink to survey]~~

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Guideline

Primary Frequency Control

January 24, 2023

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

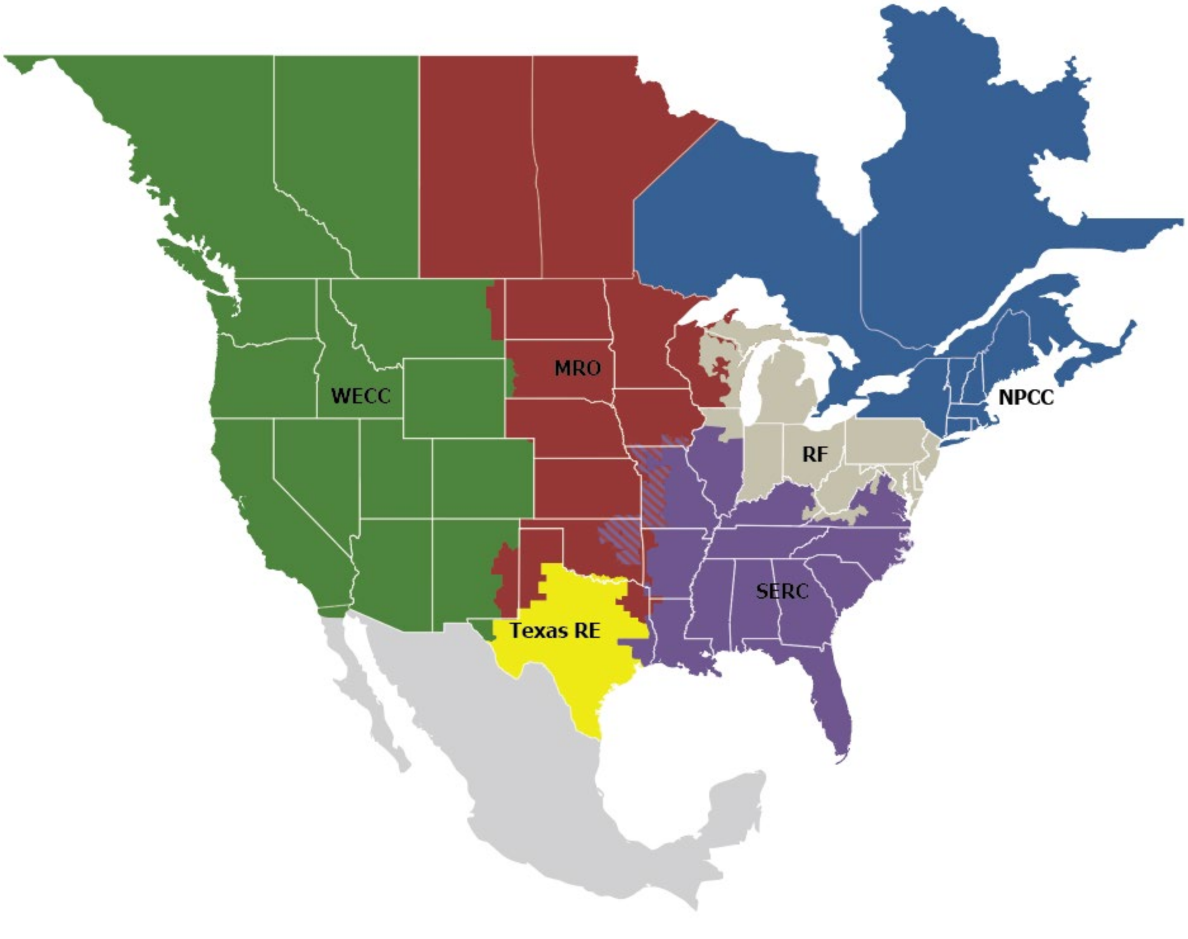
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the NERC and the six Regional Entities, is a highly reliable, resilient, and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six Regional Entity boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners /Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Preamble

The NERC Reliability and Security Technical Committee (RSTC), through its subcommittees and working groups, develops and triennially reviews reliability guidelines in accordance with the procedures set forth in the RSTC Charter. Reliability guidelines include the collective experience, expertise, and judgment of the industry on matters that impact BPS operations, planning, and security. Reliability guidelines provide key practices, guidance, and information on specific issues critical to promote and maintain a highly reliable and secure BPS.

Each entity registered in the NERC compliance registry is responsible and accountable for maintaining reliability and compliance with applicable mandatory Reliability Standards. Reliability guidelines are not binding norms or parameters nor are they Reliability Standards; however, NERC encourages entities to review, validate, adjust, and/or develop a program with the practices set forth in this guideline. Entities should review this guideline in detail and in conjunction with evaluations of their internal processes and procedures; these reviews could highlight that appropriate changes are needed, and these changes should be done with consideration of system design, configuration, and business practices.

Executive Summary

This reliability guideline provides recommendations to the industry for frequency control, covering governor deadband and governor droop settings that can enable generating resources (synchronous, inverter-based, and other technologies) to provide needed primary frequency response (PFR) to the Interconnection.

NERC Regional Reliability Standard BAL-001-TRE-1 Primary Frequency Response in the ERCOT area establishes required governor settings for generating resources operating in the Texas Interconnection. Similarly, WECC has a regional criterion (PRC-001-WECC-CRT-2) that establishes a range of acceptable governor droop settings for generators operating in their footprint.

This Guideline does not create binding norms, does not establish mandatory Reliability Standards and does not create parameters by which compliance with Reliability Standards are monitored or enforced. In addition, this Reliability Guideline is not intended to take precedence over any Regional procedure.

Introduction

Purpose

This Reliability Guideline outlines a coordinated operations strategy for resources to stabilize system frequency when frequency deviates due to a grid event. It is designed to keep frequency within allowable limits while maintaining acceptable frequency control.

Applicability

This reliability guideline is intended to assist Balancing Authorities (BAs), Generator Operators (GOPs), Generator Owners (GOs), Transmission Operators (TOPs), and Transmission Owners (TOs) in understanding the fundamentals of frequency control, the recommended governor deadband and governor droop settings (so as to provide more effective frequency response during major grid events), and the techniques of measuring frequency response at a resource level. It is offered as information to other functional model entities. It outlines a coordinated operations strategy to restore system frequency after frequency has deviated due to a BES disturbance.

The primary focus of this guideline is the PFR provided by generating resources during loss of generation scenarios. Other forms of resources providing frequency response should have similar response characteristics described herein for governors.

Chapter 1: Frequency Control – Fundamentals

The instantaneous balance between generation and load is directly reflected in an interconnected electric power system's frequency. Reliable power system operation depends on controlling frequency within predetermined boundaries above and below a nominal value. In North America, this value is 60 cycles per second (or 60 Hertz (Hz)). These concepts unambiguously apply to other Interconnections with different nominal frequencies.

BAs are responsible to dispatch generation and manage their area control error (ACE) in a manner that maintains frequency at the scheduled value using automatic generation control (AGC) on a continuous basis. NERC BAL standards establish the frequency control performance requirements for BAs.

Resilient interconnection frequency response to a sudden loss of generation or load depends upon the coordinated interplay of inertia, load damping, and defined control actions.

Figure 1.1 shows a simplified illustration of frequency and power trends that would be seen in a properly functioning power system in response to a sudden loss of generation. The event has been segmented into three periods to aid in the discussion of frequency control actions. Frequency is managed by the combined actions of primary, secondary, and tertiary controls.

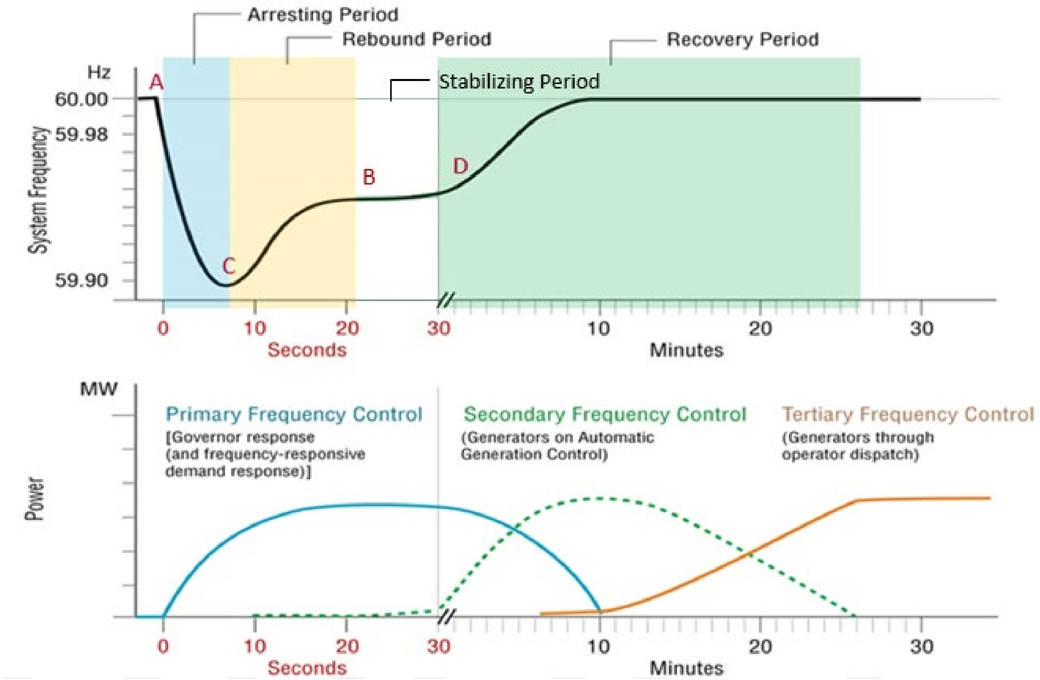


Figure 1.1: The Sequential Actions and Impacts on System Frequency of Primary, Secondary, and Tertiary Frequency Control

Source: Eto, et al. LBNL: Use of a Frequency Response Metric to Assess the Planning and Operating Requirements for Reliable Integration of Variable Renewable Generation

Arresting Period

As shown in the top trace (Figure 1.1), the "A Point" is defined as the predisturbance frequency. The time period beginning with a generation loss at T_0 and ending at the lowest frequency deviation, frequency nadir or C-Point, is labeled the "Arresting Period." Primary control action, indicated by the solid blue line in the bottom part of the figure, starts to engage immediately once frequency falls outside the deadband. In this period, the decay of frequency must be arrested to avoid triggering under frequency load shedding (UFLS). The decline of frequency is arrested only when the combined response from load changes, load damping, demand response, and PFR responsive equals the size of generator loss. Inertia plays a critical role in determining the timing with which frequency response must be delivered to arrest the decline of frequency. The behavior of frequency after the arrest depends on the effect of primary and secondary control action and load changes.

Recovery Period

The recovery period can be divided into three sub-periods referred to as rebound, stabilizing, and recovery. In the example event referenced earlier in Figure 1.1, the rebound period is defined by the sharp recovery of frequency between the C Point and T+20 seconds. Early withdrawal of primary response, as indicated by the dashed blue line, dampens the rebound and slows the recovery of frequency. The stabilizing period is defined as the window between T+20 to T+60 seconds when frequency has leveled out after the rebound period. During the stabilizing period, the collective PFR establishes a new balance between load and generation at a frequency called the settling frequency. In NERC BAL-003-1.1, the frequency defined by the period extending from T_{+20} to T_{+52} seconds is averaged and identified as the “B-Point” or the value at which frequency has been stabilized by PFR.

As mentioned above, frequency is stabilized at a value lower than the original scheduled frequency. This is an expected and necessary consequence of PFR delivered via droop control with a defined deadband. Governor droop changes resource output in proportion to the deviation of frequency once frequency has exceeded the deadband limit. PFR alone does not restore frequency to the original scheduled value primarily because governor-directed changes only occur when frequency is beyond the governor deadband.

Application of secondary control action begins when deviations of frequency and power flows are detected and continues until scheduled values have been restored. The action of automatic generation controls may be augmented or modified by manual control actions directed by system operators—such as deploying contingency reserves, demand response, or establishing emergency interchange schedules. Secondary frequency control action takes place more slowly than primary frequency control actions. For example, in the case of AGC, secondary frequency control is initiated by external automated commands sent every two to six seconds. Resources typically employ a rate-of-change limit on the AGC input to the unit control system. This results in a ramp response of a resource to secondary control action.

Secondary response may require 5 to 15 minutes (and sometimes more) to complete the restoration of frequency to the scheduled value. It is therefore critical to recognize that the sustained delivery of PFR is essential for stabilizing frequency throughout the recovery period to ensure system reliability.

Post Recovery Period

In the third stage, frequency has been restored to its scheduled value, and the reserves held to provide primary and secondary frequency control are restored by tertiary control. The goal of tertiary control actions is to restore the reserves that were used to deliver PFR and secondary frequency response during the recovery period. Reserves may be restored using redispatch, commitment of resources, or establishing new interchange schedules. Restoring these reserves completes the repositioning of the power system so that it is prepared to respond to a future loss-of-generation event.

Chapter 2: Primary Frequency Control

NERC recommends that all generating resources be equipped with a functioning governor. FERC Order 842[1] requires any new synchronous and nonsynchronous generators to install, maintain, and operate equipment capable of providing PFR as a condition of interconnection. Primary frequency control is the first active response of resources to arrest the locally measured or sensed changes in speed/frequency. Governors are continuously active, automatic, not driven by a centralized system, and respond instantaneously to frequency deviations exceeding its governor deadband limits. Governor action is delivered proportionally on the droop curve for excursions of frequency beyond the governor deadband limits. Examples of PFR to high and low frequency events by generation type can be found in **Appendix A:**.

Allocation and Distribution of Frequency Responsive Reserve for Sustained Primary Frequency Response

The sudden loss of a generating resource will cause frequency to decline. Loss of generation events are fairly common. For this reason, each Interconnection should be designed and operated to withstand the sudden loss of a certain amount of generation without jeopardizing reliability. BAs are required to meet a frequency response obligation for their areas. Providing frequency response in such events is accomplished by maintaining frequency responsive reserve (FRR) capacity that is adequate to arrest and stabilize the decline in frequency and to reserve additional headroom that is adequate to restore frequency to its scheduled value. In a scenario where the reserved capacity of generation providing frequency response and secondary response is lower than the loss of generation, frequency would continue to decline and could potentially lead to the loss of load through the triggering of UFLS. The aggregate performance of the units supplying the reserve capacities can vary based on the number of generators and the generation mix of the fleet. Overall, the expectation is that the reserved capacity exceeds its largest expected generation loss with margin in order to account for uncertainty in the actual performance of the fleet. The NERC RSTC approved Operating Reserve Management Guideline[2] provides additional details on the recommended methods to determine FRR needs.

The frequency response expected of generators should not exceed the amount they can produce before the declining frequency triggers UFLS. It is highly recommended that FRR be distributed among many generators rather than a select few in order to limit the response each unit individually needs to contribute; additionally, distributed FRR facilitates the mitigation of and recovery from wide scale events. Drawing frequency response from a large pool of geographically diverse resources makes frequency response faster, more reliable, and more effective than drawing from select isolated resources. That, in turn, helps arrest frequency earlier resulting in a higher frequency nadir and reduces the risk that some units may not provide the expected response.

The responses to generation loss from two sets of reserves are compared in Figure 2.1. One (blue trace) is composed of resources that sustain PFR throughout the event in aggregate, and the other (red trace) is composed of resources that respond initially but do not sustain PFR throughout the event in aggregate. PFR is withdrawn from the set of reserves represented by the red trace before secondary frequency response is applied. In the initial phase of the event, the frequency trends for the two simulations are nearly identical because the same amount of PFR has been delivered. However, even as the nadir is reached, the effect of a lower amount of sustaining PFR of the reserves represented by the red trace can be observed; this leads to a lower apparent settling frequency. As the event progresses, the nonsustaining portion of the reserves represented by the red trace continues to reduce the PFR delivered. During the stabilizing period, frequency begins to decline again as there continues to be an imbalance of load and resource due to nonsustained PFR. This increases the risk of load being shed due to UFLS action.

---

[1] https://www.ferc.gov/whats-new/comm-meet/2018/021518/E-2.pdf

[2] https://www.nerc.com/comm/OC_Reliability_Guidelines_DL/Operating_Reserve_Management_Guideline_V2_20171213.pdf

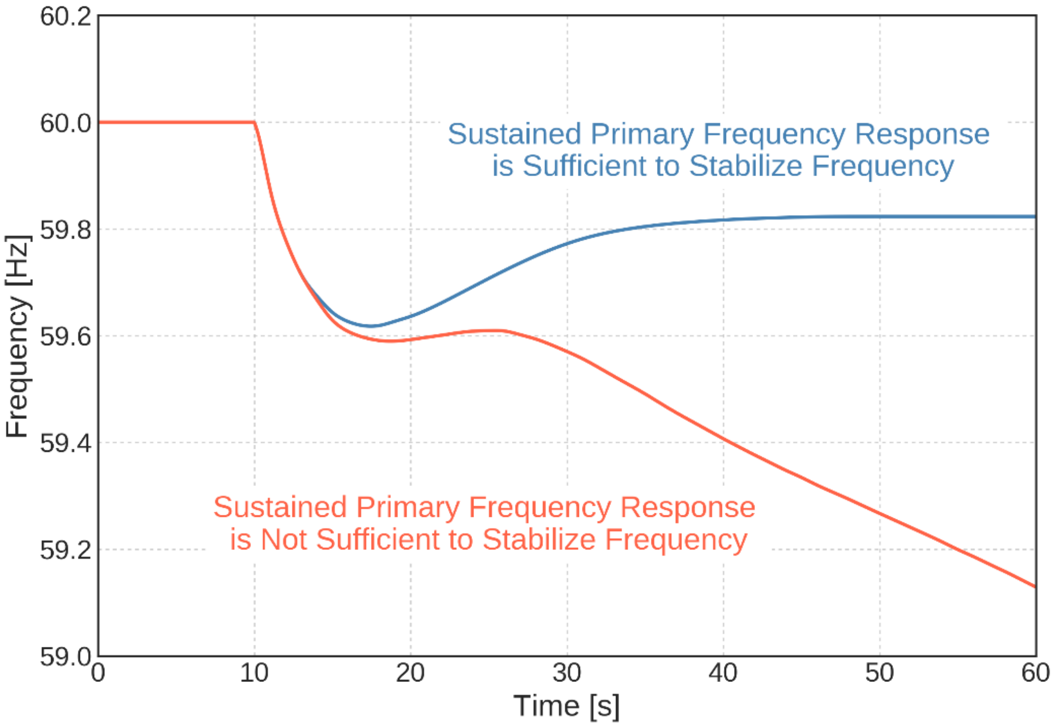


Figure 2.1: Sustaining vs Nonsustaining Primary Frequency Response Effect on System Frequency

Source: Developed by LBNL from Undrill (2018): Primary Frequency Response and Control of Power System Frequency

There are several reasons why PFR may not be sustained: The first is through withdrawal of PFR by the actions of plant-level or unit-level control of net resource output overriding and resetting the actions of the governor response to frequency deviations; the second is through actions stemming from inherent physical characteristics and limit actions of a generating resource. One example is the exhaust gas temperature limiter on certain types of combustion turbine/generators. These protective systems are intrinsic to the design of combustion turbine/generators and unlike plant-level controllers; these actions cannot be overridden or corrected. All generating resource types exhibit similar responses by equipment protection systems. These types of responses are also known as “squelched responses.”

These factors also reinforce the need to distribute reserves to numerous generators of different generation types in order to provide reliable sustained PFR. Each generating resource’s capability for providing a sustained response must be considered when accounting for expected PFR until it is replaced by response to secondary frequency control action.

Coordination between a Resource’s Governors and Output Controls

Modern generating resource control systems generally incorporate a form of plant or unit load control. These load control systems can be applied within the turbine control system, the plant or unit control system, or remotely from a central dispatch center. Regardless of their location or method of implementation, the design of secondary controls must be coordinated with that of the governor to ensure that PFR can be sustained.

Closed loop load control can exist at a minimum in one or possibly both load control loops based on operator selection. Proper coordination of control actions can be accomplished in several ways, including the following:

- Use of a frequency bias in the plant level load controller would allow it to adjust individual load targets in harmony with the governor response.

- Use of a frequency bias in the turbine level load controls in conjunction with open loop load control at the plant level would allow the turbine control panel to adjust its internal load control target in harmony with the governor response.
- In both case one and case two the plant level load controls can adjust targets in response to external input, (e.g., a revised AGC target). Plant and turbine controls must be coordinated with governor settings.
- Operation of the generating resource in pure governor control mode with manual adjustments to the speed governor target, such as analog or mechanical control systems. Some early digital controllers in use on generating resources may not be capable of operation in any form of megawatt (MW) target control.

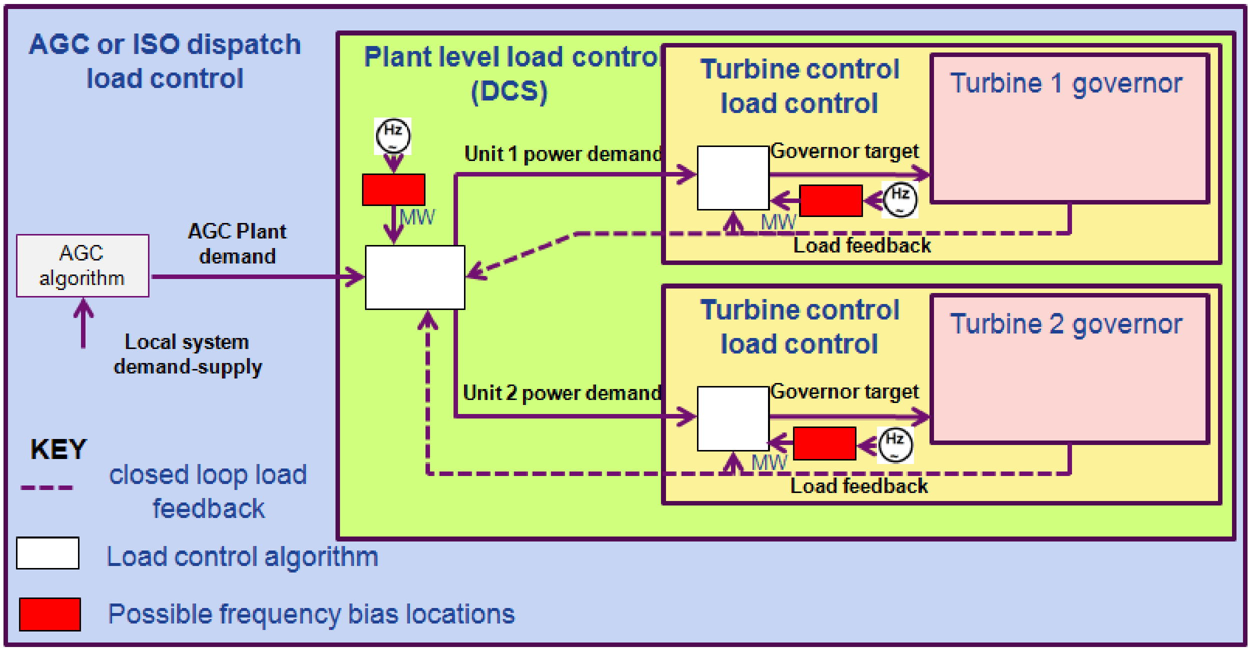
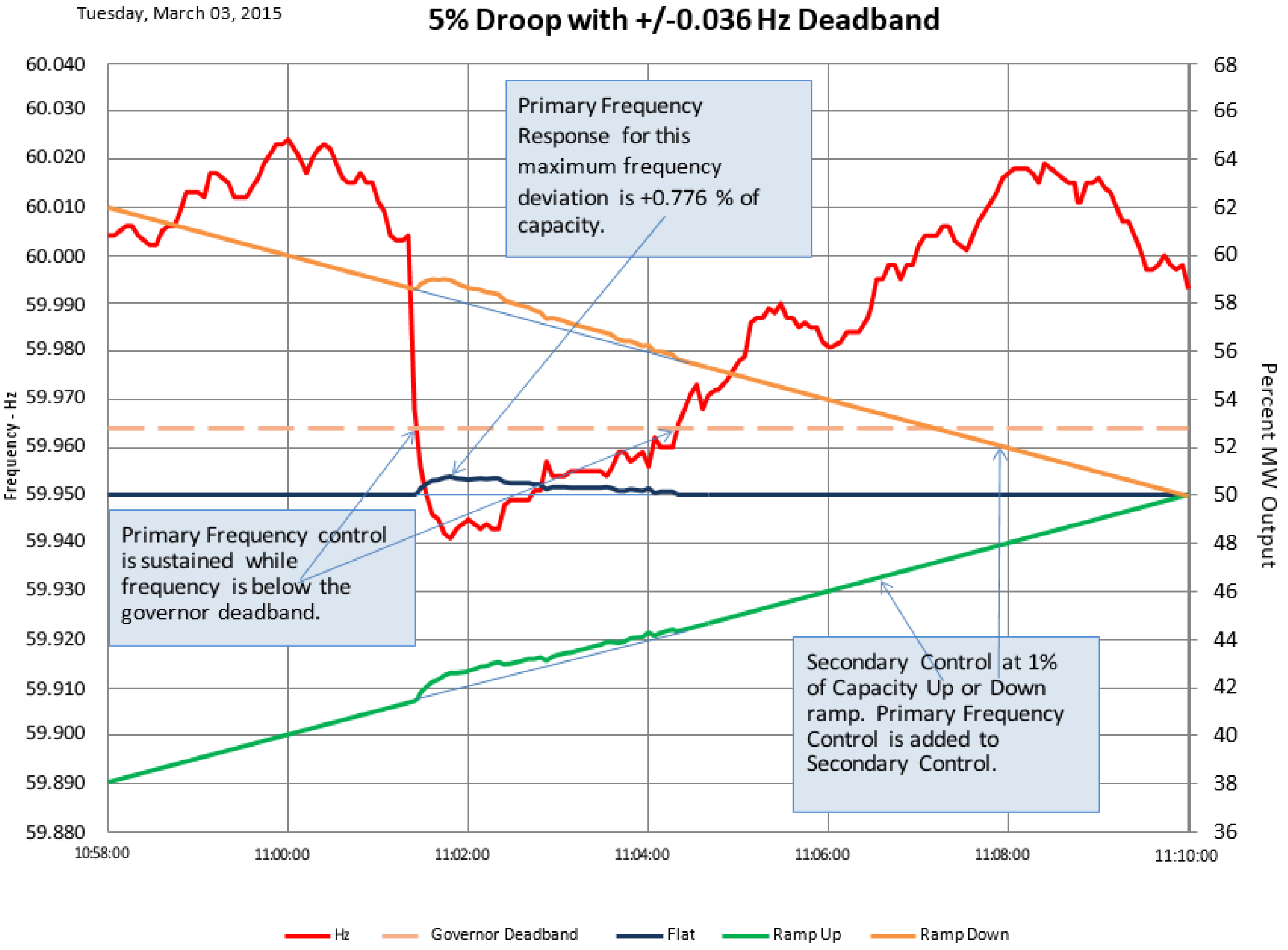


Figure 2.2: Typical High Level Generating Resource Control System

Frequency bias should be applied at all levels of closed loop MW output control for a coordinated generating resource response. See Figure 2.3 and Figure 2.4 for illustrations of expected frequency response from a generating resource that is properly coordinated to provide sustained PFR following loss of generation or loss of load when at steady output, ramping up, or ramping down.



Primary Frequency Response for this maximum frequency deviation is +0.776 % of capacity.

Primary Frequency control is sustained while frequency is below the governor deadband.

Secondary Control at 1% of Capacity Up or Down ramp. Primary Frequency Control is added to Secondary Control.

Figure 2.3: Example of Properly Coordinated Primary Frequency Control while Ramping MW Up or Down via Local or Remote Control or While Operating at a Fixed MW Output (Deadband = 36 mHz)

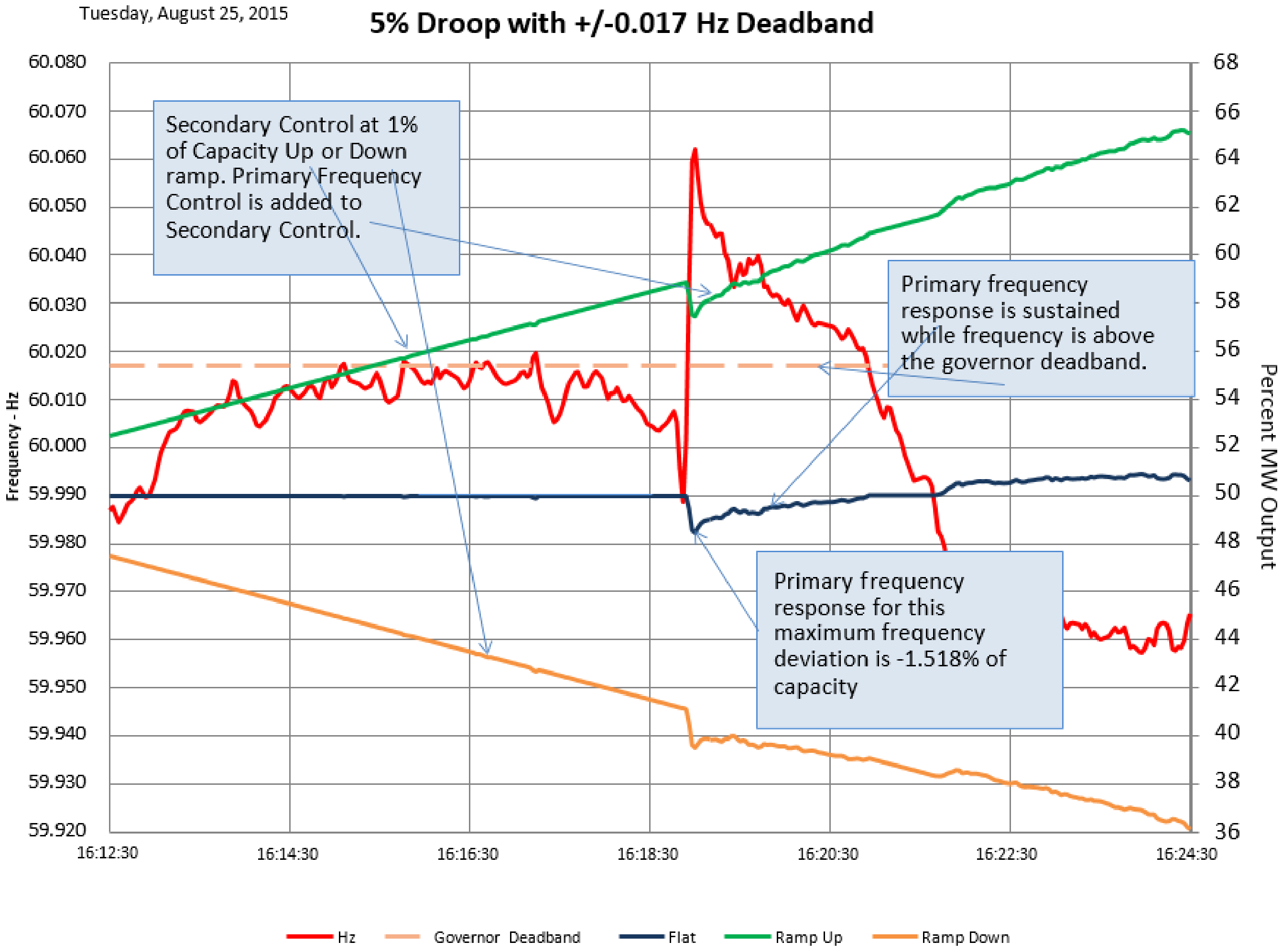


Figure 2.4: Example of Properly Coordinated Primary Frequency Control while Ramping MW Up or Down Via Local or Remote Control or while Operating at a Fixed MW Output in the Graph Above - High Frequency Excursion with a Lower Deadband (Deadband = 17 mHz)

Ability of Natural Gas Turbines to Sustain Primary Frequency Response Following Large Loss-of-Generation Events

Combustion turbine/generators are important contributors to arrest system frequency following a sudden loss of generation. However, if an under-frequency event calls for maximum output from a combustion turbine/generator, this output may not be sustainable due to reduced air flow, the working fluid of these engines, and the actions of the exhaust temperature limit protection system of the turbine. At less than nominal frequency, the combustion turbine/generator rotates more slowly and moves less air into/through the combustion process. Burning the same or greater amount of fuel with less air results in higher exhaust gas temperature. If exhaust gas temperatures exceed a preset limit, the combustion turbine/generator will reduce output automatically to protect the turbine from damage. Unlike the withdrawal of response by plant load-controls, reduction of output by this means cannot be deactivated at the discretion of the plant operator.

Moreover, there is linkage between the exhaust gas temperature protection system and system frequency that can be detrimental to reliable interconnection frequency response. If system frequency continues to be depressed or decline as the exhaust gas temperature controls reduce turbine output, then the temperature limit controls will further reduce turbine output.

Figure 2.5 illustrates this effect. The lower panel shows the control actions directed by the turbine-governor (red) and the exhaust gas temperature protection system (blue). Initially, the turbine-governor, responding to the decline in interconnection frequency, directs increased fuel flow to the turbine thus increasing the combustion rate and MW output. Once the turbine exhaust has reached its temperature limit, the protection system overrides the turbine-governor and directs lower levels of fuel flow until the exhaust temperature is below the limit. The top panel illustrates the impact these control actions could have on interconnection frequency when combustion turbine/generators predominate the generation mix in an interconnection and are operated near the exhaust temperature limit.

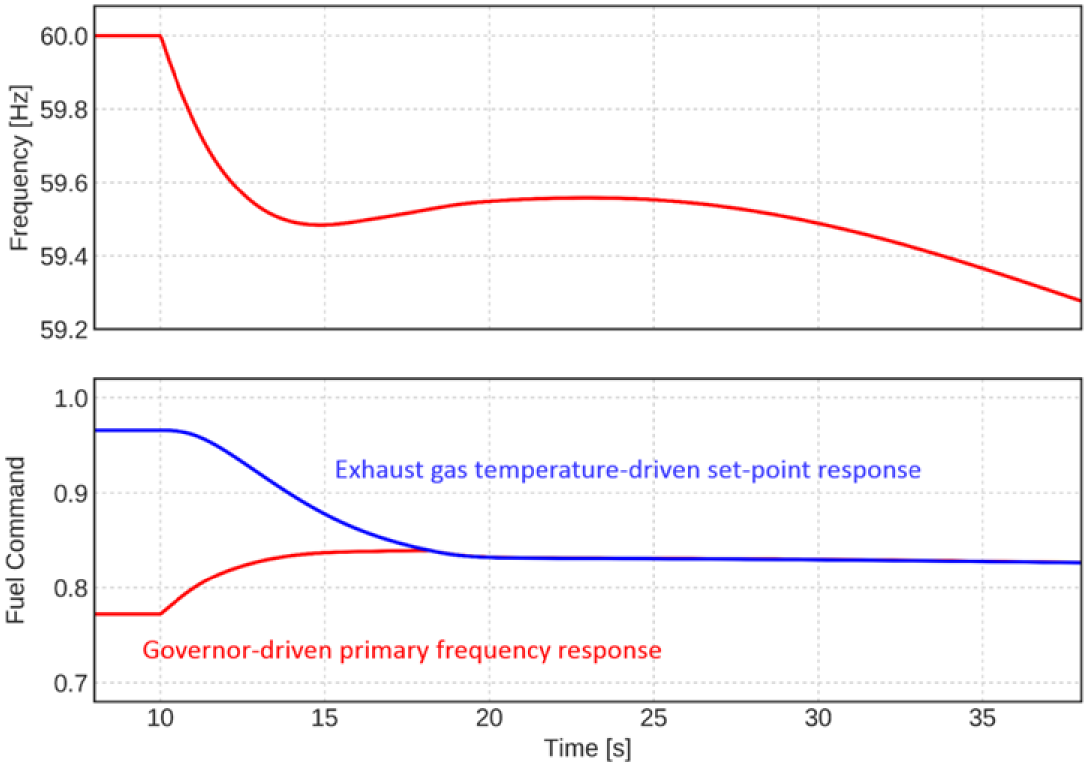


Figure 2.5: Exhaust Gas Temperature Controls on Gas Turbines Will Decrease Primary Frequency Response if Frequency Remains Depressed

Source: Developed by LBNL from Undrill (2018): Primary Frequency Response and Control of Power System Frequency

As noted, the effect of these controls cannot be overridden; they are intrinsic to the design of protection for the turbine. This reduction is better thought of as a reduction in the headroom or PFR capability of the natural gas turbine, rather than a form of withdrawal of PFR.

Primary Frequency Response from Inverter-Based Resources

Inverter-based resources (IBR) are capable of providing primary response in accordance with the common droop rule of the grid. IBRs have demonstrated their ability to respond to frequency deviation events in various Interconnections,[3] including ERCOT,[4] where it is a requirement. Most IBRs operate at maximum available output based on the availability of solar irradiance or wind speed. As a result, IBRs normally do not have headroom to provide PFR to low frequency events, but IBRs can provide very effective PFR to high frequency events. There are instances, however, where the resource may be curtailed; in these cases, IBRs would have the ability to provide PFR to frequency dips. IBRs normally have enough “down headroom” to provide PFR to high frequency events. More detailed guidance

---

[3] Demonstration of Essential Reliability Services by a 300-MW Solar Photovoltaic Power Plant

[4] Advanced Grid-Friendly Controls Demonstration Project for Utility-Scale PV Power Plants

on effective control settings, frequency measurement resolution, and speed of PFR delivery for IBRs is available in the *Power Plant Model Verification for Inverter-Based Resources Reliability Guideline.*[5]

Fast Frequency Controls on Electronically Coupled Wind Generation and Sustained Primary Frequency Response

Most modern wind turbines are Type 3 (doubly fed induction generator) or Type 4 (full-scale converter generator) and are designed to allow operation at variable speed to achieve greater efficiency. However, variable speed operation requires generator speed and system frequency to be decoupled from each other via use of power electronic converters. As a result, even though kinetic energy is stored in the rotating mass of a wind turbine, variable speed wind turbines do not inherently provide inertial response to grid disturbances. Inertia itself is not a substitute for primary frequency control because inertia, whether synthetic or real, is not a sustained source of energy injection; however, it continues to oppose frequency change in real time.

Fast frequency control systems have been developed by several wind turbine manufacturers to allow the kinetic energy stored in the rotating mass of a wind turbine to be extracted and provide temporary active power to the grid in response to a frequency trigger during low frequency events. Such fast response is not considered to be PFR because it cannot be sustained unless the resource is operating under curtailment.

Figure 2.6 shows the actual performance of a specific Type 3, 1.5 MW wind turbine equipped with "rotor inertia-based Fast Frequency Response" functionality for varied wind speeds. At 14 m/s (above nominal wind speed) there is no recovery phase. At 11.5 m/s, just below nominal wind speed, the recovery phase is the most demanding. Fast frequency control response decreases drastically at 50 percent of rated power and drops to zero at 20 percent of rated power, this is illustrated by 5 m/s (blue) trace below. This response is not proportional to frequency change and the same response will be provided for the same wind conditions for all frequency events.

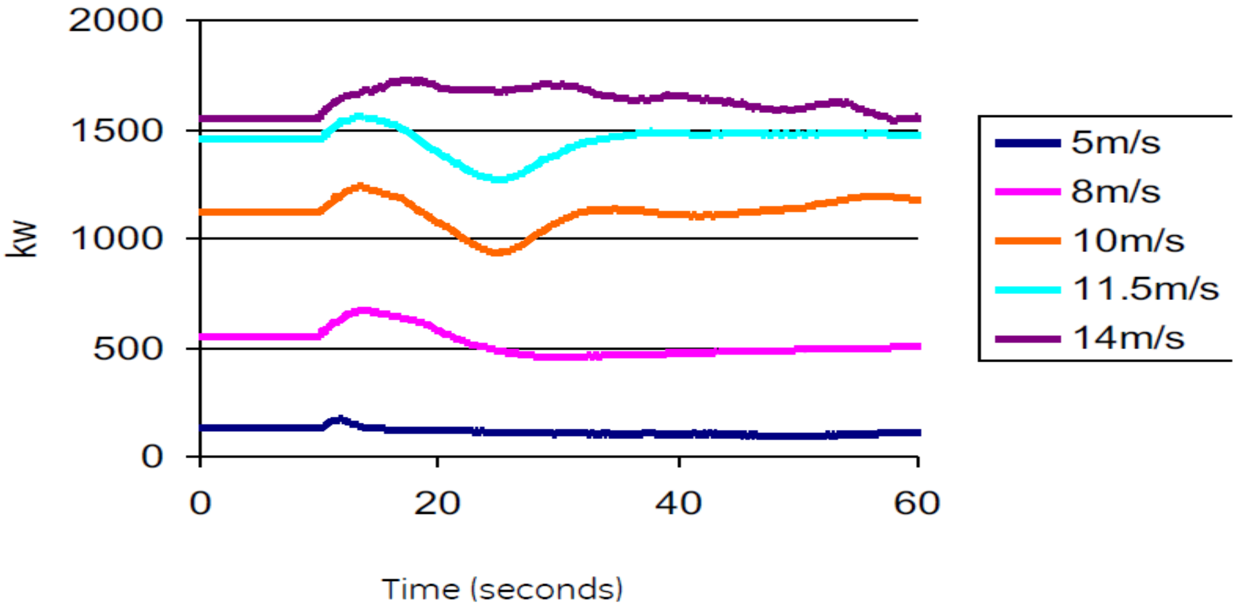


Figure 2.6: Fast Frequency Control Response of Wind Turbine at Different Wind Speed Conditions

It is important to recognize that the value of fast frequency control response is in energy being delivered during the arresting period to "buy" time for conventional PFR to act. Failing to sustain fast frequency response beyond the

---

[5] https://www.nerc.com/comm/RSTC_Reliability_Guidelines/PPMV_for_Inverter-Based_Resources.pdf

frequency nadir may lead to a prolonged recovery period. With that in mind, PFR coupled with fast frequency response from energy storage resources (activated only when headroom is allocated) and faster frequency response from IBRs with stored energy that can be tapped can help in the arresting period and is also sustained. To be beneficial to the power system, fast frequency control settings must be tuned to specific systems needs and various operating conditions. Additional details about fast frequency controls can be found in *Technology Capabilities for Fast Frequency Response,*[6] which was published by GE Energy Consulting in March 2017.

---

[6] https://www.nrel.gov/docs/fy17osti/67799.pdf

Chapter 3: Governor Deadband and Governor Droop Settings

This guideline proposes maximum governor deadband and governor droop settings to achieve desired frequency response for each of the Interconnections while subject to other technical, operational, or regulatory considerations that would prevent governors from achieving the particular governor settings. Although there are recommended governor deadband maximums for two of the Interconnections at 36 mHz, it should be noted that deadbands of 0 and 17 mHz have been successfully implemented for several generating resource types. Governor deadbands are recommended to be implemented without a step into the droop curve. A step in the droop curve exposes the generator to excessive cycling when frequency dithers about the deadband limit. An example of each scenario can be seen in Figure 3.1 (recommended) and Figure 3.2 (not recommended). A more detailed discussion of the two methods (step and no-step) can be found in **Appendix B** of *Dynamic Models for Turbine-Governors in Power System Studies,*[7] which was published by the IEEE PES in January 2013. A larger percent droop value is less responsive to frequency deviations (e.g., a five percent droop is less responsive than a three percent droop).

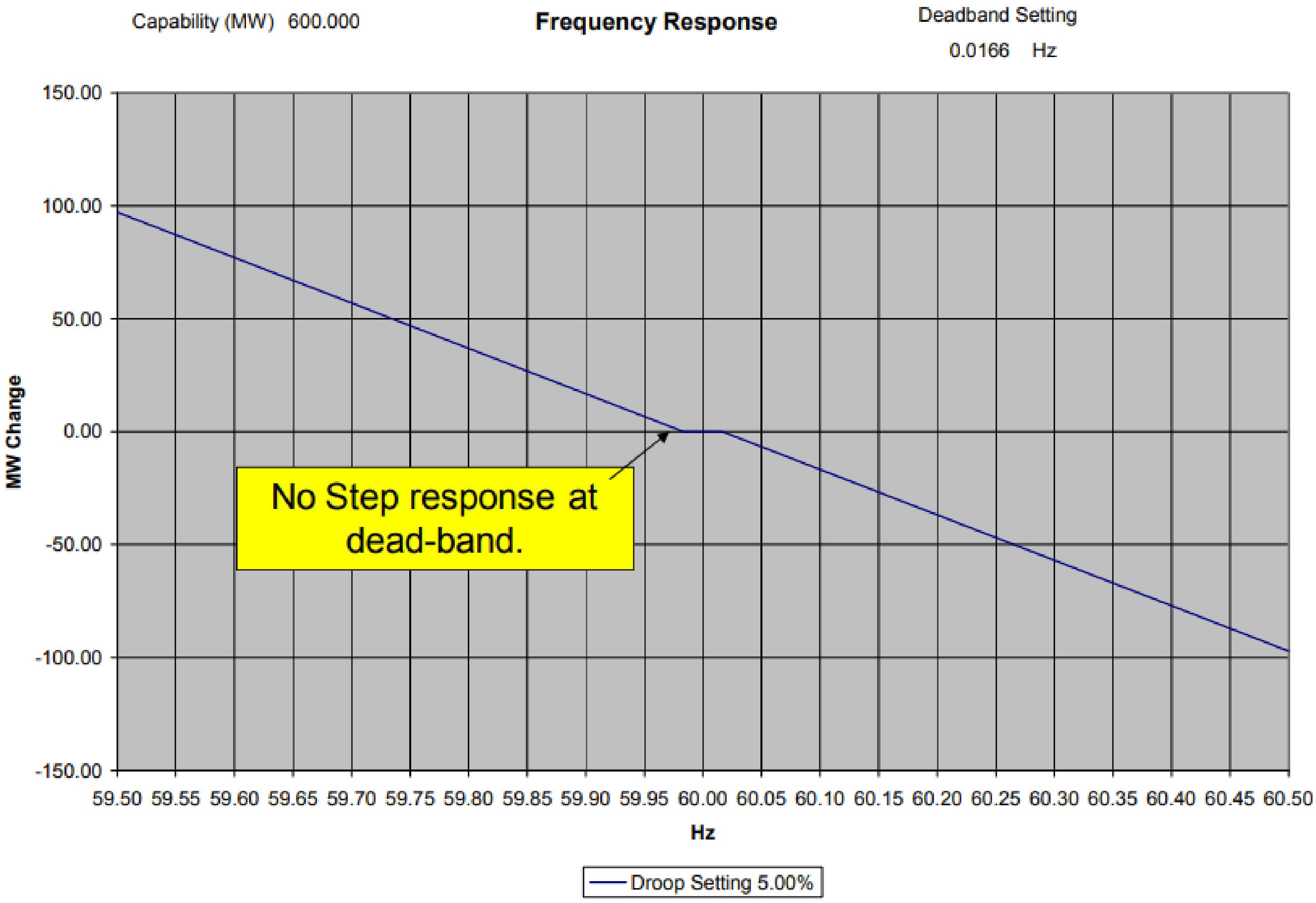


Figure 3.1: Governor Deadband Setting without Step Implementation

Source: NERC Frequency Response Initiative Report 2012[8]

---

[7] http://sites.ieee.org/fw-pes/files/2013/01/PES_TR1.pdf

[8] https://www.nerc.com/docs/pc/FRI_Report_10-30-12_Master_w-appendices.pdf Frequency Response Initiative Report 2012

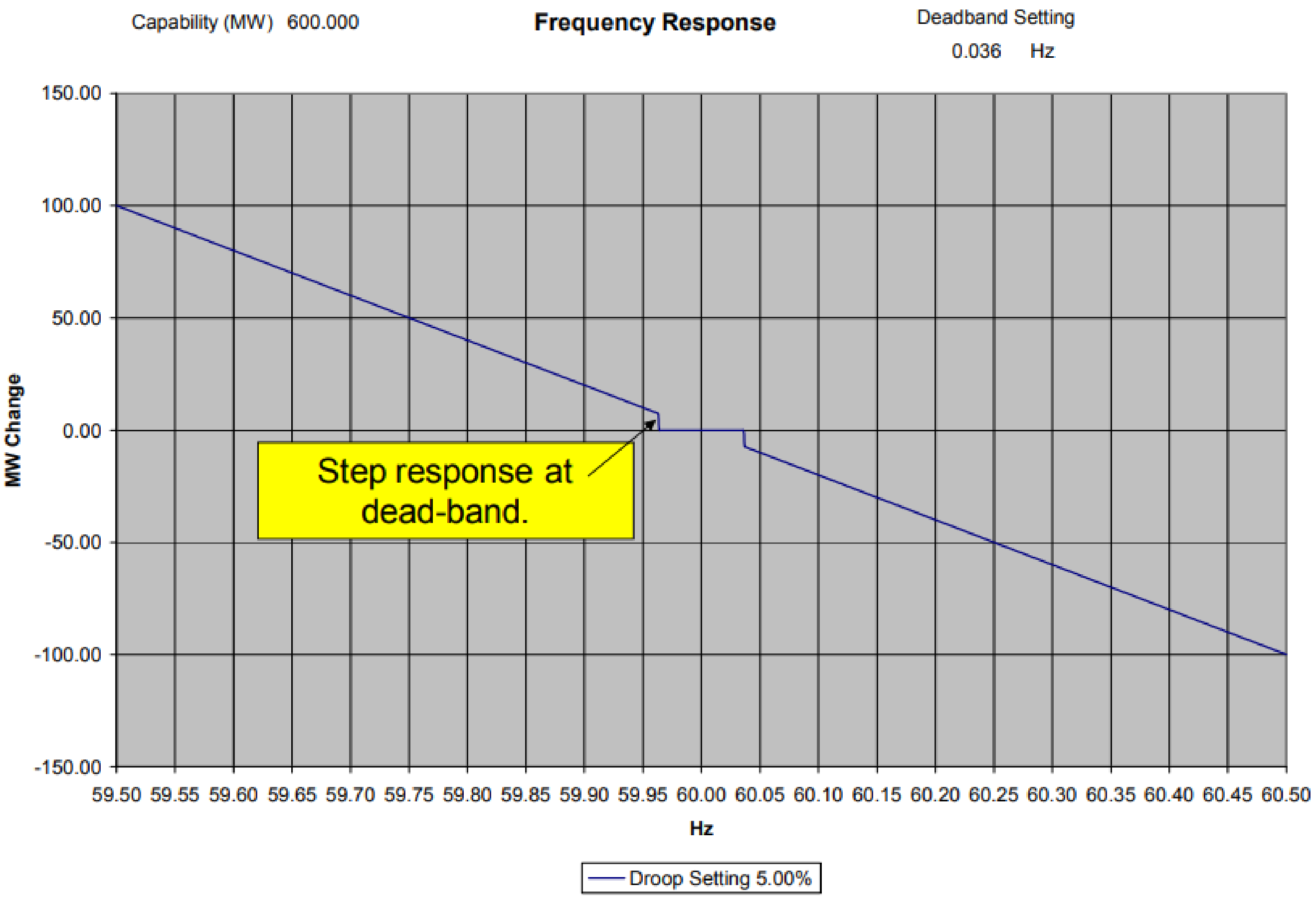


Figure 3.2: Governor Deadband Setting with Step Implementation

Source: NERC Frequency Response Initiative Report 2012

The recommended maximum governor deadband and governor droop settings for each Interconnection are as follows in this section.

Eastern Interconnection

The recommended governor deadband setting should not exceed the value stated in Table 3.1.

Table 3.1: Eastern Interconnection Deadband Settings

Generator Type	Maximum Deadband Setting
All Generating Units	+/- 0.036 Hz

The maximum expected droop performance for the entire combined-cycle facility is six percent. The effective droop of a combined-cycle plant depends on the size of the steam turbine generator in proportion to the sum of the natural gas turbine generators. Many combustion turbines in a combined-cycle configuration have a four percent droop setting. The recommended governor droop settings should not exceed the values in Table 3.2 for each type of generator.

Table 3.2: Eastern Interconnection Droop Settings

Generator Type	Maximum Droop Setting
Combustion Turbine (Combined Cycle)	4%
Steam Turbine (Combined Cycle)	5%

Table 3.2: Eastern Interconnection Droop Settings	
Generator Type	**Maximum Droop Setting**
All Others	5%

ERCOT Interconnection

The required governor deadband setting shall not exceed the values in Table 3.3 from BAL-001-TRE.

Table 3.3: ERCOT Interconnection DeadBand Settings	
Generator Type	**Maximum Dead-Band Setting**
Steam and Hydro Turbines with Mechanical Governors	+/- 0.034 Hz
All Other Generating Units/Generating Facilities	+/- 0.017 Hz

The required governor droop settings shall not exceed the values **in Table 3.4 f**or each respective type of generator from BAL-001-TRE.

Table 3.4: ERCOT Interconnection Droop Settings	
Generator Type	**Maximum Droop Setting**
Hydro	5%
Nuclear	5%
Coal and Lignite	5%
Combustion Turbine (Simple Cycle and Single-Shaft Combined Cycle)	5%
Combustion Turbine (Combined Cycle)	4%
Steam Turbine (Simple Cycle)	5%
Diesel	5%
Wind Powered Generator	5%
DC Tie Providing Ancillary Services	5%
Renewable (Non-Hydro)	5%

Western Interconnection

The recommended governor deadband setting should not exceed the value in Table 3.5.

Table 3.5: Western Interconnection Deadband Settings	
Generator Type	**Maximum Deadband Setting**
All Generating Units	+/- 0.036 Hz

The governor droop settings shall not be less than three percent or greater than five percent. Many combustion turbines have a four percent droop setting. The droop settings should not exceed the values in Table 3.6 for each respective type of generator.

Table 3.6: Western Interconnection Droop Settings	
Generator Type	**Maximum Droop Setting**
Combustion Turbine (Combined Cycle)	4%
Steam Turbine (Combined Cycle)	5%
All Others	5%

Quebec Interconnection

There shall be no intentional governor deadband set on generators within the Quebec Interconnection by local requirement, shown in Table 3.7.

Table 3.7: Quebec Interconnection Deadband Settings

Generator Type	Maximum Deadband Setting
All Generation	N/A

The required governor droop settings shall not exceed five percent for all types (synchronous, inverter based and other technologies) of generation within the Quebec Interconnection by local requirement (see Table 3.8).

Table 3.8: Quebec Interconnection Droop Settings

Generator Type	Maximum Droop Setting
All Generation	5%

Chapter 4: Performance Assessment

Some BAs have developed methods for determining if governors are working properly by reviewing energy management system scan rate data (e.g., every four seconds) stored in their data historians (e.g., OSISoft, PI, AVEVA eDNA). Verification of proper governor function within a BA can be time consuming and requires specific expertise. BAs are strongly encouraged to evaluate the governor's responses being provided within their BA area to an adequate FRR is available in real time. To assist in this effort, methods used successfully by some BA to address this task are presented below and may be used as a starting point for similar efforts of other BAs, GOPs, and GOs.

The ERCOT Interconnection is a single BA Interconnection and has developed metrics to evaluate governor response performance. These metrics are included in the Regional Reliability Standard BAL-001-TRE-1, Attachment 2 "Primary Frequency Response Reference Document." BAL-001-TRE-1 Attachment A, provides performance metric calculations for initial PFR, sustained PFR, and limits on calculation of PFR performance. PFR uses a fixed time interval to determine initial governor response to a frequency event. Sustained PFR also establishes a fixed time interval; this time is used to determine if frequency response is being sustained through the stabilization period. High scores on both metrics indicate that frequency response is being sustained as desired. Low scores on both can indicate that frequency response is not being provided. Problems with outer loop control causing frequency response to be withdrawn (i.e., squelched response) can be indicated by a relatively high score in the initial PFR metric and a lower score in sustained PFR metric.

NERC also uses a similar tool to that of ERCOT, known as the Generator Resource Survey to calculate governor PFR by using historical data or manually calculated values. This tool, which uses the NERC Reliability Standard BAL-001-TRE-1 as a starting framework, evaluates an individual resource's ability to provide PFR during both the initial period and the sustained period. This tool is used for single event and unit evaluation and is intended to be used as a benchmarking tool for an individual resource as well as for the BA. It evaluates resources for their ability to provide PFR much like the BAL-001-TRE-1 except for a few notable differences. Those differences include the lack of consideration of certain aspects of conventional steam turbine operation and natural gas turbine and combined-cycle operation due to lack of data availability to many BAs and GOs. The survey is intended to be a starting point for the evaluation of resources and their ability to provide PFR through both the initial excursion of a frequency event as well as during the arresting/stabilization period during the recovery.

Several NPCC BAs within the NPCC Region have used a graphical approach to determining if generator governor response is being sustained. Two plots of generator output and frequency are reviewed in the evaluation of a generator's response along with some supplemental data. The first plot (starting five minutes before the decline in frequency and ending 15 minutes after the decline in frequency) is used to determine if other factors (e.g., such as unit ramping or AGC control) are occurring, which may invalidate the utility of the sample (i.e., it is not a "controlled" experiment). The second plot (starting one minute before the decline in frequency and ending two minutes after the decline in frequency) is used to determine the type of response observed and to calculate an observed droop if the response is being sustained. The analysis performed is a three-step process: sample validation, response type classification, and droop verification. The process is explained further in **Appendix B**. A fixed time window is not used in the response type classification and droop verification because Eastern Interconnection frequency deviations often persist for longer than one minute, and frequency response should be sustained until the frequency returns to a value within the governor deadband.

Appendix A: Typical Unit Response to Low and High Frequency Events by Unit Type

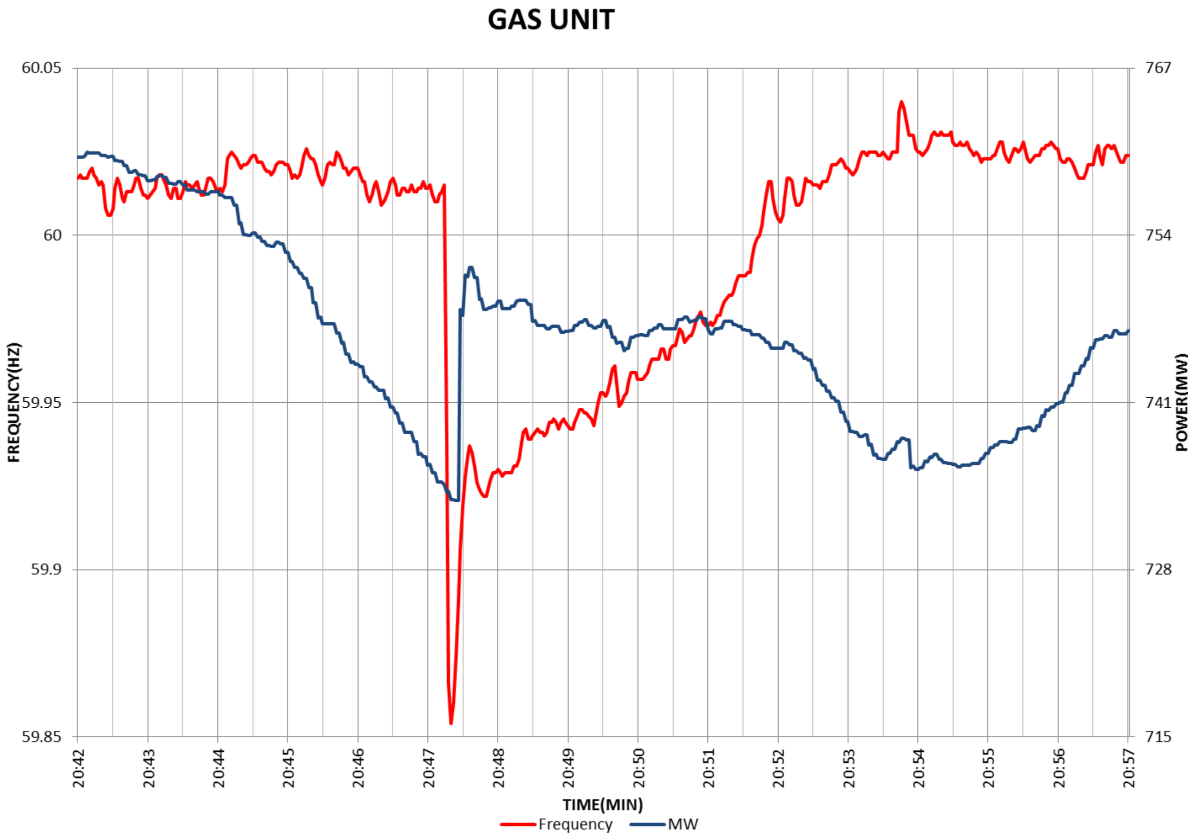


Figure A.1: Gas Unit Responding to Low Frequency Event at 17 mHz Deadband and Five Percent Droop

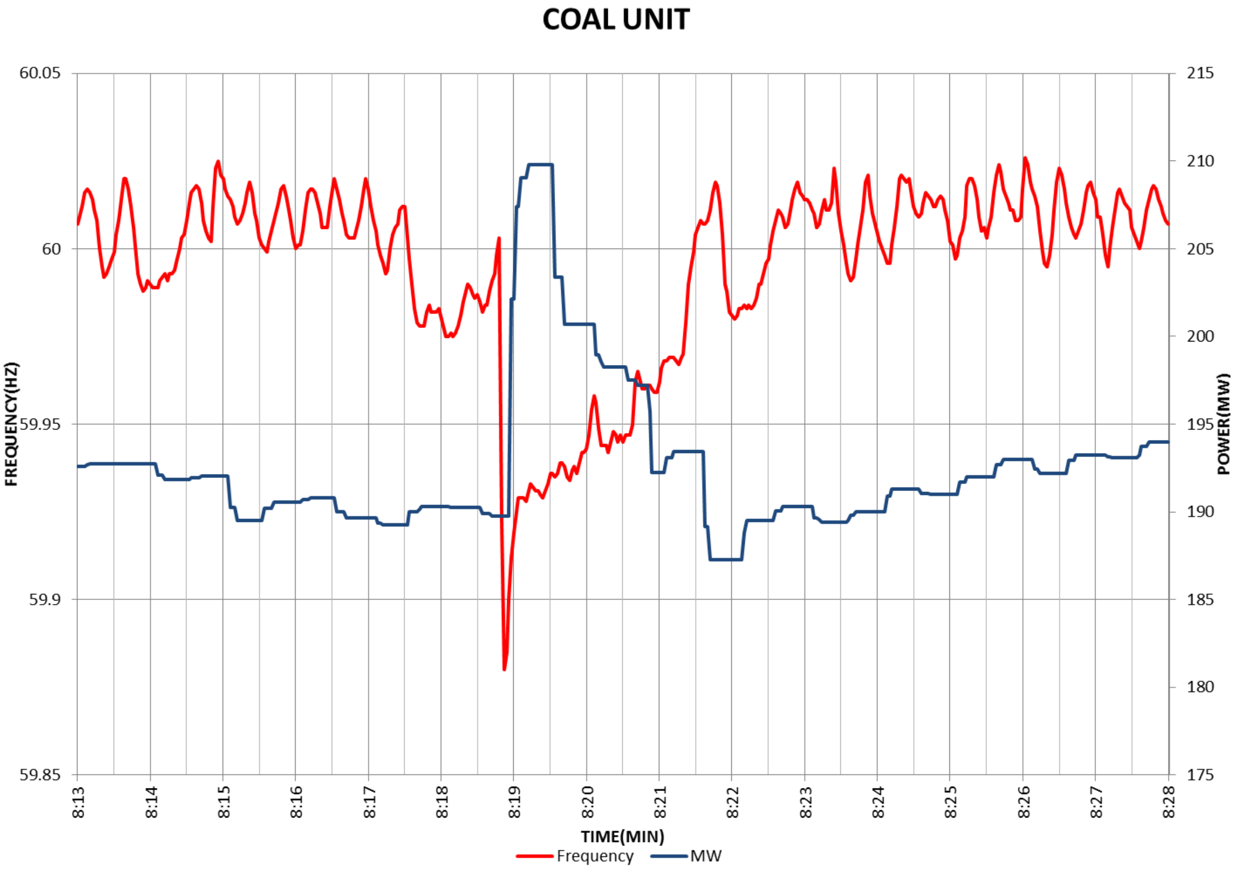


Figure A.2: Coal Unit Responding to Low Frequency Event at 17 mHz Deadband and Five Percent Droop

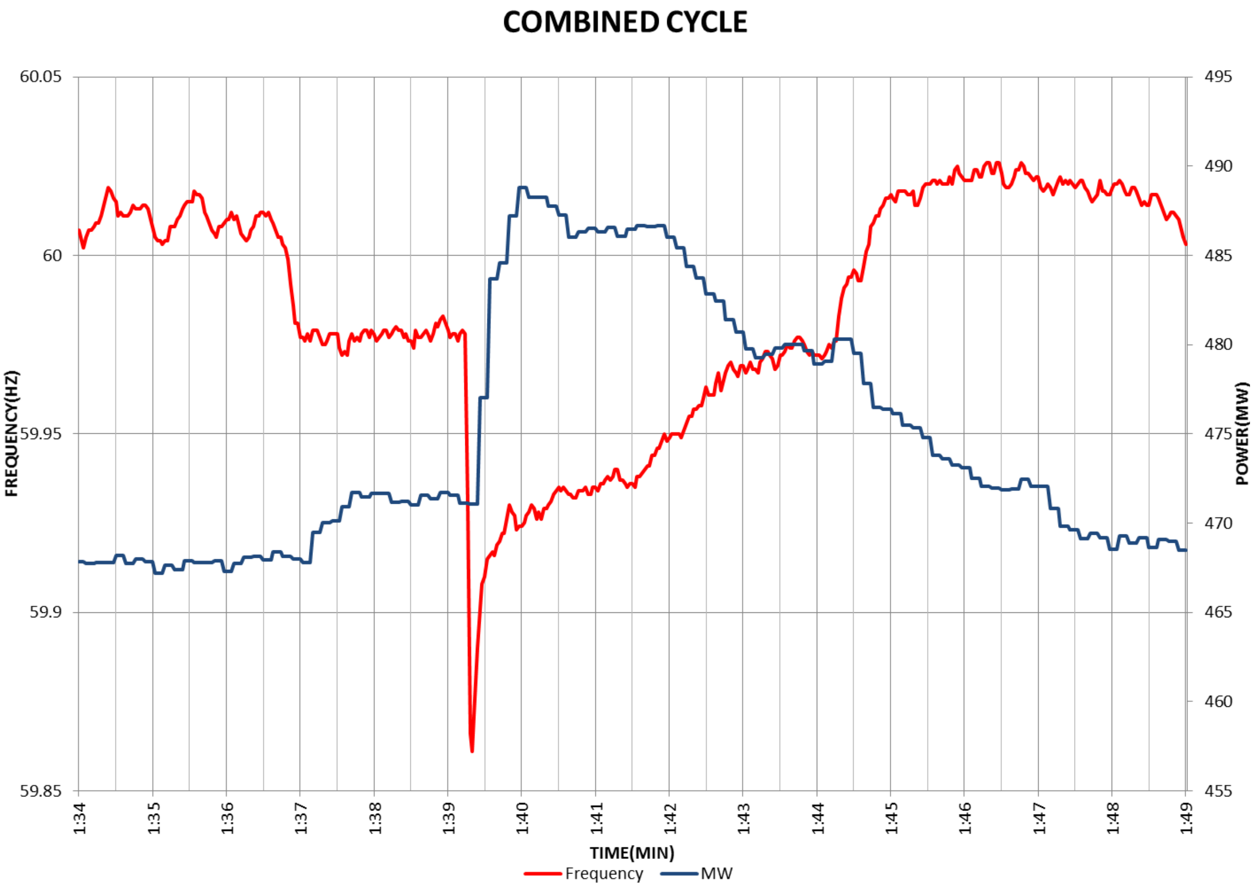


Figure A.3: Combined-Cycle Unit/Block Responding to Low Frequency Event at 17 mHz Deadband

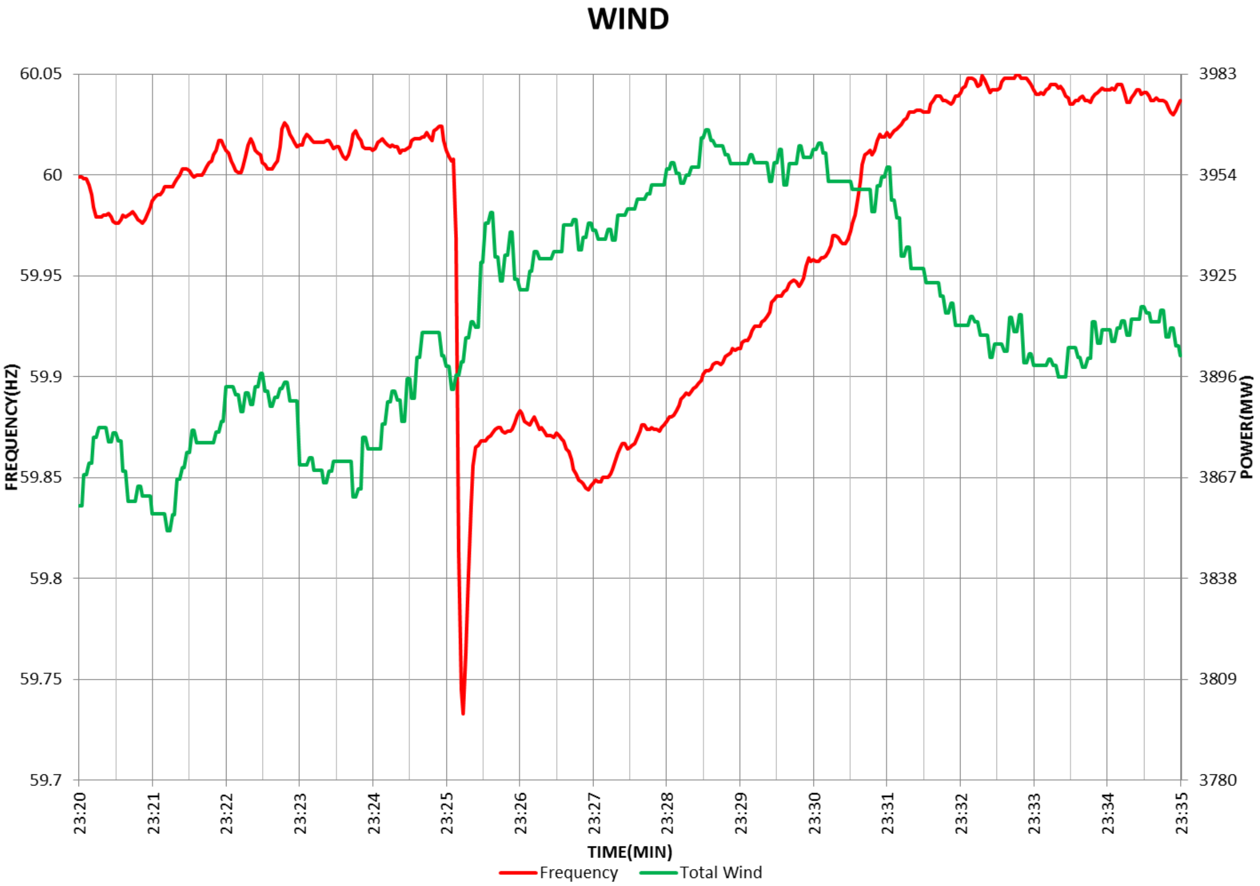


Figure A.4: Wind Resources Responding to Low Frequency Event at 17 mHz Deadband and Five Percent Droop

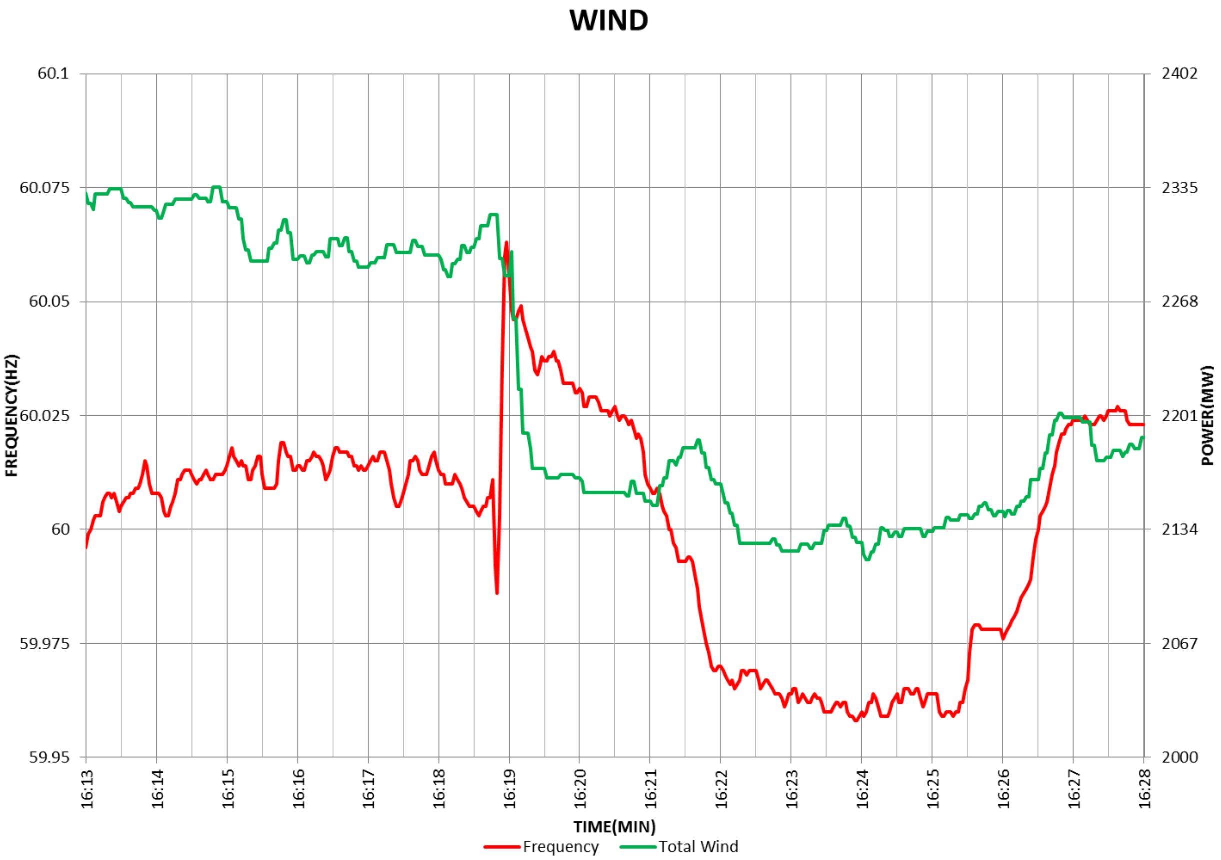


Figure A.5: Wind Resources Responding to High Frequency Event at 17 mHz Deadband and Five Percent Droop

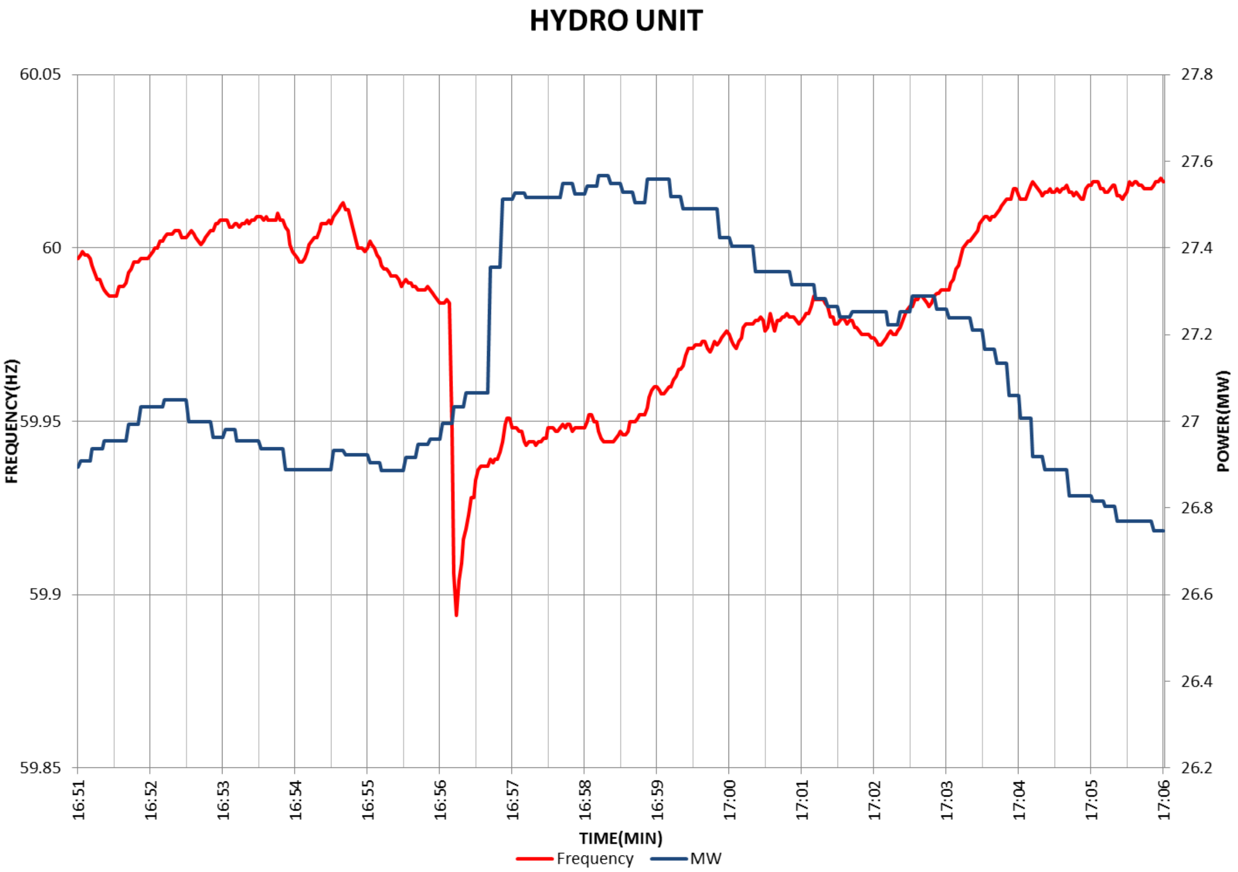


Figure A.6: Hydro Resource Responding to Low Frequency Event at 17 mHz Deadband and Five Percent Droop

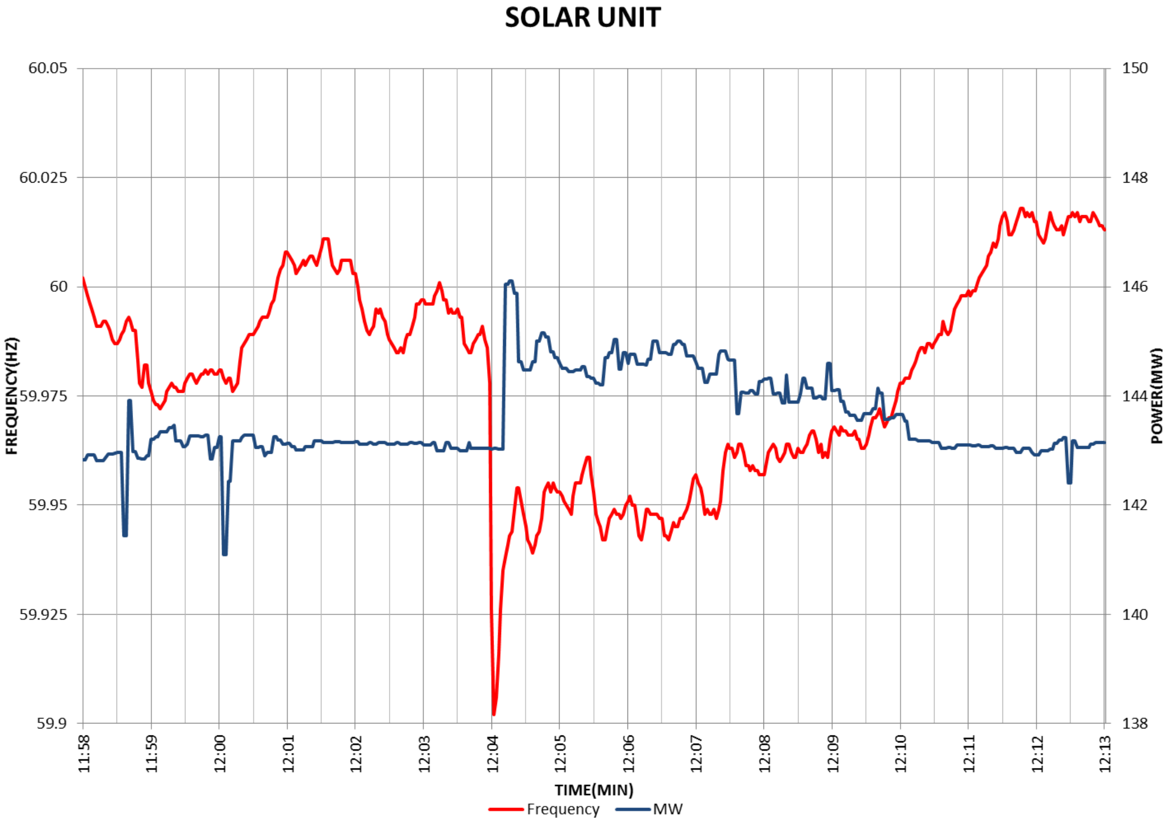


Figure A.7: Solar Resource Responding to Low Frequency Event at 17 mHz Deadband and Five Pecent Droop in ERCOT

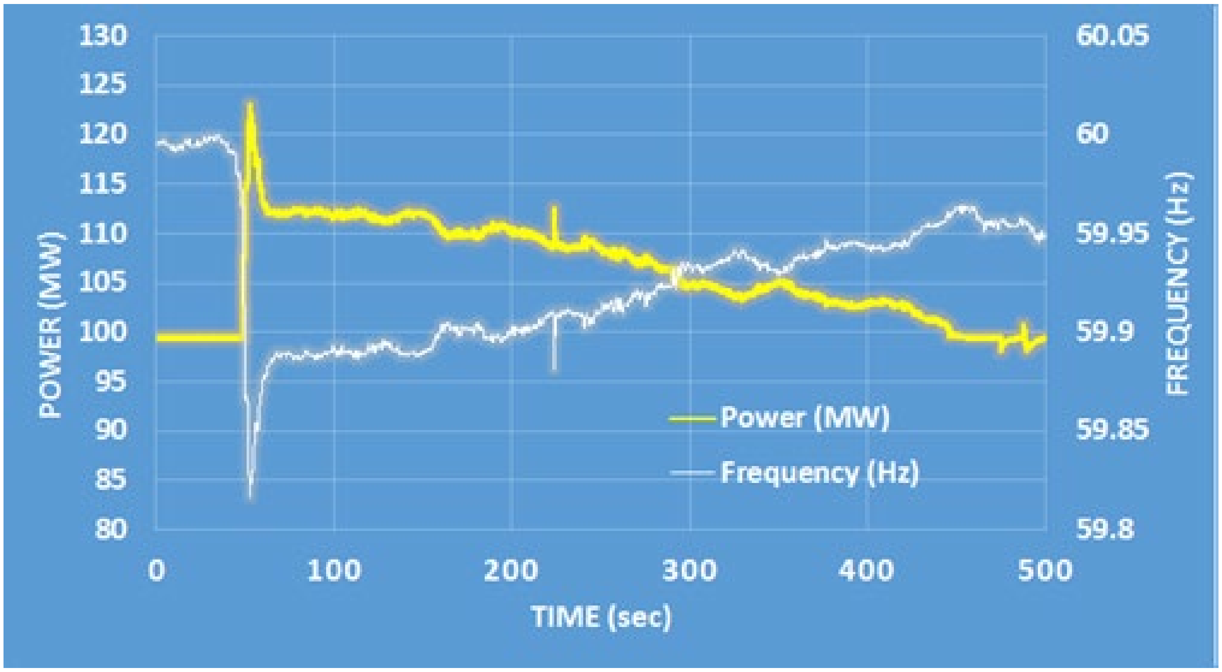


Figure A.8: Solar Resource Responding to Low Frequency Event at 36 mHz Deadband and Three Percent Droop in WECC

Appendix B: Sample Validation, Response Type Classification, and Droop/Deadband Verification

Sample Validation

There are several factors to be considered in determining if a particular declining frequency event can provide useful information about the frequency response of a particular generator. Any one of the following factors can reduce the confidence in or totally invalidate the performance sample:

- Poor signal resolution from the plant historian.
- Historian compression techniques duration and extent of frequency excursion beyond the expected governor deadband limit.
- Oscillatory generator output due to plant control tuning problems.
- Generator is off-line, ramping up or down due to dispatch instructions, or on AGC.
- Output is at or near the generator high limit at the time of the frequency event.
- Insufficient accuracy of the data acquisition system to measure and record the measured parameters.
- Noisy telemetry of the output of the generator.
- Actual high limit's sensitivity to ambient temperature versus a high limit provided based on forecasted temperature.
- Higher levels of output provided by equipment that is not frequency responsive (e.g., duct burners, steam injection).

Response Type Classification

Once a sample for a declining frequency event has been validated, an attempt is made to classify a sample as one of the following types based on a review of the plots of actual generation and frequency:

- Sustained: Output increases after the frequency deviates outside the governor deadband with frequency response that is proportional to the ongoing frequency deviation beyond the governor deadband continuing until the frequency returns to be within the governor deadband.
- Withdrawal/Squelched: Output increases after the frequency deviates outside the frequency deadband, but it decreases significantly in the direction of the output level that existed prior to the decline in frequency even though the frequency continues to be outside the governor deadband.
- No Response: Output is essentially unchanged when the frequency deviates outside the governor dead-band.
- Negative Response: Output declines as the frequency declines, possibly due to thermal limitations or improper configuration of plant controls.

Individual samples are compared to determine an overall response type classification and repeatability among samples is a key factor in this determination. A high degree of confidence in the overall classification can be developed when five to 10 samples exhibit the same response type. However, an overall assessment of squelched response may require a greater number of samples as the relative values of actual generation versus the desired dispatch level and its surrounding megawatt control deadband can result in a mixture of response types among samples. For example, out of 20 samples, six may appear to be sustained, six may appear to be squelched, six may appear to have no response, and two may appear to be negative responses.

Governor Deadband and Droop Verification

For generators classified as having sustained response, the governor deadband and governor droop settings can be verified. An expected output change for a declining frequency event can be computed based on generator size, governor deadband expected governor settings, and the frequency observed when it is relatively stable prior to the event. The computed expected response can be compared with the actual observed change in output. Greater confidence in this verification can be achieved if the mean and median of about ten events are used in the comparison.

If the droop and deadband settings are not known, but there are about 10 samples of sustained response, trial droop and deadband values can be used to estimate an effective droop/deadband pair by matching the mean and median of the observations with those expected for candidate droop/deadband pairs.

The empirical/effective droop settings can vary substantially for some conventional thermal generators based on load levels. For some generators, it may be necessary to compute different effective droop values for different output ranges. The droop rating is applicable to the entire operating range while droop performance can vary depending on the initial load (and its corresponding governor valve position) when a frequency event occurs.

Appendix C: : Definitions and Terminology

Area Control Error (ACE): The instantaneous difference between a Balancing Authority's net actual and scheduled interchange, taking into account the effects of Frequency Bias, correction for meter error, and Automatic Time Error Correction (ATEC) if operating in the ATEC mode. ATEC is only applicable to BAs in the WI.

Arrested Frequency – Value C – Point C – Frequency Nadir: The point of maximum frequency excursion in the first swing of the frequency excursion between time zero (Point A) and time zero plus 20 seconds.

Arresting Period: The period of time from time zero (Point A) to the time of Point C.

Arresting Period Frequency Response: A combination of load damping and the initial Primary Control Response acting together to limit the duration and magnitude of frequency change during the Arresting Period.

Automatic Generation Control (AGC): Equipment that automatically adjusts generation in a Balancing Authority Area from a central location to maintain the BA's interchange schedule plus Frequency Bias. AGC may also accommodate automatic inadvertent payback and time error correction.

Balancing Authority (BA): The responsible entity that integrates resource plans ahead of time, maintains load-interchange-generation balance within a BA Area, and supports interconnection frequency in real time.

Frequency: The rate at which a period waveform repeats itself. Frequency is measured in cycles per second or in hertz (Hz). The symbol is "F."

Frequency Deviation: A difference between the interconnection frequency and the interconnection scheduled frequency.

Frequency Responsive Reserve: The capacity of Governor Response and/or Frequency-Responsive Demand Response that will be deployed for any frequency excursion.

Frequency-Responsive Demand Response: Voluntary load shedding that complements governor response. This load reduction is typically triggered by relays that are activated by frequency.

Headroom: The difference between the current operating point of a generator and its maximum operating capability.

Inertia: The property of an object that resists changes to the motion of an object. For example, the inertia of a rotating object resists changes to the object's speed of rotation. The inertia of a rotating object is a function of its mass, diameter, and speed of rotation.

Load Damping: The damping effect of the load to a change in frequency due to the physical aspects of the load such as the inertia of motors and the physical load to which they are connected.

Plant Secondary Control: Secondary control refers to controls affected through commands to a turbine controller issued by external entities not necessarily working in concert with frequency management objectives. It is common for a modern power plant to have several distinct modes of secondary control implemented within the plant and to be able to accept secondary control inputs from sources external to the plant.

Primary Control Response Withdrawal: The withdrawal of previously delivered Primary Control Response, through plant secondary controls.

Primary Frequency Control: Actions that deliver power to the interconnection in response to a frequency deviation through inertial response generator governor response, load response (typically from motors), demand response (designed to arrest frequency excursions), and other devices that provide an immediate response to frequency based on local (device-level) control systems, without human or remote intervention.

Recovery Period: The period of time from when Secondary Control Response are deployed (typically about zero plus 53 seconds) to the time of the return of frequency to within pre-established ranges of reliable continuous operation.

Settling Frequency: Refers to the third key event during a disturbance when the frequency stabilizes following a frequency excursion. Point B represents the interconnected system frequency at the point immediately after the frequency stabilizes due to governor action but before the contingent control area takes corrective AGC action.

Secondary Frequency Control: Actions provided by an individual BA or its Reserve Sharing Group intended to restore Primary Control Response and restore frequency from the Arrested Frequency back to Scheduled Frequency, or to maintain Scheduled Frequency deployed in the “minutes” time frame. Secondary Control comes from either manual or automated dispatch from a centralized control system. Secondary Control also includes initial reserve deployment for disturbances and maintains the minute-to-minute balance throughout the day and is used to restore frequency to normal following a disturbance and is provided by both spinning and non-spinning reserves.

Tertiary frequency control: Encompasses actions taken to get resources in place to handle current and future changes in load or contingencies. Reserve deployment and Reserve restoration following a disturbance is a common type of Tertiary frequency control.

Appendix D: Related Documents

Frequency Control Requirements for Reliable Interconnection Frequency Response – Lawrence Berkeley National Laboratory

FERC Order 842

Reliability Guideline: Operating Reserve Management – Version 23

Demonstration of Essential Reliability Services by a 300-MW Solar Photovoltaic Power Plant

Advanced Grid-Friendly Controls Demonstration Project for Utility-Scale PV Power Plants

NERC Inverter-Based Resource Performance Task Force Fast Frequency Response Concepts and Bulk Power System Reliability Needs White Paper

IEEE PES Appendix B of "Dynamic Models for Turbine-Governors in Power System Studies"

Frequency Response Initiative Report 2012

NERC Alert A-2015-02-05-01

BAL-001-TRE-1 Attachment A

Using Renewables to Operate a low-carbon Grid: Demonstration of Advanced Reliability Services from a Utility-Scale Solar PV Plant

PRC-001-WECC-CRT-2

Contributors

NERC gratefully acknowledges the contributions and assistance of the following industry experts in the preparation of this guideline.

Name	
Troy Blalock	Dominion Energy South Carolina
Nitika Mago	ERCOT
Greg Park	Northwest Power Pool
Sam Rugel	Tucson Electric Power Company
William Shultz	Southern Company Generation/ NAGF member
Terry Bilke	
Darrel Richardson	North American Electric Reliability Corporation
Levetra Pitts	North American Electric Reliability Corporation

Guideline Information and Revision History

Guideline Information	
Category/Topic: Primary Frequency	**Reliability Guideline/Security Guideline/Hybrid:** Primary Frequency Control
Identification Number: [NERC use only]	**Subgroup:** NERC Resource Subcommittee

Revision History		
Version	**Comments**	**Approval Date**
1.0	Initial Version – *Reliability Guideline: Primary Frequency Response*	12/15/2015
2.0	Updated Document to include additional guidance for Primary Frequency Response	9/19/2018
3.0	Update document to include additional guidance for Primary Frequency Response	5/1/2019
4.0	Updated document to include references to IBRTF, added metrics and formatted to new guideline	

Metrics

Pursuant to the Commission's Order on January 19, 2021, *North American Electric Reliability Corporation*, 174 FERC ¶ 61,030 (2021), reliability guidelines shall now include metrics to support evaluation during triennial review consistent with the RSTC Charter.

Baseline Metrics

All NERC reliability guidelines include the following baseline metrics:

- BPS performance prior to and after a reliability guideline as reflected in NERC's State of Reliability Report and Long Term Reliability Assessments (e.g., Long Term Reliability Assessment and seasonal assessments).
- Use and effectiveness of a reliability guideline as reported by industry via survey.
- Industry assessment of the extent to which a reliability guideline is addressing risk as reported via survey.

Specific Metrics

The RSTC or any of its subcommittees can modify and propose metrics specific to the guideline in order to measure and evaluate its effectiveness, listed as follows:

- NERC M-4 Interconnection Frequency Response.
- NERC BAL- 003 compliance by BA or FRSG.

Effectiveness Survey

On January 19, 2021, FERC accepted the NERC proposed approach for evaluating Reliability Guidelines. This evaluation process takes place under the leadership of the RSTC and includes:

- industry survey on effectiveness of Reliability Guidelines;
- triennial review with a recommendation to NERC on the effectiveness of a Reliability Guideline and/or whether risks warrant additional measures; and
- NERC's determination whether additional action might be appropriate to address potential risks to reliability in light of the RSTC's recommendation and all other data within NERC's possession pertaining to the relevant issue.

Privacy and Security Impacts of DER and DER Aggregators: Joint SPIDERWG/SITES White Paper

Action

Approve

Background

The Federal Energy Regulatory Commission (FERC) approved Order No. 2222, which enabled Distributed Energy Resources (DERs) to participate in wholesale electric markets[1] through a Distributed Energy Resource Aggregator (DER Aggregator) that interfaces with the Independent System Operators (ISOs) and Regional Transmission Operators (RTOs). These ISO/RTOs are generally registered as the Balancing Authorities (BAs) and Reliability Coordinators (RCs) in their respective Interconnections. The NERC System Planning Impacts from DER Working Group (SPIDERWG) and the Security Integration and Enablement Subcommittee (SITES) have both authored white papers[2] analyzing the bulk system reliability and security implications of the DER Aggregator; however, no NERC industry stakeholder group has explored the technical aspects of security controls for these grid functions and their systems. This paper focuses solely on the security controls available to DER and DER Aggregators and provides recommendations[3] in order to maintain the reliability of the bulk power system (BPS).

This white paper has gone for RSTC review and is seeking approval based on the revisions to the RSTC comments and additional team member enhancements to the paper.

Summary

This paper explores the technical facets of security controls available to DER and DER Aggregators and provide an example of potential attacks that can be mitigated through the implementation of those security controls. It will also provide an overview on the security posture of distribution landscape (particularly for DER and DER Aggregators) and provide correlations to NERC Standards, should any exist. The Bulk Electric System (BES) Cyber Asset 15-minute impact test is compared to DER and DER Aggregators to understand their potential impact to the BPS. Further, privacy concerns are covered related to confidentiality of user data for DER owners in this electrical system as such data may be the target of a malicious actor. This paper will also provide high-level recommendations to DER and/or DER Aggregators on security controls or other risk mitigation measures.

---

[1] FERC Order 2222 is available here: https://www.ferc.gov/sites/default/files/2020-09/E-1_0.pdf

[2] The SPIDERWG white paper *BPS Reliability Perspectives for Distributed Energy Resource Aggregators* is available at https://www.nerc.com/comm/RSTC_Reliability_Guidelines/SPIDERWG_White_Paper_-_BPS_Persepectives_on_DER_Aggregator_docx.pdf and the SITES white paper *Cyber Security for Distributed Energy Resources and DER Aggregators* is available at https://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_Cybersecurity_for%20DERs_and_DER_Aggregators.pdf .

[3] This paper does not provide Compliance Implementation Guidance related to the CIP standards. Rather, security controls are presented at a high level and the functional interplay between DER, DER Aggregators, and other entities is considered in the context of security and security controls.

SAR	Reporting of Aggregate loss of DER during Grid Disturbances in EOP-004
Instructions	**Please use this form to submit comments on the SAR. Comments must be submitted within the review period below to NERC (John.Skeath@nerc.net) with the words "SAR Reporting of Aggregate loss of DER during Grid Disturbances in EOP-004" in the subject line. Only comments submitted in this Microsoft Excel format will be accepted. Both general and specific comments should be provided within this form. Red-line document changes, PDF versions of this document, or email comments will NOT be accepted.** Comments may be submitted by individuals or organizations. Please provide the requested information in Row 6. If comments are submitted on behalf of multiple organizations, list all organizations in Row 6. Please provide the Industry Segment and Region (if applicable) in Rows 7 and 8 and provide the requested contact information in Rows 9 and 10. If you have any questions regarding this process, please contact John Skeath (John.Skeath@nerc.net)
Review Period	Jun 15, 2023 – July 15, 2023

Organization(s)	**Page #**	**Line / Paragraph**	**Comment**	**Proposed Change**	**NERC Response**
Oncor Electric			NERC and the stakeholder community should focus efforts on the development of a Reliability Guideline before jumping to the development of additional mandatory reliability standards and/or requirements in EOP-004. The SPIDER WGNERC Reliability Standards Review clearly acknowledges that the guideline document is needed to address detection and calculation of aggregate DER losses to support accurate reporting.		Thank you for your comment. As the comment identifies, the cited paper in the SAR identifies both Standards revisions and Reliability Guideline as an outcome of the review. The proposed SAR is a result of the identified standards gap and the Reliabiltiy Guildeline is to identify accuracy enhancements to aggregate DER performance during large grid disturbances. The Reliability Guideline is not suited to fill the gap of a notice to the ERO for the treatment of DER in the forms. No change made to SAR.
Georgia Transmission Corporation	N/A	N/A	GTC is of the opinion that a reliability guideline should be created on this topic prior to the submission of a SAR that will give industry opportunity to better understand and agree to the issue being presented in the SAR and to evaluate/modify current processes prior to a reliability standard being modified. The referenced whitepaper actually recommends a reliability guideline.	The SAR should be rescinded and efforts should be focused on the development of a Reliability Guideline to identify where industry guidance is needed.	Thank you for your comment. As the comment identifies, the cited paper in the SAR identifies Reliability Guideline as an outcome of the review. Such Reliabiltiy Guildeline is to identify accuracy enhancements to aggregate DER performance during large grid disturbances. The Reliability Guideline is not suited to fill the gap of a notice to the ERO for the treatment of DER in the forms. The SPIDERWG does not seek to identify further guidance in the already identified need for guidance on accuracy enhancements and methods available to Registered Entities outside of their findings in the white paper cited.
Georgia Transmission Corporation	1	12	The referenced disturbance event occurred in the United Kingdom which is not mandated by NERC Reliability Standards. Any disturbance event used within a NERC SAR should have taken place within North America such that BES requirements are well understood.	Delete United Kingdom event and add reference to an applicable event within North America.	Thank you for your comment. Added text to fulfill part of the proposed change. No deletions made.
Georgia Transmission Corporation	1	12	The referenced disturbance event included tripping of other BES generation resources and the event was not solely attributed to the tripping of aggregated DER. It is unclear why an event category is needed solely for the loss of aggregate DER when documented events are not solely attributed to the loss of aggregated DER.	Clarity is needed on if any event should be reported solely due to the loss of aggregate DER using existing categories in EOP-004-4.	Thank you for your comment. Clarity edits made in the SAR to identify that in the events cited the DER participated as part of the entire generation set is the focus.
Georgia Transmission Corporation	2	16	Part of the SAR scope states, "The standard drafting team should also define a threshold for reporting of events where the loss of aggregate DER exceed such threshold." Does the SPIDERWG have a suggested threshold and/or a basis for this threshold?	The SAR should be rescinded and efforts should be focused on the development of a Reliability Guideline to identify how a threshold should be established for aggregate DER.	Thank you for your comment. As all standard language revisions, including propsed drafting, is best suited for a Standard Drafting Team. The SPIDERWG highlights the gap that such a threshold should be established, but does not wish to tie the revisions to a single or tiered threshold scoped inherently in the scoping of a future standard revision.

Georgia Transmission Corporation	3	20	The SAR states that additional metering is unlikely to be needed, however, this statement assumes that net load is acceptable and that the SDT is allowed to use this input. If additional metering is determined by the SDT, then the costs would be significant and an additional meter would be required for every DER installation with appropriate aggregation software to manage.	The SAR should identify that net load is the input to be utilized for reporting as the alternative to add a meter for every DER installation is not feasible.	Thank you for your comment. The SAR text already states that "net loading quantities currently tracked by the BAs, RCs, and TOPs to run their Operational Planning Statements, Real-Time Assessments, and real-time monitoring of their area are able to track loss of aggregate DER". The SDT should ensure and confirm that the chosen threshold is technically feasible for the current infrastructure cited in the SAR.
Georgia Transmission Corporation	4	30	The SAR does not consider alternatives due to the SPIDERWG's opinion that there are no sufficient alternatives. The section should be revised to clarify why other alternatives are not sufficient, and to provide justification on the risk and why the SAR is the best alternative. Furthermore, the referenced whitepaper recommends creation of a reliability guideline to address how to (do the very thing that this SAR wants to require) accurately detect and calculate aggregate DER losses. Will the guideline be completed before the SDT is convened?	The section should be revised to clarify why other alternatives are not sufficient, and to provide justification on the risk and why the SAR is the best alternative.	Thank you for your comment. The alternatives section has been revised based on this comment.
Edison Electric Institute	N/A	N/A	General Comment: EEI appreciates the opportunity to provide comments on this Draft SAR. While we support NERC efforts to be proactive in addressing emerging BES/BPS Reliability issues, we do not support this SAR at this time. The industry is currently engaged in the development of modifications to EOP-004 to address event reporting for Inverter Based Resources (IBRs) through Project 2023-01 (EOP-004 IBR Event Reporting). However, event reporting of aggregated DERs is a significantly more difficult task to accomplish given the lack of needed data and monitoring tools. We further note that much of the event data needed to assess and report the aggregated loss of DERs is largely unavailable to DPs, residing largely with the DER owners. Complicating compliance further is that event reporting is required within 24 hours of recognition of an event type, which would be an insurmountable obligation to place on Balancing Authorities (BAs), Reliability Coordinators (RC) and Distribution Providers (DPs) because we are unaware of any of these entities have real-time monitoring of DER resources. There are technical and regulatory challenges that need to be overcome first. (e.g., DP adoption of DER Management Systems (DERMs), integration of DERMs with SCADA systems) While these systems and solutions will be deployed over time, the industry is not at that point yet. We also note that until DER resources are registered with NERC similar to other resources, and have regulatory obligations similar to other registered resources, entities such as BAs, RCs and DPs may not be able to get the needed data to support Event Reporting as envisioned within this SAR.	EEI does not support moving this SAR forward because the industry does not have the tools or the ability to accurately capture aggregated DER data in a timely manner. While these technical challenges will in time be overcome, we are not at this point today. For these reasons, we ask that this SAR not be approved.	Thank you for your comment. The SAR text states that "net loading quantities currently tracked by the BAs, RCs, and TOPs to run their Operational Planning Statements, Real-Time Assessments, and real-time monitoring of their area are able to track loss of aggregate DER". In addition, the SPIDERWG agrees that the cited Project 2023-05 to address bulk connected IBRs is dissimilar in magnitude and identified gap. The SPIDERWG also identifies that EOP-004 reports are not the entirety of data submissions or analysis in these large disturbances and serve the purpose of noting broad characteristics of an event. Clarity edits made in the SAR to reflect intended flow monitoring of current infrasturcture.

Southern Company Services, Inc.	3	13,17,18, 23, 24	The technical reliability need, and addition of DER aggregator notifications to the EOP-004 standard, as proposed in the SAR is premature for the following reasons: 1) The EOP-004 standard already has proven reliability-driven notification requirements that would allow the event analysis process to dig into whether unexpected aggregated DER tripping was a contributing factor. Specifically, each of the following reliability conditions in EOP-004 could be triggered, in part, if significant DER aggregation were to trip unexpectedly and help assess if this is a reliability need that requires further monitoring and standards. Important to note that the UK example referenced for technical jusitification of the proposed SAR would have similarly triggered EOP-004 criteria and been made available for reporting, analysis, and review. oPublic appeal for load reduction oSystem-wide voltage reduction resulting from a BES Emergency oFirm Load shedding resulting from a BES emergency oBES Emergency resulting in voltage deviation on a Facility oUncontrolled loss of firm load resulting from a BES Emergency oSystem separation 2) The unexpected tripping of DER aggregation is not known to be a reliability issue in the United States to date. The aforemention existing EOP-004 criteria would enable proven reliaibility focus areas to assess whether	If the standard moves forward, it should not be appliable to the BA, RC or TOP and be solely applicable to the DPs. In addition, the 24hr requirement should either not be included or extended due to the complexity of gathering the required information.	Thank you for your comment. The SAR scopes the SDT to determine the applicable entity for reporting of aggregate DER loss during grid disturbances. As the comment indicates, multiple criteria can be selected for EOP-004 forms and revisions to SAR were made to allow the SDT flexibility to determine if aggregate DER loss should be a separate Event Type or as part of existing Event Type thresholds. SAR edits made to reflect the intent of monitoring T-D interfaces as indicated in the newly added Disturbnace report in the need section. Further, EOP-004 has language stating "Under certain adverse conditions (e.g. severe weather, multiple events) it may not be possible to report the damage caused by an event and issue a written event report within the timing in the standard. In such cases, the affected Responsible Entity shall notify parties per Requirement R2 and provide as much information as is available at the time of the notification."
Southern Company Services, Inc.	2	12	Need clarity on the usage of term DER for applicability of the standard.	Please provide the necessary clarity in the document.	Added link to SPIDERWG's terms and referenced the work in Project 2022-02 to reflect their definition of "DER".
Arizona Public Service - Marcus Bortman	n/a	n/a	AZPS agrees with EEI's comments no supporting this SAR at this time. The technical and regulatory challenges that need to be overcome prevent the addition of Aggregate DER loss reporting at this time.		Thank you for your comment. Please see response to EEI's comments for this comment's response.
Southern Indiana Gas and Electric Company d/b/a CenterPoint Energy Indiana South (SIGE)	2	Line/Paragraph 16	It is difficult to comment on the SAR at this time. SIGE the SDT define the responsible entity for reporting. Depending on who is responsible for reporting there may be substantial financial impacts for the collection of reporting data required.		Thank you for your comment. As indicated in the SAR, the current net loading values used in BAs, RCs, and TOPs can be used to attribute DER tripping during events. The comment correctly identifies that advanced metering to collect data has a cost. The SAR identifies that such advanced metering is not required.
ITC Holdings			General Comment: ITC agrees with EEI and NSRF's comments and rationale for recommending not moving forward with this SAR at this time.		Thank you for your comment. Please see response to EEI's comments and NSRF's comments for this comment's response.
Minnesota Power			Minnesota Power supports all of MRO's NERC Standards Review Forum's (NSRF) comments.		Thank you for your comment. Please see response to NSRF's comments for this comment's response.
Southwest Power Pool (SPP)			SPP can support the general concept that there is a need to report large abnormal DER resource losses. However, we are concerned on how the parameters (thresholds) will be determined for the standard from a DER perspective. We recommend that the DER drafting team coordinates with the IBR drafting team to ensure all avenues have been explored and have consistency across the board for both resources via the EOP-004 Standard.	Coordinate with the IBR drafting team in reference to parameters (thresholds).	Thank you for your comment. Clarity edits in the related standards or SARs to identify such coordination in the Standard Committee exists.

Southwest Power Pool (SPP)			SPP has a concern about the time constraints (real-time) associated with EOP-004 (Event Reporting - DERs). We understand that the data is important to the Event Analysis process. However, we don't see any value to reporting the data loss in real-time instead of a monthly or quarterly basis when it comes to reliability of the grid.	Conduct the Event Reporting on a monthly or quarterly basis instead of real-time.	Thank you for your comment. Added disturbance report indicating the participation of DERs during grid distrubances to identify the value reporting brings. Further, EOP-004-4 states that "under certain adverse conditions it may not be possible to report the damge caused by an event and issue a written event report within the timing in the standard. In such cases, the affected Responsible entity shall notify parties per Requirement R2 and provide as much information as is available at the time of the notification." Clarity edits made to Scope section of SAR
WEC Energy Group (Kane, Christine; Beilfuss, Matthew; Zellmer, Clarice; Boeshaar, David)			WEC Energy Group supports the comments submitted by EEI which state: "EEI appreciates the opportunity to provide comments on this Draft SAR. While we support NERC efforts to be proactive in addressing emerging BES/BPS Reliability issues, we do not support this SAR at this time. The industry is currently engaged in the development of modifications to EOP-004 to address event reporting for Inverter Based Resources (IBRs) through Project 2023-01 (EOP-004 IBR Event Reporting). However, event reporting of aggregated DERs is a significantly more difficult task to accomplish given the lack of needed data and monitoring tools. We further note that much of the event data needed to assess and report the aggregated loss of DERs is largely unavailable to DPs, residing largely with the DER owners. Complicating compliance further is that event reporting is required within 24 hours of recognition of an event type, which would be an insurmountable obligation to place on Balancing Authorities (BAs), Reliability Coordinators (RC) and Distribution Providers (DPs) because we are unaware of any of these entities have real-time monitoring of DER resources. There are technical and regulatory challenges that need to be overcome first. (e.g., DP adoption of DER Management Systems (DERMs), integration of DERMs with SCADA systems) While these systems and solutions will be deployed over time, the industry is not at that point yet. We also note that until DER resources are registered with NERC similar to other resources, and have regulatory obligations similar to other registered resources, entities such as BAs, RCs and DPs may not		Thank you for your comment. Please see response to EEI's comments for this comment's response.
WEC Energy Group (Kane, Christine; Beilfuss, Matthew; Zellmer, Clarice; Boeshaar, David)	1-6	Overarching comment	WEC Energy Group also supports the comments of the ISO/RTO Council and the MRO NSRF which state: "...agrees there is an Industry Need to be aware of large scale disturbances that result from the unexpected loss of DERs, this can be better accomplished under the scope of the existing project for reporting of IBR generation losses (Project 2023-01: EOP-004 IBR Event Reporting). This is because events that cause DERs to trip will likely cause IBRs to trip as well. Rather than expand the scope of EOP-004 to require the reporting of DER related disturbance events, NERC's Event Analysis process should be expanded to inquire about DER trips following the receipt of an EOP-004 report for a qualified "Loss of IBR" event. This is preferable to creating a separate EOP-004 reporting requirement for a "Loss of DERs" event."	Retire the DER SAR in its entirety. Expand NERC's Event Analysis process to inquire about "Loss of DERs" following the receipt of an EOP-004 report for a qualified "Loss of IBRs" event.	Thank you for your comment. Please see response to NSRF's comments and the ISO/RTO Council's comments for this comment's response.

WEC Energy Group (Kane, Christine; Beilfuss, Matthew; Zellmer, Clarice; Boeshaar, David)	2	12	WEC Energy Group also supports the comments of the ISO/RTO Council and the MRO NSRF which state: "The SAR seeks to require "reporting by Balancing Authorities (BAs) and Reliability Coordinators (RC) of the loss of aggregate DERs to NERC." NERC Standards collectively require what was the Control Area (now the BA and TOP) to know the status of each Transmission and Generation element within their footprint. This requirement is met by monitoring BES-connected Transmission and Generation via ICCP/SCADA. Load is calculated indirectly by measuring all generation and interchange (import/export) in the Balancing Authority Area. Neither BAs nor RCs have direct visibility into DER operation or the ability to distinguish the impact of "Loss of DERs" on load."	Retire the DER SAR in its entirety. Expand NERC's Event Analysis process to inquire about "Loss of DERs" following the receipt of an EOP-004 report for a qualified "Loss of IBRs" event from the appropriate NERC functional entities that have visibility into DER operations.	Thank you for your comment. Please see response to NSRF's comments and the ISO/RTO Council's comments for this comment's response.
WEC Energy Group (Kane, Christine; Beilfuss, Matthew; Zellmer, Clarice; Boeshaar, David)	2	16	WEC Energy Group also supports the comments of the ISO/RTO Council and the MRO NSRF which state: "The SAR recommends the SDT "clarify how loss of aggregate DER and loss of firm load are accounted so they are not canceled by netting the two." Given the sheer number of telemetry data points going into a BAs indirect calculation of load, it is not unusual to have several instances of sudden load spikes, in either direction, per day due to momentary bad telemetry. EOP-004 is a 24 hour reporting requirement that is well suited for monitoring and reporting variables that are directly measured by ICCP/SCADA such as aggregate BES connected IBR resources. It is not well suited for reporting variables that are estimated by measuring thousands of data points, which each can cause a spike if the data point goes bad. It is not unusual for larger BAs to experience multiple spikes in a day, each amounting to several hundred MWs or more."	Retire the DER SAR in its entirety. Expand NERC's Event Analysis process to inquire about "Loss of DERs" following the receipt of an EOP-004 report for a qualified "Loss of IBRs" event from the appropriate NERC functional entities that have visibility into DER operations.	Thank you for your comment. Please see response to NSRF's comments and the ISO/RTO Council's comments for this comment's response.
David Jacobson			I don't believe that we've had an event in North America where only a large amount of DER tripped. If any DER tripped, it would have been in addition to other tripped elements such as IBR on the BES. I believe it is too soon to make the proposed changes in the standard in this SAR.	As an initial change to the EOP-004 standard, perhaps it is fair for BAs and RCs to investigate whether any DER tripped during a large disturbance that is already being reported.	Thank you for your comment. The SPIDERWG indends that for the near-term, such a solution is the most likely to clarify DER participation during grid disturbances, rather than DER initiated grid disturbances. As the comment indicates, most grid disturbances contain more than one category that can be checked in the EOP-004 standard. Clarity edits made to capture this in the detailed scope section.
David Jacobson			Documenting the change in power level at the T-D interface point (assuming a radial connection) during a large disturbance could be manageable, given that the majority of DER right now is not monitored.	An increase or change in power above a threshold amount at each T-D interface point, like 5 MW (TBD), could be noted as potential DER loss. This check should only be done in conjunction with other large disturbance investigations.	Thank you for your comment. As the SAR is scoping out the required changes to the identified gap, text added to allow the SDT to consider wide area versus local (T-D Interface) applicability as part of the first scoped part. The SDT should ensure and confirm that the chosen threshold is technically feasible for the current infrastructure in the SAR.
David Jacobson			DER aggregators could also be tasked with reporting large DER loss.	Consider adding DER aggregators.	Thank you for your comment. As DER aggregators are not registered entities, no changes made to the SAR on this comment. The SPIDERWG agrees with the comment intent however.

Ann Carey-FirstEnergy	N/A	N/A	FirstEnergy supports EEI's comments, which state: EEI appreciates the opportunity to provide comments on this Draft SAR. While we support NERC efforts to be proactive in addressing emerging BES/BPS Reliability issues, we do not support this SAR at this time. The industry is currently engaged in the development of modifications to EOP-004 to address event reporting for Inverter Based Resources (IBRs) through Project 2023-01 (EOP-004 IBR Event Reporting). However, event reporting of aggregated DERs is a significantly more difficult task to accomplish given the lack of needed data and monitoring tools. We further note that much of the event data needed to assess and report the aggregated loss of DERs is largely unavailable to DPs, residing largely with the DER owners. Complicating compliance further is that event reporting is required within 24 hours of recognition of an event type, which would be an insurmountable obligation to place on Balancing Authorities (BAs), Reliability Coordinators (RC) and Distribution Providers (DPs) because we are unaware of any of these entities have real-time monitoring of DER resources. There are technical and regulatory challenges that need to be overcome first. (e.g., DP adoption of DER Management Systems (DERMs), integration of DERMs with SCADA systems) While these systems and solutions will be deployed over time, the industry is not at that point yet. We also note that until DER resources are registered with NERC similar to other resources, and have regulatory obligations similar to other registered resources, entities such as BAs, RCs and DPs may not be able to get the needed data to support Event Reporting as envisioned within this SAR.		Thank you for your comment. Please see response to EEI's comments for this comment's response.
Evergy			Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI), the MRO NSRF and ISO/RTO Council with regards to the draft EOP-004 SAR.		Thank you for your comment. Please see response to EEI's comments, NSRF's comments, and ISO/RTO Council's comments for this comment's response.
Daniel Gacek on behalf of Exelon	General Comment		Exelon supports the intent of the SAR, the project however should be postponed until changes are made to the MOD-032 standard to clarify the aggregate DER data entities are required to maintain, and until the registation requirements for owners and operators of Inverter-Based Resources are determined.		Thank you for yoru comment. Updated related SARs and standards section to include Project 2022-02 in addition to the already included Project 2023-01. Both of these can be prioritized in the Standards Committee as applicable to other ongoing standards work coming from the comment's cited efforts.
Ali Miremadi (CAISO), Bobbi Welch (MISO), Elizabeth Davis (PJM), Charles Young (SPP), Kennedy Meier (ERCOT), Kathleen Goodman (ISONE), Helen Lainis (IESO), Gregory Campoli (NYISO)	1-6	Overarching comment	While ISO/RTO Council agrees there is an Industry Need to be aware of large scale disturbances that result from the unexpected loss of DERs, this can be better accomplished under the scope of the existing project for reporting of IBR generation losses (Project 2023-01: EOP-004 IBR Event Reporting). This is because events that cause DERs to trip will likely cause IBRs to trip as well. Rather than expand the scope of EOP-004 to require the reporting of DER related disturbance events, NERC's Event Analysis process should be expanded to inquire about DER trips following the receipt of an EOP-004 report for a qualified "Loss of IBR" event. This is preferable to creating a separate EOP-004 reporting requirement for a "Loss of DERs" event	Retire the DER SAR in its entirety. Expand NERC's Event Analysis process to inquire about "Loss of DERs" following the receipt of an EOP-004 report for a qualified "Loss of IBRs" event.	Thank you for your comment. The SAR cites ongoing Project 2023-01 as an ongoing project on EOP-004. Text added to scope section for SDT to identify if a separate Event Type should exist for aggregate DER reporting, or if such reporting and identified thresholds shoudl be added to existing Event Types.

Ali Miremadi (CAISO), Bobbi Welch (MISO), Elizabeth Davis (PJM), Charles Young (SPP), Kennedy Meier (ERCOT), Kathleen Goodman (ISONE), Helen Lainis (IESO), Gregory Campoli (NYISO)	2	12	The SAR seeks to require "reporting by Balancing Authorities (BAs) and Reliability Coordinators (RC) of the loss of aggregate DERs to NERC." NERC Standards collectively require what was the Control Area (now the BA and TOP) to know the status of each Transmission and Generation element within their footprint. This requirement is met by monitoring BES-connected Transmission and Generation via ICCP/SCADA. Load is calculated indirectly by measuring all generation and interchange (import/export) in the Balancing Authority Area. Neither BAs nor RCs have direct visibility into DER operation or the ability to distinguish the impact of "Loss of DERs" on load.	Retire the DER SAR in its entirety. Expand NERC's Event Analysis process to inquire about "Loss of DERs" following the receipt of an EOP-004 report for a qualified "Loss of IBRs" event from the appropriate NERC functional entities that have visibility into DER operations. If the SAR moves forward, it should be revised to clarify that any resulting Reliability Standard revisions should be limited to requiring RCs, BAs, and TOPs to use information that is already available to them, and should not contain any explicit or implicit obligation for these entities to provide information that is not already available to them or to expand their information-gathering capabilities to comply with the standard	Thank you for your comment. The cited text is not taken from scoped sections but is a reduction of a background statement on the current status of EOP-004. The scope of the SAR is to require reporting of "loss of aggregate DERs by applicable entities". The SAR scopes the SDT to determine the applicable entity. The SAR further states the "SDT can consider monitoring net load" for their established threshold. The SDT should ensure and confirm that the chosen threshold is technically feasible for the current infrastructure in the SAR.
Ali Miremadi (CAISO), Bobbi Welch (MISO), Elizabeth Davis (PJM), Charles Young (SPP), Kennedy Meier (ERCOT), Kathleen Goodman (ISONE), Helen Lainis (IESO), Gregory Campoli (NYISO)	2	16	The SAR recommends the SDT "clarify how loss of aggregate DER and loss of firm load are accounted so they are not canceled by netting the two." Given the sheer number of telemetry data points going into a BAs indirect calculation of load, it is not unusual to have several instances of sudden load spikes, in either direction, per day due to momentary bad telemetry. EOP-004 is a 24 hour reporting requirement that is well suited for monitoring and reporting variables that are directly measured by ICCP/SCADA such as aggregate BES connected IBR resources. It is not well suited for reporting variables that are estimated by measuring thousands of data points, which each can cause a spike if the data point goes bad. It is not unusual for larger BAs to experience multiple spikes in a day, each amounting to several hundred MWs or more.	Retire the DER SAR in its entirety. Expand NERC's Event Analysis process to inquire about "Loss of DERs" following the receipt of an EOP-004 report for a qualified "Loss of IBRs" event from the appropriate NERC functional entities that have visibility into DER operations.	Thank you for your comment. This is a near duplication of a comment in row 124. See response to the comment there.
MRO NERC Standards Review Forum (MRO NSRF)	1-6	Overarching comment	While the MRO NSRF agrees there is an Industry Need to be aware of large scale disturbances that result from the unexpected loss of DERs, this can be better accomplished under the scope of the existing project for reporting of IBR generation losses (Project 2023-01: EOP-004 IBR Event Reporting). This is because events that cause DERs to trip will likely cause IBRs to trip as well. Rather than expand the scope of EOP-004 to require the reporting of DER related disturbance events, NERC's Event Analysis process should be expanded to inquire about DER trips following the receipt of an EOP-004 report for a qualified "Loss of IBR" event. This is preferable to creating a separate EOP-004 reporting requirement for a "Loss of DERs" event	Retire the DER SAR in its entirety. Expand NERC's Event Analysis process to inquire about "Loss of DERs" following the receipt of an EOP-004 report for a qualified "Loss of IBRs" event.	Thank you for your comment and agreement on Industry Need. The SAR does already link Project 2023-01 as an impacted ongoing project that the Standards Committee may assign this SAR as scoped work to the team. Added text to the scope section based on this and other comments to scope the determination of Event Type for the reporting of aggregate DER.

MRO NERC Standards Review Forum (MRO NSRF)	2	12	The SAR seeks to require "reporting by Balancing Authorities (BAs) and Reliability Coordinators (RC) of the loss of aggregate DERs to NERC." NERC Standards collectively require what was the Control Area (now the BA and TOP) to know the status of each Transmission and Generation element within their footprint. This requirement is met by monitoring BES-connected Transmission and Generation via ICCP/SCADA. Load is calculated indirectly by measuring all generation and interchange (import/export) in the Balancing Authority Area. Neither BAs nor RCs have direct visibility into DER operation or the ability to distinguish the impact of "Loss of DERs" on load.	Retire the DER SAR in its entirety. Expand NERC's Event Analysis process to inquire about "Loss of DERs" following the receipt of an EOP-004 report for a qualified "Loss of IBRs" event from the appropriate NERC functional entities that have visibility into DER operations.	Thank you for your comment. This is a near duplication of a comment of row 120. See the response there for this comment's response.
MRO NERC Standards Review Forum (MRO NSRF)	2	16	The SAR recommends the SDT "clarify how loss of aggregate DER and loss of firm load are accounted so they are not canceled by netting the two." Given the sheer number of telemetry data points going into a BAs indirect calculation of load, it is not unusual to have several instances of sudden load spikes, in either direction, per day due to momentary bad telemetry. EOP-004 is a 24 hour reporting requirement that is well suited for monitoring and reporting variables that are directly measured by ICCP/SCADA such as aggregate BES connected IBR resources. It is not well suited for reporting variables that are estimated by measuring thousands of data points, which each can cause a spike if the data point goes bad. It is not unusual for larger BAs to experience multiple spikes in a day, each amounting to several hundred MWs or more. Therefore, requiring the BA (or RC) to report "loss of load" events could result in the reporting of a substantial number of extraneous events.	Retire the DER SAR in its entirety. Expand NERC's Event Analysis process to inquire about "Loss of DERs" following the receipt of an EOP-004 report for a qualified "Loss of IBRs" event from the appropriate NERC functional entities that have visibility into DER operations.	Thank you for your comment. The net load indicated in the SAR was intended to determine the aggregate of monitored T-D Interfaces and not in the indirect measurement to calculated net internal load for items like ACE. Clarity edits added to that effect in the SAR. Further clarity added for SDT to ensure their threshold does not dramatically increase extraneous events reported through EOP-004.
MRO NERC Standards Review Forum (MRO NSRF)			Prior to developing DER standards, the term DER must be defined. This could be accomplished as part of the existing Project 2022-02: Modifications to TPL-001 and MOD-032 or as a standalone project. Project 2022-02 objectives (see pages 1-2 of the SAR): "Update MOD-032-1 to: (1) include "data requirements and reporting procedures" for DER that are necessary to support the development of accurate interconnection-wide models, (2) replace Load-Serving Entity (LSE) with Distribution Provider (DP) because of the removal of LSEs from the NERC registry criteria, (3) enable the SDT to review any additional gaps in DER data collection with the de-registration of LSE."	Define the term DER under the scope of existing Project 2022-02: Modifications to TPL-001 and MOD-032 or initiate a new, standalone project to do so.	Thank you for your comment. Updated SAR to reference the work done by Project 2022-02 to define DER.
Tacoma Power			Tacoma Power supports comments from MRO NSRF		Thank you for your comment. Please see response to NSRF's comments for this comment's response.
Tacoma Power			The Scope identifies a need to align the DOE-417 form with any changes made to EOP-004. This is indeed critical to the success and alleviation of reporting burden to entities.		Thank you for your supportive coment. No changes made based on this comment.

Tacoma Power			As noted in comments to draft MOD-032, not all distribution utilities are registered as DPs. As such, BAs may not be able to obtain information on DERs within these utilities and have no path to enforce providing this information. This issue must be addressed and backstopped by NERC before the intent of this DERs SAR is reasonably achievable.		Thank you for this comment. The SAR has scope for the SDT to determine the responsible entities as identified.
Tacoma Power			The reporting timelines existing under the DOE-417 are 1-hour, 6-hours, 1-day and 1-business day. Considering that these events may require significant analysis by the utility to determine DERs contribution to events, and the intent of this SAR is for post-event analysis, a new reporting timeline should be considered OR this reporting should not be accomplished by the OE-417 process.		Thank you for your comment. The SAR states to ensure "consistency of reporting by the forms accepting for this reporting in the Attachments of the Reliability Standard", indicating the SDT is scoped to be able to consider this comment's solutions as part of their deliberations.
Tacoma Power			The current EOP-004 and DOE-417 process already captures uncontrolled load loss of various thresholds. Perhaps a simple means of identifying that DERs may have been involved would be sufficient. This would signal to the ERO a need to investigate further. Because of the OE-417 reporting timeframes Real-Time NCSOs are often the staff submitting these reports on behalf of the utility. None of the items reported via the OE-417 require in-depth investigation prior to the submission of the form.		Thank you for your comment. As this comment identifies, there already exist other load loss thresholds the SPIDERWG reviewed and did not exclude a future SDT from language edits as the comment indicates. Text added to the scope section for clarity.

Privacy and Security Impacts of DER and DER Aggregators

Joint SPIDERWG/SITES White Paper

September 2023

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of NERC and the six Regional Entities, is a highly reliable, resilient, and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six Regional Entities as shown on the map and in the corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners/Operators (TO/TOPs) participate in another.

MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Executive Summary

The Federal Energy Regulatory Commission (FERC) approved Order No. 2222, which enabled distributed energy resources (DERs) to participate in wholesale electric markets[1] through a DER aggregator that interfaces with Independent System Operators (ISO) and Regional Transmission Operators (RTO). These ISO/RTOs are generally registered as the Balancing Authorities (BAs) and Reliability Coordinators (RC) in their respective Interconnections. The NERC System Planning Impacts from the DER Working Group (SPIDERWG) and the Security Integration and Technology Enablement Subcommittee (SITES) have both authored white papers[2] analyzing the bulk system reliability and security implications of the DER aggregator; however, no NERC industry stakeholder group has explored the technical aspects of security controls for these grid functions with their systems. This paper focuses solely on the security controls available to DERs and DER aggregators and provides recommendations[3] in order to maintain the reliability of the BPS.

This paper explores the technical facets of security controls available to DERs and DER aggregators and provides examples of potential attacks that can be mitigated through the implementation of those security controls. It also provides an overview of the security posture for the distribution landscape (particularly for DERs and DER aggregators) and correlations to relevant NERC Reliability Standards. The Bulk Electric System (BES) cyber asset 15-minute impact test is compared to DERs and DER aggregators to understand their potential impact to the BPS. Furthermore, privacy concerns are covered related to the confidentiality of user data for DER owners as such data may be the target of a malicious actor. This paper will also provide high-level recommendations to DERs and/or DER aggregators on security controls or other risk mitigation measures.

---

[1] FERC Order 2222 is available here: https://www.ferc.gov/sites/default/files/2020-09/E-1_0.pdf

[2] The SPIDERWG white paper *BPS Reliability Perspectives for Distributed Energy Resource Aggregators* is available here: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/SPIDERWG_White_Paper_-_BPS_Persepectives_on_DER_Aggregator_docx.pdf and the SITES white paper *Cyber Security for Distributed Energy Resources and DER Aggregators* is available here: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_Cybersecurity_for%20DERs_and_DER_Aggregators.pdf.

[3] This paper does not provide Compliance Implementation Guidance related to the CIP standards. Rather, security controls are presented at a high level, and the functional interplay between DER, DER aggregators, and other entities is considered in the context of security and security controls.

Introduction

Intended Audience

This paper is intended for the following NERC Registered entities, external stakeholders, and broader groups:

- Planning Coordinators (PC)
- Transmission Planners (TP)
- TOPs
- Distribution Providers (DP)
- DER owners, aggregators, and developers
- ISOs/RTOs (i.e., the BAs and RCs)

This paper includes recommendations to DER owners, DER aggregators, and NERC registered entities as they assess or analyze their security and privacy-protective posture. The complexity of managing the security and privacy of these systems is further compounded by the increasing DER penetrations. This paper is not intended to alter the DP's interconnection requirements nor to alter the electrical specifications to produce DER equipment. Rather, this paper is seeking to recommend security measures or requirements that improve the electrical ecosystem's security posture.

Definitions

To clarify terms and definitions to accurately scope what constitutes resources in a DER aggregator versus the SPIDERWG set of terms, the following main points should be noted:

- The SPIDERWG "DER" definition[4] of "any Source of Electric Power located on the Distribution system" is the preferred definition for discussing reliability concerns. The following is additional context:
    - This is different from the definition of DER in the FERC order, which is "a source or sink of power that is located on the distribution system, any subsystem thereof, or behind a customer meter."[5] Namely, the reliability-focused (i.e., SPIDERWG) definition focuses on generation only while the FERC definition includes load.
    - This is also slightly different from current discussions in Project 2022-02,[6] which is attempting to consolidate definitions and avoid the addition of many new terms. The Project 2022-02 definitions are not currently approved at the time of this document's publication.
- FERC Order 2222 introduces the definition of "DER aggregator," which (for this paper) is the entity[7] that controls the aggregation of generation (i.e., DERs) and load end-use devices.
    - The DER aggregator may have control over both load and generation, and it may control existing demand response programs.
- Both definitions include inverter-based resources (IBR) and non-IBR generation. For example, a 1 MW Solar PV plant and a 500 kW steam cogeneration facility would both be DERs if they are distribution connected.

---

[4] The SPIDERWG terms and definitions, including DER, Source of Electric Power, and Distribution System are available here: https://www.nerc.com/comm/RSTC/SPIDERWG/SPIDERWG%20Terms%20and%20Definitions%20Working%20Document.pdf

[5] Taken from FERC Order 2222 on page 85. Available here: https://www.ferc.gov/sites/default/files/2020-09/E-1_0.pdf

[6] Project 2022-02 website is located here: https://www.nerc.com/pa/Stand/Pages/Project2022-02ModificationstoTPL-001-5-1andMOD-032-1.aspx

[7] Furthermore, there are various names for the entities that control and aggregate DERs besides the DER aggregator. Examples include virtual power plant or emergency load reduction programs (excluded demand response). For this paper, DER aggregator and these other entities are synonymous as they functionally aggregate DERs (i.e., generation) on the distribution system.

DER management system (DERMS) and virtual power plant (VPP) control schemes will likely have different communications architecture.[8] For this paper, the terms DER aggregator, VPP, and utility systems that manage the control of DER are equivalent, and recommendations to a DER aggregator apply to these entities as well. However, each has a specific architecture that require different attack surface evaluations. Since this paper is a reliability-focused discussion on the privacy and security impacts of DERs and DER aggregators, it uses the SPIDERWG set of definitions. In instances where the load portion of a DER aggregator is relevant the load will be separated from generation by using terms like "DERs and load".

IEEE 1547-2018

The latest update to IEEE 1547-2018[9] makes it possible for the utility, or any other entity, to deploy DERMS and cohesively monitor and manage the diverse mix of DER technologies[10] and brands being deployed today. Utilities and third-party aggregators are deploying DERMS, making them an integral part of system operations. However, the large and diverse number of DERs, their evolving capabilities, and their continuous interconnection and retirement pose significant challenges to security and reliability of the DER ecosystem. Standardization efforts like IEEE 1547-2018 make DER integration practical by keeping DER operational functions simple and leaving more complex operational functions to the control and integration systems (i.e., DERMS or VPP). The standard also only dictates the communication protocols and intentionally left cybersecurity out of scope.

UL Solutions Standard 2941

UL Solutions announced the publication of UL 2941,[11] the *Outline of Investigation for Cybersecurity of Distributed Energy and Inverter-Based Resources*, developed in cooperation with National Renewable Energy Laboratory (NREL). The requirements will provide a single unified approach for testing and certification of DERs in advance of the anticipated rapid deployment.[12]

These new requirements prioritize cyber security enhancements for power systems technologies, particularly for inverter-based resources and DERs. UL 2941 is anticipated to promote the cyber security of new IBR and DER systems.[13] The standard outlines various testing needed to pass in order to achieve certification.

Regional Autonomy and Network Architecture

In the context of DER aggregators, security includes availability. The electric power system is designed with the ability for given area to isolate from surrounding areas for reliability purposes. For example, it may be possible for a given BA to maintain service within its footprint when a blackout is occurring in adjacent areas. As DERs become more common, there is increased potential for power system operability at local levels.

For regional power systems to operate, both the energy and the communication systems involved must be available. If DERs play a role of any significance, then the communication networks that manage DERs must remain functional. This can be an issue for some communication architectures. Grid equipment is integrated via networks that remain available when the local area is operating, but DERs within the area may not be available if they are managed via systems or networks in some other location where operation has been interrupted. For example, if a DER aggregator operates DERs in the Western Interconnection, then it isn't practical for the associated control system to have dependencies in a different system, such as the Eastern Interconnection.

---

[8] Primarily that utility implemented DERMS will likely have direct control and on-premises security controls while VPPs are more inclined to utilize cloud solutions for their security controls.

[9] IEEE 1547-2018 is available here: https://standards.ieee.org/standard/1547-2018.html

[10] E.g., Battery Energy Storage, Solar Photovoltaic, or synchronous DERs.

[11] Available here: https://www.shopulstandards.com/ProductDetail.aspx?productId=UL2941_1_O_20230113

[12] https://www.nrel.gov/docs/fy23osti/84709.pdf

[13] https://www.ul.com/news/ul-solutions-and-nrel-announce-distributed-energy-and-inverter-based-resources-cybersecurity

Chapter 1: Security Controls Available to DERs and DER Aggregators

The draft *IEEE P1547.3 Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems,*[14] currently out for industry comments, provides guidance and recommendations for cyber security practices and controls to ensure secure communication of DER protocols (e.g., IEEE Std 1815, IEEE Std 2030.5, SunSpec Modbus, and IEC 61850) specified in the IEEE 1547-2018.

The P1547.3 guide includes considerations relating to the following cyber security topics:

- Risk assessment and management
- Communication network engineering
- Access control
- Data security
- Security management
- Coping and recovering from security events
- Testing and commissioning for cyber security and conformance with the IEEE P1547.3.

Though not exhaustive, the following sections provide a high-level overview of security controls available to DER devices and installation sites, DER aggregators and their control systems. **Figure 1.1** graphically shows the new communication pathways (in red) introduced with the addition of the DER aggregator to the electric ecosystem. Although their equipment, such as DER gateways, may be at the DER site, the DER aggregator logically sits at the T-D Interface and may communicate its DER control capabilities to the ISOs and RTOs (i.e., the BAs and RCs), who may then determine the utilization of those capabilities in coordination with distribution system operators. The DER aggregator issues operating commands to the DERs it manages as well as communicates necessary information with the additional key entities in the ecosystem. These new communication pathways necessitate a thorough understanding of associated risks and the available mitigating controls essential to protecting data security, privacy, and grid reliability.

---

[14] IEEE P1547.3 website: https://sagroups.ieee.org/scc21/standards/ieee-std-1547-3-2007-revision-in-progress/

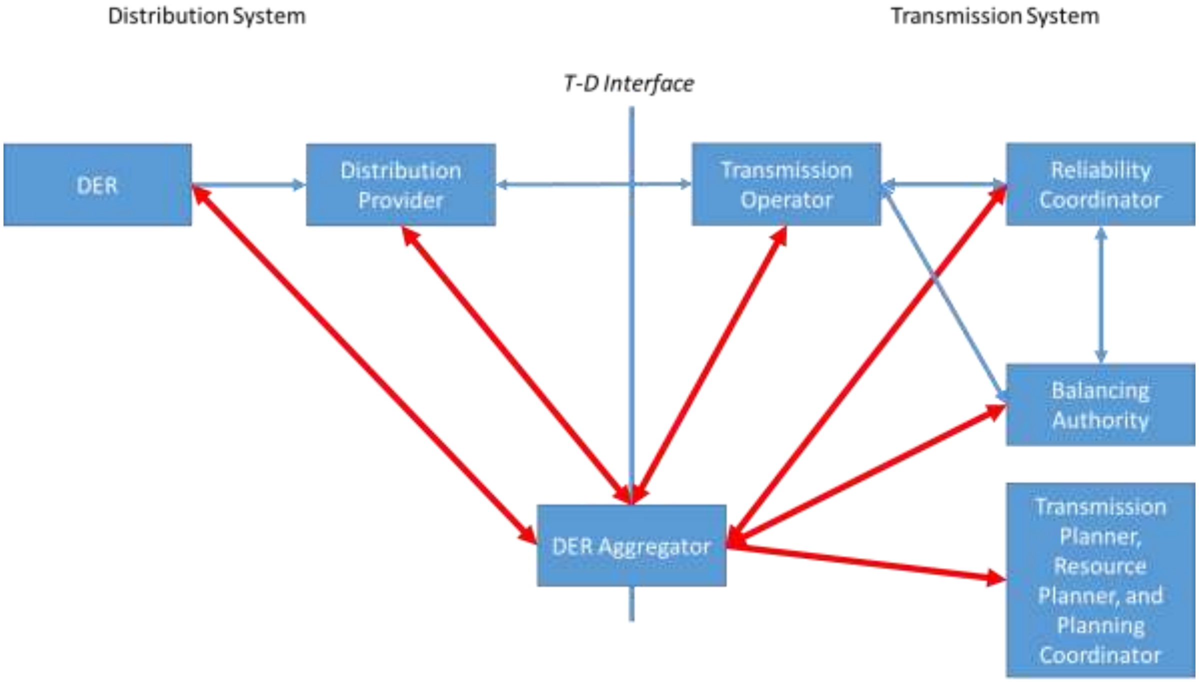


Figure 1.1: High-level Diagram of Added Communication for DER, DER aggregators, and the BES[15]

Network and Protocol Security

DERs, DER aggregators, and utility networks should be separated based on ownership, control capabilities, and trust relationships within specific implementations. The increased attack surface stemming from the connection of numerous DERs demands network architectures[16] that do not rely on implicit trust relationships. In the event of a single device or entire network segment compromise, proper network segmentation and additional security controls should ensure the continued operation of other segments.

Securely designed network architecture for DERs and DER aggregators may include the following:

- **Demilitarized zones, subnets, and VLANs**: These logical network segments isolate sensitive or critical systems from other parts of the networks; they establish security zones based on criticality of assets or operations and limit unauthorized access and potential damage from cyber attacks.
- **Intrusion prevention systems and intrusion detection systems:** These systems enable comprehensive visibility into network traffic through the monitoring and detection of suspicious activity or potential threats. Passively and continuously scanning and analyzing network traffic for known common vulnerabilities and exposures in addition to abnormal patterns these systems can identify and prevent potential cyber threats and enhance overall network security. This type of technology can be deployed in the demilitarized zone of the network to segment operational networks from business networks in and between subnets and VLANs for “East-West” protection.
- **Absence of implicit trust relationships:** Network architectures should be designed without assumptions of trust between connected devices or systems, minimizing the potential for unauthorized access and lateral movement of attackers within the network.

---

[15] Note that attacks scenarios can target communications outside of those highlighted in the Figure 1.1. For instance, original equipment manufacturer to DER communication as well as DERs directly to the RCs or BAs.

[16] This includes architectures that are centrally-managed and contain source-traceable components. Implicit trust can be designed out of an architecture and implicit trust should not be assumed even when an entity owns all components of the architecture.

- **Secure network boundaries:** Firewalls control incoming and outgoing network traffic based on predetermined rules while data diodes ensure one-way data flow that add layers of protection to network boundaries.
- **Strong encryption:** Implementing advanced encryption algorithms, such as Advanced Encryption Standard,[17] Elliptic Curve Cryptography, and Rivest-Shamir-Adleman,[18] ensures the confidentiality and integrity of sensitive data transmitted across networks.
- **Secure Protocols:** Communication protocols with built-in security features ensures the safe and reliable exchange of information between DER devices and control systems such as DNP3-SA.[19] These protocols incorporate robust authentication, encryption, forward-secrecy,[20] and non-repudiation, providing a strong foundation for secure DER communication.
- **Authentication:** Robust authentication mechanisms (e.g., digital certificates, public key Infrastructure, phishing-resistant multi-factor authentication) validate the identities of devices and users.
- **Authorization:** Implementing access control policies based on the "least privilege" principle ensures that users and devices have the minimum necessary access rights, limiting the potential impact of compromised credentials.
- **Virtual private networks (VPN):** VPNs create secure and encrypted connections over public networks (i.e., the internet) that protect data transmission from eavesdropping and tampering.
- **Efficient logging and alerting:** Security information and event management systems collect, analyze, and correlate log data from various network devices that generate alerts for potential security incidents and facilitating timely response.
- **Hardened networking equipment:** Applying security technical implementation guide recommendations ensures that networking equipment adheres to industry-standard security practices and reduce vulnerabilities and attack surfaces.

Besides isolating networks based on trust relationships and ownership, DER aggregator and utility networks should also be segregated within their internal networks (e.g., isolating corporate networks from industrial control systems). Implementations and specific security controls will depend on the use cases for a given DERMS. Isolated networks can range from decentralized VPP architectures, centralized distribution utility DERMS, or hybrid implementations. In addition, these networks should be securely segmented from other networks, including corporate networks. Insufficiently segmented networks with weak or lax security controls could enable cyber attacks to spread across multiple systems and network segments. DER endpoints,[21] being the most vulnerable links in these networked systems, present a higher risk of targeted attacks, such as DERs and DER gateways. **Figure 1.2** shows an example network architecture of a DER-managing entity controlling both small-scale DERs and utility level DERs. **Figure 1.2** highlights the effective use of network segmentation and firewalls to establish security zones, providing network boundaries to deploy further security controls.

---

[17] 100 bits or above should be used to be secure.

[18] 2,048 bits or above should be used to be secure.

[19] Other secure protocols exist. This is used as an example of one such secure protocol.

[20] Forward secrecy methods implemented within protocols ensures that past communication sessions cannot be decrypted if either session or private keys are compromised.

[21] Endpoints of a security system are where the "door meets the outside" for any given system. These are access points designed in system architecture and are frequently targeted by malicious actors. See here for a panel that discusses more of the reasons why endpoints are vulnerable: https://webinars.govtech.com/Closing-the-Endpoint-Security-Gap-in-State-and-Local-Government-102979.html#:~:text=According%20to%20intelligence%20firm%20IDC,and%20administrative%20passwords%2C%20and%20more.

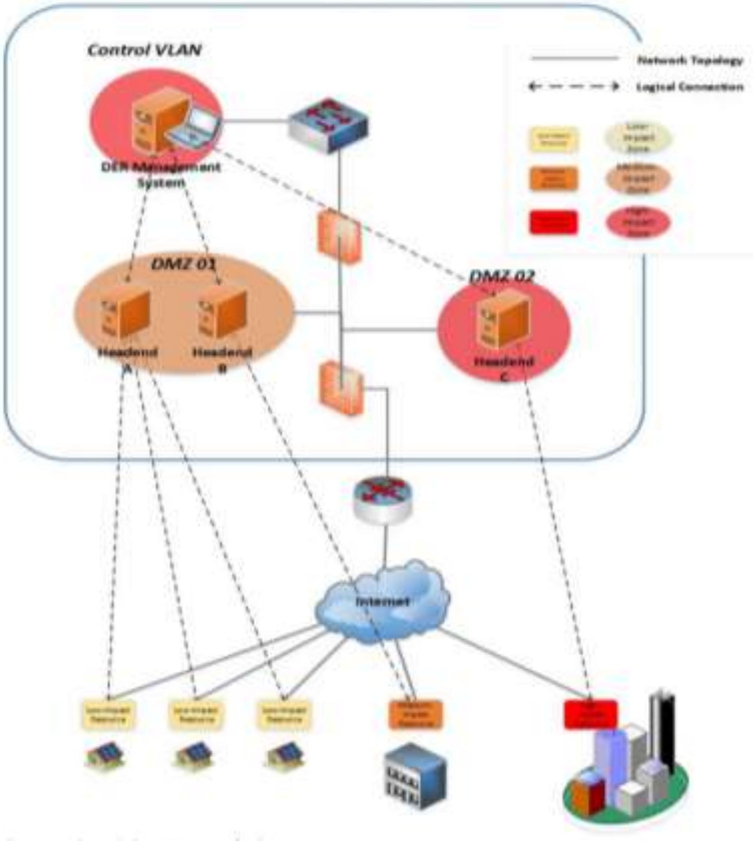


Figure 1.2: Example DER Managing Utility Architecture [Source: EPRI]

In general, network and protocol security are fundamental to proper cyber security practices. As such, the types of threats and adversary tactics they mitigate are diverse and numerous.

Internal Network Security Monitoring

Internal network security monitoring (INSM) controls are available for all networks involved, potentially including owners of the DER network,[22] the DER aggregator's network, a utility's network, or an original equipment manufacturer's (OEM) network. INSM monitors the traffic flowing internal throughout the network and provides alerts when suspect traffic is detected. These solutions include network mapping, vulnerability management, anomaly detection, logging, and alerting when malicious traffic is detected. Some INSM implementation may also block network communications to and from suspected compromised nodes. Proper patching and updates to malicious code signatures or heuristic detection schemes are critical to assure effectiveness of these network-based security controls.

Monitoring and logging are a prerequisite for any automated prevention or response-based controls, including access control lists, endpoint security, and security orchestration tools. In addition, the monitoring controls and their associated logs and reports facilitate security event triage and are key components[23] of security incident response activities. Their monitoring and alert data can also be sent to security information and event management solutions for security operations center analysts and/or handled by managed security service providers.

---

[22] It is not expected that residential DER owners would implement advanced controls beyond the default configuration at the time of their DER installation.

[23] Due to their pivotal nature, these controls will be required for high impact or medium impact with external routable connectivity control centers in the NERC CIP standards per FERC Order 887. Text available here: https://www.ferc.gov/media/e-1-rm22-3-000

Complete INSM solutions can be implemented for greater network visibility, but limitations in architecture, bandwidth, or device capabilities may preclude the monitoring of 100% of all network segments. This monitoring is analogous to the current and voltage relaying equipment[24] typically found on the electrical monitoring equipment in substations; however, these controls can take some automated action to mitigate against specific traffic. The following malicious activities can typically be detected by successful implementations of INSM:

- Active scanning of networks by malicious actors
- Lateral movement between internal network nodes, such as servers and workstations, and DER endpoints
- Download of known malware
- Command and control traffic
- Communications parameters and malformed packets
- New devices connecting to networks
- Weak and cleartext passwords
- Appliance usage and health logs
- Threat intelligence indicators of compromise (e.g., malicious IP addresses)

In general, INSM defends against internal reconnaissance, lateral movement within the network, and malware deployment to reduce the severity from incidents and compromise. Additionally, should a malicious actor compromise a DER or DER aggregator network, INSM may be able to detect outbound command and control communications, which is a prerequisite for a coordinated attack utilizing many compromised DER devices.

Interactive Remote Access Controls

Physical access to the DER site by the utility or DER aggregator is typically unlikely outside of routine meter reads and similar calls. Consequently, DER gateway communication interfaces will need to facilitate remote access capability to perform routine patching, firmware updates, or even the altering inverter settings. Any remote access[25] (and the communications network required to facilitate it) introduces a credible attack vector to the DER, gateway, and DER aggregator ecosystem. The absence of security controls, improperly configured and maintained security controls, or vulnerabilities at the DER site or within a DER aggregator's network could be exploited. Securely implemented and maintained remote access is critical for DER aggregators, utilities, and OEMs to service and manage DERs.

Remote access may require software and certain functionality on both sides of the communication link. Thus, security controls may exist on the utility network, DER aggregator network, or on the DER device or DER gateway in order to provide remote access capability in a secure manner. A simple but inadequate form of a security control authentication credentials;[26] more sophisticated remote access control mechanisms are needed. Secure remote access technologies include the following:

- VPNs using encrypted tunnels for network traffic
- Network access controls limiting device connections to authorized and accessed[27] devices

---

[24] As substation circuit breakers requires the voltage and current waveforms in order to isolate faults from the system. As such, more complex security solutions require monitoring and logging to perform their objective.

[25] Programmatic or interactive

[26] Another mitigation example is adding a timeout session of remote access.

[27] Assessed in this context means assessing the security posture of the device prior to it being allowed access to network resources. Security posture assessment may include firmware patch level, antivirus version, hardening level, MAC address, or other criteria used to assess the security "health" of the device.

- Phishing-resistant multi-factor authentication (MFA)[28] for interactive remote access
- Certificate based authentication for programmatic application access or system-to-system access
- Zero trust architectures requiring constant re-authentication and re-authorization
- Secure protocols

These methods are essential for securing remote access, a high-demand function for the current digitalized landscape. With an increasing number of access points through remote DER connections, secure networks are paramount to facilitating DER adoption and management through DER aggregator and utility systems. While the implementation and specific functionality of a technology will determine the vulnerability to particular threats and attacks, secure remote access implementations can generally mitigate the following types of malicious activities:

- Unauthorized external remote access
- Man-in-the-middle attacks
- Remote system discovery and reconnaissance
- Compromised trust relationships

Any security controls improperly configured or unpatched systems for vulnerabilities may allow attackers to circumvent remote access controls. Thus, the above mitigations support proper cyber-hygiene and a defense-in-depth approach. Both are important to balance the need for remote access with the security risk.

Data Management and Access Controls

Data, particularly at the DER aggregator level, can scale exponentially. Data management policies that address storage, transit, use, and retention measures are essential to ensuring the establishment of a holistic data management program.[29] Data management and access controls secure the access and management functions of data. Applied to DER and DER aggregators, these controls limit the credentials of who can read, write, and transfer data from a particular entities network. At the DER device level, these functions are broad per 1547-2018, particularly Clause 10 language, which allows for wide read, write, and transfer capabilities inherent in the DER equipment itself. Other device standards, like UL2941, are more specific in their requirement language for data storage and data transit. As stated above, 1547-2018 requires that DERs support necessary monitoring and management at the local interface and does not specify cyber security at this interface. With this, DER aggregators and DER owners need to implement these cyber security controls on their respective networks.

The controls themselves reside in the privileges granted to users to read, write, extract, and otherwise alter the data on the DER, DER aggregator, or other entity's network. Best practice security controls include storage, extraction, and deletion policies for data. These practices are particularly useful when exchanging equipment at the DER aggregator level that may have private information stored about the DER it controls or even for DER owners that exchange devices to wipe the private information stored locally. Effective implementations ensure the security and privacy of data as well as mitigate against IT sourced attacks on OT equipment in this environment. Specific attacks mitigated by data management and access controls could include the following:

- Credential harvesting or access
- Privilege escalation

---

[28] *Implementing Phishing-Resistant MFA*. CISA: October 2022. https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[29] Some data management policies allow for off-site, on-site, or hybrid approaches to manage data. Cloud security practices are important once data management and access controls include off-site or hybrid data management solutions.

- Account manipulation
- Data deletion, encoding, obfuscation, or manipulation
- Cryptographic (private) key exfiltration

Data management controls can further mitigate against data exfiltration or ransomware by a malicious actor. Privilege escalation is a common technique in the cyber criminal's toolbox, allowing the individual or malware to overcome a number of inhibiting controls to access data. Controls, such as data loss prevention, intrusion detection systems/intrusion prevention systems, and endpoint security, provide a greater assurance to detect or prevent the exfiltration or malicious encryption of data.

DER Gateways

DERs face a broad range of local threats and vulnerabilities that are presently outside of utility responsibility and control. For example, a DER can have a variety of interfaces in addition to the standardized one, including those used for aggregators, owners, and OEM management. Each of these interfaces present a potential backdoor to the DER, any local networks, and the upstream managing entity's systems. IEEE 1547-2018 requires one open standard interface but does not prohibit these other interfaces. There are currently no specifications or requirements that apply to other DER interfaces. IEEE 1547-2018 does not specify cyber security requirements for DER and its local interfaces because they are generally untrusted systems to the DER managing entity[30] due to these risk exposures.

Key Takeaway:
Although endpoint controls may be applied to the DER to accomplish security objectives, these controls are not guaranteed to be adequately maintained over their lifetimes, and existing DERs may not be technically equipped to accommodate them. DER gateways are required to mitigate the lack of endpoint controls on the DER devices and to ensure secure interoperability with upstream managing entities. Alternatively, endpoint controls on the DER devices may accomplish some of the same security objectives.

Furthermore, current compliance and certification frameworks are limited in their scope of enforcement[31] to ensure that necessary security controls are adequately met among DER owners. In the absence of enforceable requirements at all DER interfaces, managing entities cannot establish assurances that critical security controls use for secure communications, including certificate management, private key protection, firewall policies, user access control, and other device-specific security features that are routinely reviewed and maintained over the DER's lifetime. This gap presents a challenge for managing entities where the integrity and availability of data and functionalities cannot be fully established for communications to the DER, where risk exposures[32] are much broader. This gap exposes all interfacing parties to a variety of attack scenarios against communications critical for grid interoperability, including the following:

- **Man-in-the-Middle:** Data that is supposed to flow only between a managing entity and the DER flows through a middle node that reads or modifies data before it is sent on its way.
- **Denial of Service:** A group of compromised DERs deliberately overload upstream managing systems with useless traffic and the resource-exhausted network or managing system cannot perform its functions. Alternatively, a certificate expires on the DER and prevents the managing system from accessing it. In both cases, this could impact a power system operator trying to control the power system.

---

[30] The special case exception to this is when the DER managing entity is also the DER manufacturer.

[31] Due to the voluntary nature of the IEEE Standards, and the varying nature of the regulatory framework for the local distribution of energy. Furthermore, it is not feasible to require action at the DER Owner level for their networks.

[32] This is especially true for cases where DERs integrate using public, internet-based networks.

- **Replay:** A command being sent from the managing entity to the DER is copied by an attacker. This command is then used at some other time to cause unexpected actions performed by the DER.
- **Malware**: An attacker adds malware to a DER, allowing it to propagate upstream to the managing entity.

DER gateways can serve as local platforms that house features and functions important to the DER managing entity, but they can also perform several important perimeter security functions that prevent these attack scenarios. This local platform physically resides at the DER site and includes a wired, physical interface that establishes a private connection to the DER through the gateway though the definition is still under revision in IEEE as defined by IEEE 1547.

Placing security requirements for DER gateways assumes that there are deficiencies in DERs and establishes a higher degree of trust in the communications to and from DER sites to protect critical utility systems, such as DERMS and advanced distribution management systems, from internal and external threats. These requirements include translating the DER's communication to trusted transport layer security (or similar) communications, implementing data access rights through role-based controls, configuring network access control and segmentation through firewall policy, performing network and application-layer monitoring for threats, and verifying firmware updates through signature-based methods. Because these and other security features are implemented on a gateway that is owned, implemented, maintained, and certified by the managing entity rather than the DER-owner or manufacturer, managing entities can ensure secure integration over public, untrusted networks with its DERMS or other management software operations.

Firmware updates are necessary to maintain security. For example, mobile phones, browsers, and computer operating systems are engineered with great attention to security, and yet frequently updated due to discovered vulnerabilities. It is not practical to expect that a DER managing entity could or would update firmware in a customer's DER for several reasons:

- The system is made up of a broad diversity of makes, models and vintages.
- Only the manufacturers of each DER can produce a new/patched code.
- The manufacturer of DER's may not be in business or supporting the models in the field and are not required by interconnection agreements to provide future updates.
- Manufacturers may not have a network path or connection to reach the DER to perform an update.
- There may be risk of harming (i.e., rendering unusable) a device when updating its code.

However, DER managing entities may readily maintain the firmware of DER gateways that may be of consistent design and under their direct control. For example, firmware updates are commonly pushed to thousands of utility supervisory control and data acquisition radios, millions of AMI meters, etc. Furthermore, complete systems of DER gateways and the communication networks they use can be retired and replaced, when necessary, but it is not practical to force the retirement of a customer's DER.

A new IEEE recommended practice, the *IEEE P1547.10 Recommended Practice for Distributed Energy Resource Gateway Platforms,*[33] is currently under development with contributions from several stakeholder groups (e.g., DER and DER gateway developers, owners, and operators, software producers, distribution and transmission system planners and operators, certification providers). The purpose of this project is to maintain coherency between the family of P1547.x and P2030.x standards as well as other related projects for DERs and DERMS within the evolving smart grid interoperability reference model with a focus on DER gateway platforms. The recommended practices within P1547.10 will enable utilities deploying DERMS and other DER integration systems to integrate DER with grid

---

[33] PAR available at https://development.standards.ieee.org/myproject-web/app - viewpar/13494/9866

edge intelligence, while allowing DER devices to serve their core functions, focused on simplicity, interoperability, and long-term stability. The scope of IEEE P1547.10 includes gateway platform functions and communications, including operational procedures and data collection recommendations. Additionally, recommended procedures for cyber security, centralized manageability, monitoring, grid edge intelligence and control, multiple entities management, error detection and mitigation, events tracking, and notification, communication protocol translation, and communication network performance monitoring. **Figure 1.3** illustrates the use of DER gateways. As indicated by the dashed lines, the gateways are physically at the DER site but are part of the aggregation/management system as shown by the coloring.

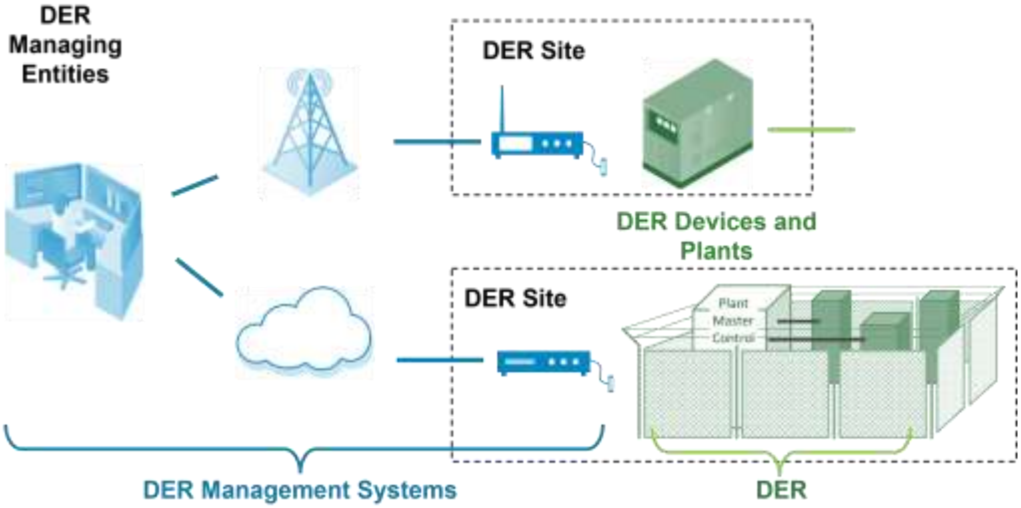


Figure 1.3: Example DER Gateway interface [Source: EPRI]

Carrier Controls Inherent in Communication

Many of the communications channels anticipated for information sharing between DERs and DER aggregators may traverse fiber networks using TCP/IP protocols. Devices (e.g., DER inverters or DER aggregator control centers) using routable protocols over fiber networks, including some private fiber networks, will have a carrier entity install and maintain these communication lines. Entities should ensure that business agreements with third-party carriers of these fiber networks ensure security controls are implemented.

Chapter 2: Current Distribution Security Landscape of DER and DER Aggregators

As evidenced in recent presentations[34] to SPIDERWG and SITES, the distribution landscape is primarily supported by equipment standardization with little to no standard design criteria about specific hardware, technologies, and engineering. This practice is in an effort to ensure that non-engineering technicians can install cost-effective solutions geared towards mitigating commonly reported customer problems within the affected portion of the distribution system. From a cyber security perspective, this may seem to involve major interoperability challenges that would need solid endpoint controls to limit access to the centralized ecosystem. Specific security requirements, however, are left up to each distribution entity's regulatory and corporate bodies to enable specific security controls for DERs. Additionally, FERC Order 2222 does not require any specific security protections to enable the participation of DERs in the wholesale ISO/RTO markets. Thus, SPIDERWG and SITES reviewed all available information on the distribution system and characterized a few main points, summarized below.

Telecommunications Networks: Distribution utilities use a combination of private fiber connections, public internet fiber connections, and radio communication interfaces for their monitoring and switching action. Utility-level DERs are more likely to emulate BPS architectures by using private networks for communication back to their shared locally geographic control centers. Most concerning, however, are geographically decentralized residential and commercial DERs utilizing public networks (i.e., the internet). Commonly, these connections do not use the IEEE 1547-2018 specified interface but a variety of other interfaces for which there is presently no requirements at all. Accordingly, adding cyber security requirements to the IEEE 1547-2018 standard interface would have no effect.

Public internet access for DERs utilizes Wi-Fi and cellular 4G/5G wireless networks, which are susceptible to interception and require strong encryption and authentication. Wired Ethernet and fiber-optic networks can be compromised through physical access or device vulnerabilities at the site of the DER endpoint. In some cases, private networks between the DER aggregator and their controlled DERs are achieved over the internet through the use of VPNs. Such communication offers increased security if the communication is properly terminated for remote sessions. Regardless of the medium for access, the use of public internet leaves both DER and DER aggregator control systems more exposed to remote attacks from anywhere on the globe. To ensure the resilience and stability of residential and commercial DER ecosystems, it is crucial to implement comprehensive security measures tailored to the specific requirements of each telecommunication network.

Electrical Protection Measures: It is still a common practice to use fuse-based protection in most distribution networks; some distribution entities may use more advanced solid state relay protection. In these instances, the protection seeks to limit backfeed to the transmission system or to enhance a secondary area network scheme's ability to recover from fault. The distribution system is thus much more fuse-based, providing single-use protection that is not present in the same ways or same densities on the transmission grid.

Distribution Entities Reliance on Equipment Standardization: With the need to lower cost to their consumers, distribution companies rely on turnkey solutions that are based on standard designs when upgrading or fixing a circuit. This allows the distribution system to be reconfigured by non-engineering staff and field crews while still maintaining high levels of reliability (e.g., using proven designs to limit the system average interruption frequency index and the system average interruption duration index)

Lack of Distribution System Design Security Integration: Rather than installing security protections, distribution companies rely on well-run line crews to recover the system and restore damaged equipment by using local spare equipment. As distribution poles and associated equipment are relatively cheap, some perceive this as a cost-

---

[34] In particular the presentations at the SPIDERWG February 2023 meeting. Available here: https://www.nerc.com/comm/RSTC/SPIDERWG/SPIDERWG_Presentations.pdf

effective solution to the security challenge posed by overhead distribution. However, the proliferation of DERs, the upward trend of cyber attacks against both internet of things and industrial control systems, and the potential for aggregate attack against DER ecosystems are changing these perspectives.

The common distribution system does not currently have a robust set of security requirements and controls to protect it from malicious activity. Rather, the system is currently designed around quick response to equipment damage (e.g., due to tree limbs, downed distribution poles, or other faults) and reconfiguration to maintain a high degree of reliability to their system. Current research and scenario development[35] to secure the distribution system and DERs at large is progressing rapidly, especially by review of equipment standards and implementing security controls. This research is leading to improved equipment-level standards so distribution entities can use standard equipment when integrating DERs into their system. For example, UL Solutions is seeking to investigate a way to certify the functional requirements of secure communication to limit the impact of a security compromise of a single DER at an equipment level. These updates to equipment standards and the certification of distribution equipment are anticipated to maintain the current distribution paradigm and enhance it to support a strong security posture.

Differentiation of Utility-Scale DERs versus Retail-Scale DERs landscape

The security posture between utility-scale DERs (U-DER) and retail-scale DERs (R-DER) can differ. The retail-scale may not have a private fiber connection to the utility itself and can use public networks for communication. Furthermore, the DER owners of R-DER are not able to practically acquire, implement, and maintain the above security controls and as such have no requirements to do so. In the utility-scale side there is a higher likelihood that the connection will be over a private network to the utility and may already have a small attack surface and stronger security controls inherent to the design. These end-use devices will then move towards having fewer recommended additional controls for managers of U-DERs than for management of R-DER devices. Namely, R-DER devices are assumed untrustworthy as a default. However, these categorizations do not alter the current distribution landscape as the same equipment standardization will likely be used to electrically connect both U-DERs and R-DERs to the distribution system. These categorizations are important when considering the “trustworthiness” of a type of communication and for producing standardized designs to incorporate U-DERs, R-DERs, or a combination of both into the distribution system. DER aggregators in particular should implement and maintain security controls that allow for strong protection against attack through the DER it controls regardless of U-DER or R-DER classification.

Distribution Management Systems and Emerging Distribution Landscape Considerations

Currently, efforts are ongoing to implement DERMS at various entities. These systems have functional specifications housed in the IEEE 2030.11-2021,[36] which is a guide that houses the various configurations and required functions of such a management system. Such a guide allows the functions of the DERMS to exist within an entity’s premises, off-site at a cloud-based system, or a hybrid solution that interplays between the two. As stated in the guide, “it is possible to deploy a DERMS in an off-site location where the infrastructure is provided by a third-party computer hosting provider.” While 2030.11 lists the various common communication protocols and concepts required to be addressed, it does not directly address the cyber security requirements of a DERMS. Rather, the guide provided other referenced material (e.g., IEEE C37.240-2014[37]) and allows the integrator of a DERMS to determine the exact cyber security requirements. The guide lists that the security of data in such deployments should be reviewed and include the following:

- Security of data in transit between on-site and off-site locations
- Security of data at the off-site locations

---

[35] One example of the research into recommendations and test cases for cyber security scenarios pertaining to DERs is available here: https://www.osti.gov/biblio/1832209

[36] Available here: https://ieeexplore.ieee.org/document/9447316

[37] Available here: https://standards.ieee.org/ieee/C37.240/5029/

- Security of requests sent from the off-side location to the external internet
- Backups of off-site data
- Hosting service availability

In such instances, the ongoing implementation of a DERMS will have direct tie-ins to the ongoing evaluation of cloud-hosted services and the security requirements of such applications. Most utilities at this time do not have a DERMS and likely lack the sufficient infrastructure to fully utilize a DERMS should they choose to do so. Utilities looking to implement a DERMS in order to manage and dispatch DERs should have stringent specification for cybersecurity requirements when using off-site hosting services as part of their DERMS. Furthermore, DER aggregators are assumed to require a DERMS or similar management system in order to accomplish their goal and should also require stringent cybersecurity requirements when implementing any functions of a DERMS off-site. As a first step, requiring strong cybersecurity controls as part of their service agreements with the off-site hosting service can initiate a bilateral agreement with the off-site hosting service in order to secure the DERMS from malicious interaction.

Security Posture of DER Aggregators

DER aggregators are relatively new entities to the ecosystem of aggregate control of multiple end-use devices to participate in wholesale ISO/RTO markets. The ISO/RTOs consist of the PCs, BAs, and RCs of the transmission system while the DER aggregator is a middle entity that constitutes a pathway for previously independently controlled DER assets. A DER aggregator currently does not have security requirements relative to the risk-impact it has on the bulk system nor does it have OT security requirements outside of those required by regulators over the DER aggregator. As such, the NERC SPIDERWG and SITES have assumed the following with respect to the DER aggregator:

- The DER aggregator will act to protect itself against common information technology (IT) attacks targeting personal data required to award bids.
- The protections on a DER aggregator's IT software will not allow operation technology (OT) compromise by an IT intrusion.
- The DER aggregator has minimal OT security and relies on the utility (i.e., ISO/RTOs) to dictate the required security controls on the aggregator and the DER it controls.
- The DER aggregator will use cloud solutions for their DER management due to the amount of data to process.

Confidentiality of Data at the DER and DER Aggregator

In order to conduct a proper study of the electrical impact of DER and DER aggregators, specific electrical models need to be developed and shared to represent the aggregate impact DERs have on the BPS. SPIDERWG has multiple reliability guidelines associated with the model development of aggregate DERs; however, the representation of a DER aggregator can vary; DERs should be represented with the impact they have on load flow and transient stability. As with bulk-connected resources, some information may be tied to confidential agreements between OEMs or owners, and data sharing of that confidential data is not allowed. This requirement to represent the end-use electrical equipment to study impact of aggregate DERs[38] does not require the type of data typically secured under confidential and private agreements between the DER owner, manufacturer, DER aggregator, or the utility. Entities handling DER information (e.g., TPs, PCs, DPs) should ensure that the security controls they have in place include proper data management and access controls to ensure the sharing of required modeling data can occur while maintaining a high level of confidence in the privacy-protective treatment of end-user data.

---

[38] Operated under a DER aggregator or in independent operation.

Chapter 3: Review of Standards, Frameworks, and Alternatives

As both DER aggregators and DERs do not have a NERC registered entity category that directly covers their applicability to NERC Reliability Standards, SPIDERWG, and SITES identified similarities where the privacy and security practices of DERs and DER aggregators may need to be examined to determine any future applicability to NERC Reliability Standards, especially concerning whether DERs or DER aggregators provide BES reliability operating services. These services are typically assessed for any impact over a 15-minute time frame. **Table 3.1** is from CIP-002-5.1a,[39] which can help relate the electrical function provided by a registered entity and what has been identified to have a grid reliability impact. SPIDERWG and SITES note that the DER aggregator can provide some of these functions for the DER it controls in some instances; however, the capacity of the DER aggregator in a particular area can determine if the service has an impact on BES reliability operating services.

Table 3.1: Impact of Registered Entity and Associated Reliability Functions

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load and Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

In Order No. 2222 Paragraph 130, FERC specified that RTO/ISOs must "…allow distributed energy resources to provide all services that they are technically capable of providing through aggregation." If capable, the DER aggregator's DER aggregations may begin providing services that resemble BES reliability operating services. To determine whether DER aggregator cyber assets meet the definition of BES cyber assets, new and improved models for simulating a DER aggregator's impact on the BES will be required. Without accurate development of electrical models[40] that represent the control behavior pertinent to the functions above, completing the impact test of whether control of the asset may materially impact the bulk system requires engineering judgement. For instance, if DER aggregators are providing frequency regulation (balancing supply and demand on the electric system by changing energy injection or energy withdrawal within seconds), then the impact of rendering the DER aggregator's DER aggregation cyber asset "unavailable, degraded, or misused" within 15 minutes on the BA area should be carefully studied. A DER aggregator providing 1 MW of frequency regulation compared to a DER aggregator providing 100 MW of frequency regulation will clearly have a different level of impact on the BPS (i.e., to area control error).

---

[39] CIP-002-5.1a is available here: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf

[40] These models can take on a variety of data sources, the most common software platforms that represent the BES are positive sequence models. Models here include load flow and transient dynamic representations of the behavior exhibited by DER and DER aggregator actions. Current SPIDERWG modeling documents exist for DER operating independently of a DER aggregator. It is available here: https://www.nerc.com/comm/Pages/Reliability-and-Security-Guidelines.aspx

BES Cyber Asset

The BES Cyber Asset definition can be found at the NERC Glossary of Terms and defines when Cyber Assets become BES Cyber Assets. When DER aggregators contain assets that act as a BES Cyber Asset, they should take appropriate action based on how such assets may materially affect the reliable operation of the BPS.

Key Takeaway:
When DER aggregators contain assets that act as a BES Cyber Asset, they should take appropriate action based on how such assets may materially affect the reliable operation of the BPS.

Limitations on Assessment and Applicability of DER, DER Aggregators, or other Distribution Entities

The *NERC Rules of Procedure* Appendix 5B's material impact test[41] defines the way in which a potentially compromised asset in the generation, transmission, or distribution of energy can impact the BES. The materials impact test questions are as follows:

- "Is the entity specifically identified in the emergency operation plans and/or restoration plans of an associated Reliability Coordinator, Balancing Authority, Generator Operator or Transmission Operator?
- Will intentional or inadvertent removal of an Element owned or operated by the entity, or a common mode failure of two Elements as identified in the Reliability Standards (for example, loss of two Elements as a result of a breaker failure), lead to a reliability issue on another entity's system (such as a neighboring entity's Element exceeding an applicable rating, or loss of non-consequential load due to a single contingency)? Conversely, will such contingencies on a neighboring entity's system result in issues for Reliability Standards compliance on the system of the entity in question? Appendix 5B – Statement of Compliance Registry Criteria (Revision 7) 8
- Can the normal operation, misoperation or malicious use of the entity's cyber assets cause a detrimental impact (e.g., by limiting the operational alternatives) on the operational reliability of an associated Balancing Authority, Generator Operator or Transmission Operator?
- Can the normal operation, misoperation, or malicious use of the entity's Protection Systems (including UFLS, UVLS, Special Protection System, Remedial Action Schemes and other Protection Systems protecting BES Facilities) cause an adverse impact on the operational reliability of any associated Balancing Authority, Generator Operator or Transmission Operator, or the automatic load shedding programs of a PC or TP (UFLS, UVLS)?"[42]

As seen by the language above, NERC identifies the material impact on the BPS through an element's ability to affect the operational state and functions performed by a BA, GOP, or TOP. A few other questions focus on distribution-enabled relaying (i.e., under frequency load shedding (UFLS) and under voltage load shedding) that DERs and DER aggregators may more strongly impact depending on feeder configuration and the specific implementation[43] of a PC's UFLS program. Many of these questions do not currently apply to OEM interactions for proprietary connections to the asset but instead deal with the element's electric impact on the BPS. Proprietary connections are allowable per 1547-2018 at the local DER interface, allowing for the DER device to be compromised and possibly leading to misoperation or malicious use if unprotected. Thus, it is important to represent the potential impact of these devices in studies that assess the performance of the BPS, including the applicable level these assets reach in NERC's

---

[41] Available here: https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix%205B.pdf

[42] Taken from the NERC Rules of Procedure Appendix 5B. Available here: https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix%205B.pdf

[43] SPIDERWG has drafted a reliability guideline on this topic, which is available here: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Recommended_Approaches_for_UFLS_Program_Design_with_Increasing_Penetrations_of_DERs.pdf

Reliability Standard CIP-002-5.1a. A thorough understanding of the interaction between DERs, DER aggregators, and utility systems is required to appropriately categorize these devices with the impact test.

BES Impact Test and Meaning

DER aggregators may potentially meet the material impact test as per the "BES Cyber Asset" definition as part of the NERC *Glossary of Terms*[44] and through the understanding of the control of assets the DER aggregator has in its system. SPIDERWG and SITES do not anticipate that any one DER outage will have the size and impact that can adversely affect the operational reliability of any associated BA, GOP, TOP, RC, or other NERC entity. Rather, the aggregate impact of DERs onto the BPS can affect the performance of the bulk system during grid disturbances. SPIDERWG has developed reliability guidelines[45] to address the modeling and verification of DERs in bulk system studies and is currently drafting guidance[46] on the studies performed that incorporate these aggregate models. Furthermore, the SITES has also identified[47] that the individual DER under malicious control has a different impact than the DER aggregator. Depending on the size[48] and control mechanisms in place, a DER aggregator may reach a level of BES impact. The SPIDERWG and SITES recommend further analysis in this area to determine the impact of a DER aggregator (or similar entity) has on the BES.

Security Standards, Frameworks, and Alternatives

Outside of the NERC CIP standards, other governmental and national labs have provided frameworks to categorize multiple aspects of a strong security posture for the electric ecosystem. Other cybersecurity forums have also provided certification, tests, and other communication protocols that enhance the efficacy of modern security controls. In some instances, these alternatives can include resilience focused projects that do not fully rely on security controls, akin to how many distribution companies have "hot swappable" equipment. Some of these alternatives include the following:

- The Cybersecurity Capability Maturity Model,[49] which is a tool for organizations to evaluate cybersecurity capabilities for IT and OT environments
- The Distributed Energy Resource Cybersecurity Framework[50] by NREL, which is a tool designed specifically to evaluate the cybersecurity posture of DERs for the U.S. federal government
- Idaho National Lab's Standards to Secure Energy Infrastructure,[51] which allows for quick searches of applicable standards or guidance material in this area
- Underwriter Laboratory Cybersecurity Assurance Program,[52] which offers a suite of tools, testing, and certifications (e.g., UL 2941[53]) to manage and apply commercially available cyber security capabilities
- Sunspec's Cybersecurity Certification Program,[54] which also seeks to certify functions for DERs, particularly for compliance to IEEE 2030.5

---

[44] Glossary of terms here: https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf

[45] The SPIDERWG reliability guidelines are available here: https://www.nerc.com/comm/Pages/Reliability-and-Security-Guidelines.aspx

[46] See SPIDERWG Work Plan, available here: https://www.nerc.com/comm/RSTC/SPIDERWG/SPIDERWG%20Work%20Plan.pdf

[47] Identified in *Cyber Security for Distributed Energy Resources and DER Aggregators*, available here: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_Cybersecurity_for%20DERs_and_DER_Aggregators.pdf

[48] For reference, the CIP-002-5.1a Medium impact threshold for generator control centers is 1,500 MW of active power resources and 1,000 MVAR of reactive power resources

[49] Available here: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

[50] Available here: https://dercf.nrel.gov/

[51] Available as part of the Office of Cybersecurity, Energy Security, and Emergency Response here: https://energyicsstandards.inl.gov/

[52] Available here: https://www.ul.com/services/ul-cybersecurity-assurance-program-ul-cap

[53] Standard available here: https://www.shopulstandards.com/ProductDetail.aspx?productId=UL2941_1_O_20230113

[54] Available here: https://sunspec.org/sunspec-cybersecurity-certification-work-group/

- Sandia National Lab's Recommendations for Distributed Energy Resource Access Control,[55] which provides a framework to minimize the risk of unauthorized access to DER systems.
- The National Institute of Standards and Technology's set of protocol[56] standards, which define information system security practices.

Many of these alternatives are self-answered questionnaires that highlight areas of improvement for an organization to build new capabilities or leverage existing technology to improve their cyber security postures. As such, SPIDERWG and SITES encourage DER owners, DER aggregators, and similar entities to leverage these more exhaustive tools in addition to the recommendations found in this paper.

Market rules may also offer an avenue for enhanced cyber security measures for DERs as they dictate the participation requirements for each participant in the energy market. It is outside the scope of this paper to evaluate particular markets for their structure or adequacy in meeting cybersecurity objectives; however, market rules that specify heightened cyber security postures for all participants may be an avenue to ensure DERs and DER aggregators maintain cyber security practices in both the IT and OT environments. ISOs and RTOs are encouraged to incorporate reliability-focused security practices in their rules such that the reliable operation of the BPS is not compromised by latent or unknown security threat by the participants of the electric market. Utilities are likewise recommended to ensure proper cyber security hygiene when integrating command and control over DERs into their distribution control centers or DERMS.[57]

Sponsored certification programs reach a sort of standardization depending on the test bed and protocol. One example from the NREL aims to provide testing and certification procedures[58] for common cyber security controls. Additionally, NREL is also working to build a framework[59] that identifies the common threats against DERs in order to standardize incident response and other key players in securing the DER landscape.

National and International Lessons Learned

Current efforts to aggregate DER control and dispatch include the PG&E VPP pilot project[60] with Tesla to leverage distribution-connected battery energy storage systems during times of high peak demand. At the time of this paper, these efforts have led to many thousands of end-users supplying a peak power output of nearly 30 MW of generation during times of high strain on the grid. Internationally, vehicle-to-grid initiatives that aggregate the ability for electric vehicles to discharge when called upon by the system operator have had some success in the European Union. One of the European Union's vehicle-to-grid VPP programs is looking to a pilot project[61] to provide short-term frequency response to grid disturbances with strong collaboration between the grid operator and the VPP operator. These pilot projects have the same structural compositions seen by DER aggregators.

---

[55] Available here: https://www.osti.gov/biblio/1765273

[56] Primarily NIST's *Security and Privacy Controls for Information Systems and Organizations*, available here: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final, and their Technical Note 2182, available here: https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2182.pdf.

[57] A DER Management System is identified in the IEEE 2030.X family of standards. Particularly 2030.11-2021, which can be found here: https://standards.ieee.org/ieee/2030.11/7259/

[58] Available here: https://www.nrel.gov/docs/fy22osti/80581.pdf

[59] Available here: https://www.nrel.gov/docs/fy20osti/75044.pdf. Other work by NREL includes supply chain concerns (https://www.nrel.gov/docs/fy23osti/84752.pdf) and measuring framework compliance by an emulated environment (https://www.nrel.gov/docs/fy23osti/84079.pdf)

[60] Information related to this pilot program can be found on PG&E's website for the Emergency Load Reduction Program. Available here: https://elrp.olivineinc.com/

[61] Information for this one particular project is available here: https://www.next-kraftwerke.com/products/balancing-energy. For this pilot, available lessons learned can be found at the integrating German utility, available here: https://www.amprion.net/

Furthermore, it is known that many cyber security recommendations, standards, and frameworks speak to a limited scope of applicable assets, threats, and known threat actors. In areas like DERs and the distribution system security landscape, many of these frameworks are vague in their applicability to the threats facing DERs, DER aggregators, and the distribution system at large. This is largely due to inherent assumptions, a lack of threat information sharing, and assumed minimal threat of distribution facilities.

Entities that lack specific threat information sharing have found that technical design specifications and framework adaptations improve the overall reliability of their system. To improve the reliability of the entire electric ecosystem, this should also include threats facing the distribution system. Current advancements in this area include specifying technical security requirements[62] that historically have not existed for DERs.

---

[62] One example of these specifications comes from NREL. Their report on functional specifications is available here: https://www.nrel.gov/docs/fy22osti/79974.pdf

Chapter 4: Conclusions and Recommendations to DER and DER Aggregators

While there are a variety of security controls available to DER aggregators and owners, some controls are better suited at the end-user device (i.e., the DER) or at the entity that controls aggregate DERs (e.g., DER aggregator or VPP). The types of security controls, types of mitigated attack, implementation notes and recommended entity for these security controls are summarized in **Table 4.1**. This table is a summary of the information contained in the above sections. Furthermore, DER aggregators implementing a DERMS all or in-part at an off-site hosting service should ensure that strong cyber security requirements are in the service agreement, including similar or greater protection than at their own premises.

Table 4.1: Security Control Recommendations

Security Control	Types of Attacks Mitigated by Proper Control Implementation	Applicable Entitles	Implementation Notes
Internal Network Security Monitoring	Phishing, Active Scanning, Gathering Victim Network or Organization Information, Malware Deployment	Der Aggregators	INSM alerts and logs may be inputs for other activities, such as automated responses, forensics, or incident response.
DER Gateways	Man in the Middle, Malware Deployment, Denial Of Service, and Replay Attacks	Der Aggregators**	DER gateways are currently under development for technical specification and may change per IEEE P1547.10 outcomes.
Remote Access Controls	Unauthorized External Remote Access, Trusted Relationship Compromises, Remote System Discovery, and Most Forms of Reconnaissance	All Entities*	DER aggregators in particular should enable strong remote access security controls on the DERs they control.
Data Management and Access Controls	Credential Harvesting or Access, Privilege Escalation, Account Manipulation; and a Broad Set of Data Deletion, Encoding, Obfuscation, or Manipulation	Der Aggregators**	These controls can also be used to mitigate privacy concerns by end-users as well as their intended security functions.
Network and Protocol Security	a Majority of Current and Future Cyber Security Threats	Der Aggregators	Certain endpoints in the chosen DER aggregator's environment may not support all desired protocols. The implementation of these controls may be software-based, specifically for cloud implemented controls.

* denotes that a DER owner's implementation of the control doesn't need to be as sophisticated as DER aggregators or utilities

** denotes that, while DER aggregators are applicable, the control may require DER owner coordination to implement

The SPIDERWG and SITES joint team has developed recommendations for the ISO/RTOs (collectively registered as BAs and RCs), DER aggregators, and DERs in order to enhance the security posture of the electric ecosystem. Cyber attacks that utilize simple social engineering or other low-level tactics can readily compromise credentials, making security controls based on credentials alone insufficient. DERs constitute a large attack surface with potentially thousands of entry points into a network, so the compromise of any one side of a communications network can allow for interconnected networks to also become compromised, potentially facilitating malware propagation and malicious actor lateral movement (e.g., DER devices, DER aggregator networks, and utility networks). With an ever increasing number of DER access points, robust security controls are high priority to ensure the security of the electric grid.

To that end, SPIDERWG and SITES jointly developed the following high-level recommendations for the ISO/RTOs:

- ISOs/RTOs should ensure that their market rules do not prohibit entities from enhancing their cyber security posture beyond a minimum level of protection.
- ISOs/RTOs should also explore and consider market rule enhancements that encourage participants to incorporate cyber security best practices while not imposing a risk to the reliable operation of the BES. This is part of proper cyber hygiene for entities.

SPIDERWG and SITES also jointly developed the following high-level recommendations for DER aggregators:

- DER aggregators should implement proper data management and access controls for its network in order to assure confidentiality of private data as well as mitigate against specific cyber attacks. DER aggregators should start by performing a privacy impact assessment[63] and implement the necessary data management and access controls identified as needed from the assessment.
- DER aggregators should implement strong network access controls, particularly for remote access, and require multi-factor authentication for remote access of their network and applications.
- DER aggregators should implement strong internal controls, such as intrusion detection systems, so they are notified of a compromise and can take proper actions to mitigate it.
- DER aggregators should ensure endpoint controls, such as through DER gateways, are deployed at DER sites where a gap exists.

Furthermore, SPIDERWG and SITES jointly developed the following high-level recommendations for DERs:

- DER owners should ensure they wipe personal information from old hardware and, to the degree possible, implement data management and access control to their network. In particular, U-DERs should implement strong access controls.
- DER owners should understand agreements with DER aggregators, including the criteria for the proper use and handling of their personal data, including data exchanged with third-parties and requirements related to the DER owner's prior consent.
- U-DERs should implement network access controls as much as possible, particularly for remote access. For programmatic remote access, public key infrastructure through a DERMS or other management system by the utility should be enabled.

State Coordination of Implementation of Recommendations

FERC Order 2222 does not specify requirements for cyber security and data privacy. Rather the order recommends that "… that RTOs/ISOs coordinate with distribution utilities and relevant electric retail regulatory authorities (e.g., state PUCs) to establish protocols for sharing metering and telemetry data, and that such protocols minimize costs and other burdens and address concerns raised with respect to privacy and cybersecurity." Due to the various jurisdictions on utility procedures and security measures, strong collaboration and coordination among transmission and distribution entities is highly recommended.

---

[63] These assessments evaluate the data exchange and storage that may potentially hold energy consumption data that infers customer behaviors or personally identifiable information. Common assessment tools also include follow-up recommendations based on the identified risk exposure in the assessment.

The overall security posture of the BPS can be impacted by the potential security risks associated with DERs or DER aggregators, and SPIDERWG and SITES recommend that DER aggregators register for NERC standards applicability when they act as BES cyber assets that can impact the reliability of the BES. The recommendations above should be coordinated with appropriate and open stakeholder engagement where the security measures and controls are agreed on for the local distribution system. These entities can assist in building the design basis threat or other risk assessment that prioritize the most effective security controls to mitigate their anticipated threats. State coordination is a high priority where DER-site-specific physical security measures are identified.

In general, the key risk considerations in this broader coordination effort[64] include data privacy for both personal and market data, data integrity among entities, and data availability.

Data Confidentiality

Per FERC Order 2222, RTOs/ISOs must revise their tariffs such that DER aggregators provide "a list of the individual resources in its aggregation, necessary information that must be submitted for individual DERS, and retain performance data for individual DERs." Entities participating in energy markets must be aware of data privacy regulations, understand the potential impact to customer privacy in the event of data-loss-events, and ensure both technical and procedural controls are implemented for data transparency and protection for consumer data. The recommended coordination should identify these and similar confidentiality requirements, especially as they relate to protecting against a widespread DER compromise.

Data Integrity

Entities should coordinate development of cyber security criteria for DER systems and communication protocols used for interoperability and data exchanges, include NIST-approved cryptographic suites and protocols to protect against data manipulation, and establish protocols to ensure adequacy of security control implementations. Testing standards for DER systems and communication protocols should also be included in the implementation of recommendations.

Data Availability

Risk assessment methodologies need to be created in order to evaluate a grid entity's role in the electric sector and the associated security control and redundancy measures these roles must adopt and maintain. These measures can account for various financial, safety, reliability, privacy considerations that result from cyber attacks against the entity's systems and data.

---

[64] Additional resources on how this participation in markets can be influenced by DER aggregators is available at here: EPRI, DER Aggregation Participation in Electricity Markets: EPRI Collaborative Forum Final Report and FERC Order 2222 Roadmap, Palo Alto, 3002020599

Chapter 5: Contributors

NERC wishes to thank the following subject matter experts for contributing to this document. NERC also wishes to thank NREL and EPRI for their contributions and review of the white paper.

Name	Entity
John Biasi	Burns and McDonnell
Dan Kopin	VELCO
Jens Boemer	EPRI
Jose Cordova	EPRI
Xavier Francia	EPRI
Abrez Mondal	EPRI
John Schmall (SPIDERWG vice chair)	ERCOT
Shayan Rizvi (SPIDERWG chair)	NPCC
Shannon Mickens	SPP
Morgan King	WECC
Nick Hatton	WECC
Sam Chanoski	INL
Karl Perman	CIP Corps
Jordan Petersen	NREL
Danish Salem	NREL
Ryan Cyar	NREL
Tom Hofstetter	NERC
Dan Goodlett	NERC
Larry Collier (SITES Coordinator)	NERC
JP Skeath (SPIDERWG Coordinator)	NERC

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Privacy and Security Impacts of DER and DER Aggregators

Joint SPIDERWG/SITES White Paper

September 2023

Background

The Federal Energy Regulatory Commission (FERC) approved Order No. 2222, which enabled Distributed Energy Resources (DERs) to participate in wholesale electric markets[1] through a Distributed Energy Resource Aggregator (~~DER Aggregator~~DER aggregator) that interfaces with the Independent System Operators (ISOs) and Regional Transmission Operators (RTOs). These ISO/RTOs are generally registered as the Balancing Authorities (BAs) and Reliability Coordinators (RCs) in their respective Interconnections. The NERC System Planning Impacts from DER Working Group (SPIDERWG) and the Security Integration and Technology Enablement Subcommittee (SITES) have both authored white papers[2] analyzing the bulk system reliability and security implications of the ~~DER Aggregator~~DER aggregator; however, no NERC industry stakeholder group has explored the technical aspects of security controls for these grid functions and their systems. This paper focuses solely on the security controls available to DER and ~~DER Aggregator~~DER aggregators and provides recommendations[3] in order to maintain the reliability of the bulk power system (BPS).~~)~~

This paper explores the technical facets of security controls available to DER and ~~DER Aggregator~~DER aggregators and provides~~provide~~ ~~an~~ examples~~examplesexample~~ of potential attacks that can be mitigated through the implementation of those security controls. It ~~will~~ also provides~~provide~~ an overview ~~on~~ of the security posture ~~of~~ for the distribution landscape (particularly for DER and ~~DER Aggregator~~DER aggregators) and provides~~provide~~ correlations to relevant NERC Standards~~, should any exist~~. The Bulk Electric System (BES) Cyber Asset 15-minute impact test is compared to DER and ~~DER Aggregator~~DER aggregators to understand their potential impact to the BPS. Further, privacy concerns are covered related to confidentiality of user data for DER owners in this electrical system as such data may be the target of a malicious actor. This paper will also provide high-level recommendations to DER and/or ~~DER Aggregator~~DER aggregators on security controls or other risk mitigation measures.

Intended Audience

Commented [JS1]: From Bill Allen:
JP and Shayan,

I have a couple comments to relay from security experts in our organization:

Good paper. Wish it had some stronger recommendations but at least the issue is getting discussed.

Some the of the high points I took away that we talk about internally:

- Need to separate the utilities from the DERs.
  - One of the concerns we have on the security side is the utilities desire to pilot partial ownership of DERs in the form of BESS and Microgrids, while still outsourcing the support opening holes in our grids.
  - This also assumes "trust relationships" between us and the DERs versus leveraging "zero trust".
- Concern with relied dependance on internet based communication and the susceptibility of cellular to interference.
  - As mentioned above, outsourced support is a major concern.
  - These DERs are outside our fiber footprints and rely heavily on commercial cellular.
- "Reliance on turnkey" solutions versus standard designs. We see the utilities going out and signing contracts for packaged solutions versus developing these inhouse which significantly impacts our abilities to monitor and support the systems and requires heavy external support.
- DERs are not like traditional distribution systems where you can roll a truck and replace broken parts with spares. These are complex ICS systems at times and need to have security at the forefront.

Commented [JS2R1]: Thank you for your comment. Strengthened slightly some of the recommendations and added a cloud security section.

Commented [JS3]: From Marc Child:
John and Shayan, cloud security issues are suspiciously absent from this document which is otherwise excellent. DERMS systems are much more likely to be cloud-based than other control systems (ex. BES). It feels worthy of a paragraph or two.

Commented [JS4R3]: Added section on DERMS.

---

[1] FERC Order 2222 is available here: https://www.ferc.gov/sites/default/files/2020-09/E-1_0.pdf

[2] The SPIDERWG white paper *BPS Reliability Perspectives for Distributed Energy Resource Aggregators* is available at https://www.nerc.com/comm/RSTC_Reliability_Guidelines/SPIDERWG_White_Paper_-_BPS_Persepectives_on_DER_Aggregator_docx.pdf and the SITES white paper *Cyber Security for Distributed Energy Resources and DER Aggregators* is available at https://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_Cybersecurity_for%20DERs_and_DER_Aggregators.pdf .

[3] This paper does not provide Compliance Implementation Guidance related to the CIP standards. Rather, security controls are presented at a high level and the functional interplay between DER, DER Aggregators, and other entities is considered in the context of security and security controls.

This paper is intended for the following NERC Registered entities, external stakeholders, and broader groups:

- Planning Coordinator (PC)
- Transmission Planner (TP)
- Transmission Operator (TOP)
- Distribution Provider (DP)
- DER owners, aggregators, and developers
- ISO/RTOS (i.e., the BAs and RCs)

This paper includes recommendations to DER owners, ~~DER Aggregator~~DER aggregators, and NERC registered entities as they assess or analyze their security and privacy-protective posture. The complexity of ~~securely managing~~managing the security and privacy of these systems is further compounded by the increasing penetration of DER. This paper is not intended to alter the DP's interconnection requirements nor to alter the electrical specifications to produce DER equipment. Rather, this paper is seeking to recommend security measures or requirements that improve the electrical ecosystem's security posture.

Definitions

To clarify terms and definitions to accurately scope what constitutes resources in a ~~DER Aggregator~~DER aggregator versus the SPIDERWG set of terms, the following main points should be noted:

~~2.~~1. The SPIDERWG definition[4] of **Distributed Energy Resource (DER)**,~~),~~ which is "any Source of Electric Power located on the Distribution system", is the preferred definition for discussing reliability concerns.
    a. This is different from the definition of DER in the FERC Order, which is "a source or sink of power that is located on the distribution system, any subsystem thereof, or behind a customer meter".[5] Namely, the reliability focused (i.e., SPIDERWG) definition focuses on generation only, while the FERC definition includes load.
    b. This is also slightly different from current discussions in Project 2022-02,[6] which is attempting to consolidate definitions ~~as to not add~~and avoid the addition of many new terms. The ~~project~~ Project 2022-02 definitions are not currently approved as of this paper.

Commented [QC5]: maybe :"managing the security and privacy of these systems"? I feel this paragraph is the overall purpose of the paper and privacy is not mentioned here

Commented [JS6R5]: change made as proposed

Commented [SM7]: What NERC documentation would house these security measures and requirements? Ie…standards, guidelines, implementation guidance

Commented [JS8R7]: Please see the recommendations section of this whitepaper for the recommended measures. Other alternatives are also listed in this paper that house cybersecurity requirements.

Commented [CJ9]: Should we include a paragraph like the one used in the BPS perspectives for DER Aggregators?

"SPIDERWG has defined "DER" to strictly refer to *sources* of electric power on the distribution system (not inclusive of load resources). On the other hand, the definition presented in FERC Order No. 2222 defines DER as *any resource* located on the distribution system. The distinct difference between definitions is that the FERC definition is inclusive of demand response and load elements; whereas the SPIDERWG working definition excludes demand response as it is not considered a source of power. Rather, it is considered a load modifier in the set of SPIDERWG terms as it modifies load and energy consumption rather than being a source of power."

Commented [JS10R9]: The way it currently flows seems ok. Improved footnote to aid in clarity for the source.

Commented [QC11]: should this be briefly explained or at least cited?

Commented [JS12R11]: Cited page

Commented [QC13]: is this referring to project 2022-02? If so, need to clarify

Commented [JS14R13]: clarified

Commented [MA15]: Does this definition include energy storage (specially the charging aspect)? Not very clear

Commented [CJ16R15]: DER definition includes a Source of Electric Power which is defined as
Resources that inject or exchange power (e.g., Distributed Generation and Energy Storage Facilities)

Commented [JS17R15]: Added clarity to footnote

---

[4] The SPIDERWG terms and definitions, including DER, Source of Electric Power, and Distribution System are available here: https://www.nerc.com/comm/RSTC/SPIDERWG/SPIDERWG%20Terms%20and%20Definitions%20Working%20Document.pdf

[5] Taken from FERC Order 2222 on page 85. Available here: https://www.ferc.gov/sites/default/files/2020-09/E-1_0.pdf

[6] Project 2022-02 website is located here: https://www.nerc.com/pa/Stand/Pages/Project2022-02ModificationstoTPL-001-5-1andMOD-032-1.aspx

~~3.~~2. FERC Order 2222 introduces the definition of **DER a~~A~~ggregator**, which for this paper is the entity[7] that controls the aggregation of generation (i.e., DER) and load end-use devices.

   a. The **DER a~~A~~ggregator** ~~has~~ may have control over both load and generation and it ~~can~~ may control existing Demand Response programs.

Commented [SM18]: Should the term "DER Aggregator" be capitalize. It's not defined in the NERC Glossary of terms. I'm recommending lower casing the term. This recommendation would align with the format in IEEE 2800

Commented [JS19R18]: Change made as proposed

~~4.~~3. Both definitions include ~~both~~ i~~I~~**nverter-b~~B~~ased ~~R~~resources (IBR)** and non-IBR generation. For example, both a 1 MW Solar PV plant as well as a 500 kW steam cogeneration facility would both be DERs, assuming both are distribution connected.

Commented [SM20]: Should the term "Inverter-Based Resources (IBR)" be capitalize. It's not defined in the NERC Glossary of terms. I'm recommending lower casing the term. This recommendation would align with the format in IEEE 2800

Commented [JS21R20]: Made as proposed

~~5. DER Aggregator~~DER aggregators’ **DER Management System (DERMS)** and **Virtual Power Plants’ (VPP)** control schemes will likely have ~~a~~ different communications architecture.[8] For this paper, the ~~architecture~~ terms ~~of DER Aggregator~~DER aggregators, VPP~~s~~, and utility systems that manage the control of DER are equivalent and recommendations to a DER aggregator apply to these entities as well. However, their specific architectures may present different attack surfaces to be evaluated.~~consideredin scope. equivalent.~~

Commented [SB22]: I'm not sure that "equivalent" is the right word here to convey the intended meaning. Certainly, from both performance and security perspectives, different communication architectures are not "equivalent". For example, a vendor aggregator system that routes via world-wide-web through a foreign country is in no way similar to an isolated local system with small attack surface.

Commented [JS23R22]: Altered language a bit. Goal is the applicability is the same. Agree architecture differences can pose a differing attack surface.

This paper uses the SPIDERWG set of definitions ~~as this is a~~ because this paper is a reliability focused technical discussion of the privacy and security impacts of DER and ~~DER Aggregator~~DER aggregators. In instances where the load portion of a ~~DER Aggregator~~DER aggregator is relevant, it will be called out as such (e.g., ~~in~~ using terms like “DER and load”).

IEEE 1547-2018

Commented [CR24]: Recommend adding a section below this detailing UL 2941

Commented [JS25R24]: Added section on UL2941

The ~~recent~~ latest update to IEEE 1547-2018[9] makes it possible for the utility, or any other entity, to deploy DER management systems (DERMS) and cohesively monitor and manage the diverse mix of DER technologies[10] and ~~manufacturers~~ brands being deployed today. Utilities and third-party aggregators are deploying DERMS, making them an integral part of system operations. However, the large and diverse number of ~~diverse mix~~DERs, their evolving capabilities, as well as continuous interconnection and ~~retirement, pose~~retirement, pose significant challenges to security and reliability of the DER ecosystem. Standardization efforts like IEEE 1547-2018 make DER integration practical by keeping DER operational functions simple and leaving more complex operational functions to the control and integration systems (i.e., DERMS or VPP). The standard also only dictates the communication protocols and intentionally left cybersecurity out of scope.

Commented [DJ26]: May be important to note that this standard only dictates communications protocols and specifically/intentionally left cybersecurity out of scope

Commented [JS27R26]: added

UL Solutions Standard 2941

UL Solutions announced the publication of UL 2941,[11] the *Outline of Investigation for Cybersecurity of Distributed Energy and Inverter-Based Resources*, developed in cooperation with National Renewable

---

[7] Further, there are various names for the entity that controls and aggregates DER outside of the DER Aggregator. Examples include Virtual Power Plant (VPP) or emergency load reduction programs (excluded Demand Response). For this paper, DER Aggregator and these other entities are synonymous as they functionally aggregate DER (i.e., generation) on the distribution system.

[8] Primarily that utility implemented DERMS will likely have direct control and on-premises security controls while VPPs are more inclined to utilize cloud solutions for their security controls.

[9] IEEE 1547-2018 is available here: https://standards.ieee.org/standard/1547-2018.html

[10] E.g., Battery Energy Storage, Solar Photovoltaic, or synchronous DERs.

[11] Available here: https://www.shopulstandards.com/ProductDetail.aspx?productId=UL2941_1_O_20230113

Energy Laboratory (NREL). The requirements will provide a single unified approach for testing and certification of DERs in advance of the anticipated rapid deployment.[12]

These new requirements prioritize cybersecurity enhancements for power systems technologies, particular for inverter-based resources and DERs. UL 2941 is anticipated to promote the cybersecurity designed into the equipment of new inverter-based resources (IBR) and distributed energy resource (DER) systems.[13] The standard outlines various testing needed to pass in order to achieve certification.

~~Jose to provide text~~

Regional Autonomy and Network Architecture

In the context of DER aggregator~~ions~~s, security includes availability. The electric power system is designed with the ability for given regions to isolate from surrounding regions for reliability purposes. For example, it may be possible for a given balancing authority to maintain service within its footprint when a blackout is occurring in adjacent areas. As DER become more common, there is increased potential for power system operability at local levels.

For regional power systems to operate, both the energy and the communication systems involved must be available. If ~~aggregations of~~ DER play a role of any significance, then the communication networks that manage DER must remain functional. This can be an issue for some communication architectures.~~ As illustrated in Figure 0-3, g~~ Gridgrid equipment is integrated via networks that remain available when the local ~~region~~area ~~(green shaded)~~ is operating. -But DER may not be available, even though they lie inside the region~~,~~ if they are managed via systems or networks in some other location where operation has been interrupted. For example, if ~~an aggregation of battery units is critical to grid operation~~a DER aggregator operates DER in the Western Interconnection, then it isn't practical for the associated control system to have dependencies in a different ~~region~~system such as the Eastern Interconnection.

~~ or country.~~

---

[12] https://www.nrel.gov/docs/fy23osti/84709.pdf

[13] https://www.ul.com/news/ul-solutions-and-nrel-announce-distributed-energy-and-inverter-based-resources-cybersecurity

~~Figure 0-3~~

Commented [JS28]: moved as this was background from added content from edits. Also edited as this seemed to be copied and lost context. Deleted figure as text description was sufficient to describe.

Security Controls Available to DER and DER Aggregators

The draft *IEEE P1547.3 Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems*[14], currently out for industry comments, provides guidance and recommendations for cybersecurity practices and controls to ensure secure communication of DER protocols (e.g., IEEE Std 1815, IEEE Std 2030.5, SunSpec Modbus, and IEC 61850) specified in the IEEE 1547-2018.

Commented [SM29]: Is there a need to explain the difference between a guide and standard in the IEEE development process?

Commented [JS30R29]: Not in this context. This is discussing the controls available and not what they're subject to.

The ~~1547~~P1547.3 guide includes considerations relating to the following cybersecurity topics:

- Risk assessment and management~~,~~
- Communication network engineering~~,~~
- Access control~~,~~
- Data security~~,~~
- Security management~~,~~
- Coping and recovering from security events~~,~~
- Testing and Commissioning for Cybersecurity and Conformance with the IEEE ~~1547~~P1547.3.

Though not exhaustive, the following sections provide a ~~high level~~high-level overview of security controls available to DER devices and installation sites, ~~or to DER Aggregator~~DER aggregators and their control systems. Figure 0-1:2~~Figure 1~~ graphically shows the new communication pathways (in red) introduced with the addition of the ~~DER Aggregator~~DER aggregator to the electric ecosystem. Although their equipment,

Formatted: Cross Reference Char

---

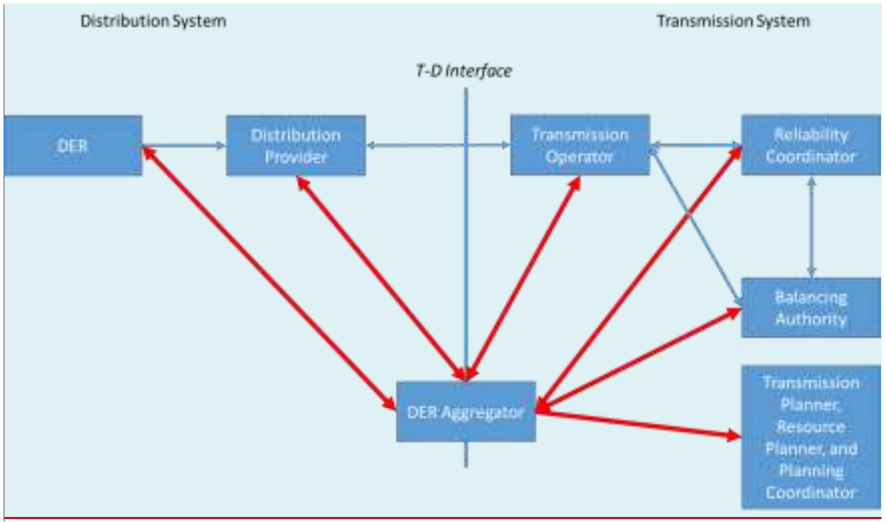
[14] IEEE P1547.3 website: https://sagroups.ieee.org/scc21/standards/ieee-std-1547-3-2007-revision-in-progress/

such as DER gateways, may be at the DER site, t~~T~~he ~~DER Aggregator~~DER aggregator logically sits at the T-D Interface and may communicate~~s~~ its DER control capabilities to the ISOs and RTOs (i.e., the BAs and RCs), who may then determine the utilization of those capabilities~~.~~ in coordination with distribution system operators~~DSOs~~.~~.~~ ~~Additionally, the~~The ~~DER Aggregator~~DER aggregator issues operating commands to the DERs it manages, as well as communicates necessary information with the additional key entities in the ecosystem. These new communication pathways necessitate a thorough understanding of associated ~~security~~ risks and the available mitigating controls essential to protecting data ~~integrity~~security, privacy, and grid reliability.

Commented [DG31]: Not defined

Commented [QC32]: just integrity? Maybe replace with security here

Commented [JS33R32]: made as proposed



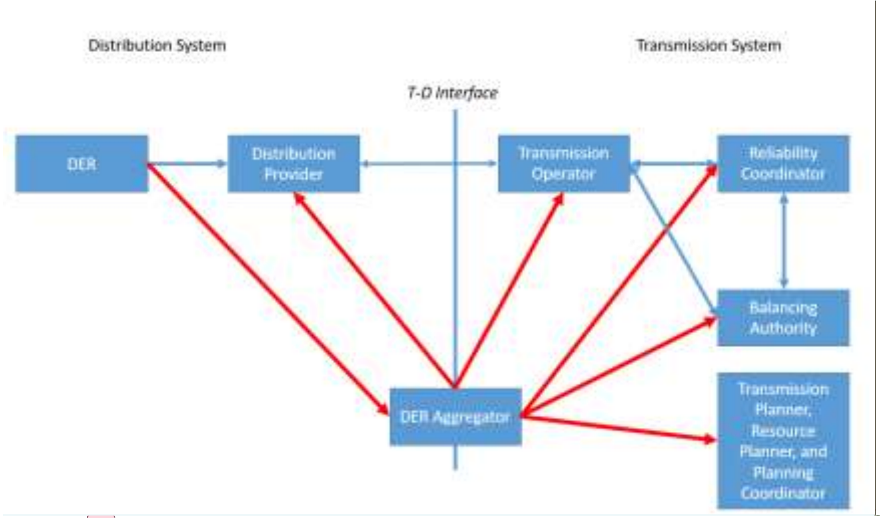


Figure ~~1:~~0-1~~1~~:2~~1:~~: High-level Diagram of Added Communication for DER, ~~DER Aggregator~~DER aggregators, and the BES[15]

Commented [CJ34]: Add double-headed arrows as communication should go both ways

Commented [JS35R34]: Replaced for double headed arrows.

Commented [SB36]: I'm not clear on the meaning of the direction of the arrows. For example, DER aggregators must communicate "to" DERs to control them. Some others like aggregator-to-DSO
might be better as two-way arrows.

Is there a reason that it's called "distribution provider" but "Transmission operator"? I'd suggest calling both operators (TSO and DSO).

Commented [SB37]: I'm not clear on the meaning of the direction of the arrows. For example, DER aggregators must communicate "to" DERs to control them. Some others like aggregator-to-DSO might be better as two-way arrows.

Is there a reason that it's called "distribution provider" but "Transmission operator"? I'd suggest calling both operators (TSO and DSO).

Commented [JS38R37]: Distribution Provider is the NERC terminology best used for that entity. Transmission Operator further is a NERC defined term here.

Commented [JS39]: Figure 1 should indicate which communications (Red Arrows) are bi-directional. For example, the DER Aggregator issues operating commands to the DER and receives indication of DER operation. Should communications with TOP, RC, and BA also be bi-directional?

Commented [JS40R39]: All were intended to be bidirectional for monitoring and sending dispatch sending statuses etc.

Formatted: Space After: 0 pt

Network and Protocol Security

---

[15] Note that attacks scenarios can target communications outside of those highlighted in the figure. For instance, Original Equipment Manufacturer to DER communication as well as DER directly to the RCs or BAs.

DER, ~~DER Aggregator~~DER aggregators, and utility networks should be separated based on ownership, control capabilities, and trust relationships within specific implementations. The increased attack surface stemming from the connection of numerous DERs demands network architectures[16] that do not rely on implicit trust relationships. In the event of a single device or entire network segment compromise, proper network segmentation and additional security controls should ensure the continued operation of other segments.

Securely designed network architecture for DERs and ~~DER Aggregator~~DER aggregators may include the following:

- **Demilitarized Zones (DMZ), subnets, and VLANs**: These logical network segments isolate sensitive or critical systems from other parts of the networks, establishing security zones ~~by~~ based on criticality of assets or operations, and limiting unauthorized access and potential damage from cyberattacks.
- **Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS):** These systems enable comprehensive visibility into network traffic, through the monitoring and detection of suspicious activity or potential threats. ~~Actively~~ Passively and continuously scanning and analyzing network traffic for known CVEs and abnormal patterns identifies and prevents potential cyber threats, enhancing overall network security. This type of technology can be deployed ~~at~~ in the ~~perimeter~~ DMZ of the network to segment operational networks from business networks, ~~for border protection or~~ in and between subnets and VLANs ~~internal to the network~~ for "East-West" protection.
- **Absence of implicit trust relationships:** Network architectures should be designed without assumptions of trust between connected devices or systems, minimizing the potential for unauthorized access and lateral movement of attackers within the network.
- **Secure network boundaries:** Firewalls control incoming and outgoing network traffic based on predetermined rules, while data diodes ensure one-way data flow, adding layers of protection to network boundaries.
- **Strong encryption:** Implementing advanced encryption algorithms, such as Advanced Encryption Standard (AES),[17]~~,~~ Elliptic Curve Cryptography (ECC),~~)~~ and Rivest-Shamir-Adleman (RSA),[18]~~,~~ ensures the confidentiality and integrity of sensitive data transmitted across networks.
- **Secure Protocols:** Utilize communication protocols with built-in security features to ensure the safe and reliable exchange of information between DER devices and control systems, such as DNP3-SA,[19] which incorporates robust authentication, encryption, forward-secrecy[20], and non-repudiation, providing a strong foundation for secure DER communication.

---

[16] Including architectures that are centrally-managed and contain source-traceable components. Implicit trust can be designed out of an architecture and implicit trust should not be assumed even when an entity owns all components of the architecture.

[17] 100 bits or above should be used to be secure.

[18] 2,048 bits or above should be used to be secure.

[19] Other secure protocols exist. This is used as an example of one such secure protocol.

[20] Forward secrecy methods implemented within protocols ensures that past communication sessions cannot be decrypted if either session or private keys are compromised.

Commented [SB41]: This comment, together with the related bullet below, may be confusing to some readers in that it obscures the difference between components that are traced and directly manageable by the provider of a given segment of the overall system vs the hardware that is not traced or manageable.

Zero-trust architectures show how, even if your company manufactures all the elements of a given system, you can design to not implicitly trust the elements. In this way, your system may be less affected if a given product ends up compromised, for example due to something unexpected that was inserted in the supply chain.

What it does not mean is that all equipment is equally manageable or of equal risk (e.g. your own vs something bought on Alibaba).

For example: an aggregation system design should include centrally-manageable, source-traceable gateways, but the aggregator should not implicitly trust their own gateways.

Commented [JS42R41]: Added footnote

Commented [XF43]: One set of controls that seems to be missing are a couple of bullets addressing network availability. In some aspects of the communication architecture, network load balancers may be required for DERMS or VPPs, to handle numerous connection sessions across a large swath of DERs. Network-based Denial of Service protection may also be warranted to protect from Botnet/DDoS type of attacks.

Commented [JS44R43]: No change made based on this comment.

Commented [DJ45]: Where does secure remote access fit? Does this deserve its own bullet?

Commented [SB46R45]: This is an important catch. For DER use cases, denial of service can be as severe as any direct manipulation. In other words, no need to hack the device or network, just block it.

Commented [JS47R45]: No change made based on this comment. See section on remote access below

Commented [DJ48]: This terminology is becoming outdated in the market, we are seeing continuous monitoring tools captured as "vulnerability and threat detection solutions"

Commented [JS49R48]: Thank you for your comment. No change made

Commented [QC50]: should you also mention at least some of the other protocols listed above (e.g., IEEE Std 1815, IEEE Std 2030.5, SunSpec Modbus, and IEC 61850) or are you implying that DNP3-SA is the most secure protocol?

Commented [JS51R50]: Added footnote. This is just one example. Not trying to say most versus least secure.

- **Authentication:** Robust authentication mechanisms, such as digital certificates, Public Key Infrastructure (PKI), and Phishing-Resistant Multi-Factor Authentication (MFA), validate the identities of devices and users. ~~, reducing unauthorized access.~~
- **Authorization:** Implementing access control policies based on the 'least privilege' principle ensures that users and devices have the minimum necessary access rights, limiting the potential impact of compromised credentials.
- **Virtual Private Networks (VPN):** VPNs create secure, encrypted connections over public networks (i.e., the internet), protecting data transmission from eavesdropping and tampering.
- **Efficient logging and alerting:** Security Information and Event Management (SIEM) systems collect, analyze, and correlate log data from various network devices, generating alerts for potential security incidents and facilitating timely response.
- **Hardened networking equipment:** Applying Security Technical Implementation Guides (STIGs) ~~or Original Equipment Manufacturer (OEM)~~ recommendations ensures that networking equipment adheres to industry-standard security practices, reducing vulnerabilities and attack surfaces.

Besides isolating networks based on trust relationships and ownership, ~~DER Aggregator~~DER aggregator and utility networks should also be segregated within their internal networks (e.g., isolating corporate networks from industrial control systems). ~~Actual architectural implementations~~Implementations and specific security controls will depend on the use cases for a given DERMS. ~~These~~ Isolated networks can range from decentralized VPP architectures, centralized distribution utility DERMS, or hybrid implementations. In addition, these ~~industrial control system (ICS)~~ networks should be securely segmented from other networks including corporate networks. Insufficiently segmented networks with weak or lax security controls could enable cyberattacks to spread across multiple systems and network segments. DER endpoints,[21] being the most vulnerable links in these networked systems, present a higher risk of targeted attacks. This includes DERs and DER gateways~~DER endpoint sites, including DERs and DER gateways~~~~DER endpoints, being the most vulnerable links in these networked systems, are likely to account for the majority of attack vectors~~. **Figure 3**~~**Figure 2**~~ shows an example network architecture of a DER managing entity controlling both small-~~-~~scale DER and utility level DER. The figure highlights the effective use of network segmentation and firewalls to establish security zones, providing network boundaries to deploy further security controls.

Commented [KM52]: Consider changing to either 'to prevent unauthorized access.' or to 'to mitigate unauthorized access.' Actually, to be consistent with all the other controls consider just removing the 'why' and put a period after 'users.'

Commented [JS53R52]: Made as proposed

Commented [SB54]: This doesn't sound right. "OEM recommendations" is undefined …could be anything and doesn't ensure anything.

Commented [MA55R54]: Agree that "OEM recommendations" may be anything at the manufacturer's discretion and may not be vetted

Commented [JS56R54]: deleted

Commented [KM57]: Consider removing the word 'Actual' and change to -

'Implementations and specific security controls may depend on the use cases for a given DERMS.'

Commented [JS58R57]: Made as proposed

Commented [KM59]: Consider changing to 'Isolated networks'….

Commented [JS60R59]: Made as proposed

Commented [CR61]: Could describe more.

Commented [QC62R61]: perhaps one additional clarification sentence on why endpoints are the most vulnerable links

Commented [JS63R61]: added footnote

Commented [KM64]: DER endpoints, being the most vulnerable links in these networked systems, present a higher risk of targeted attacks.

Commented [JS65R64]: Made as proposed

Formatted: Cross Reference Char

---

[21] Endpoints of a security system are where the "door meets the outside" for any given system. These are access points designed in system architecture and are frequently targeted by malicious actors. See here for a panel that discusses more of the reasons why endpoints are vulnerable: https://webinars.govtech.com/Closing-the-Endpoint-Security-Gap-in-State-and-Local-Government-102979.html#:~:text=According%20to%20intelligence%20firm%20IDC,and%20administrative%20passwords%2C%20and%20more.

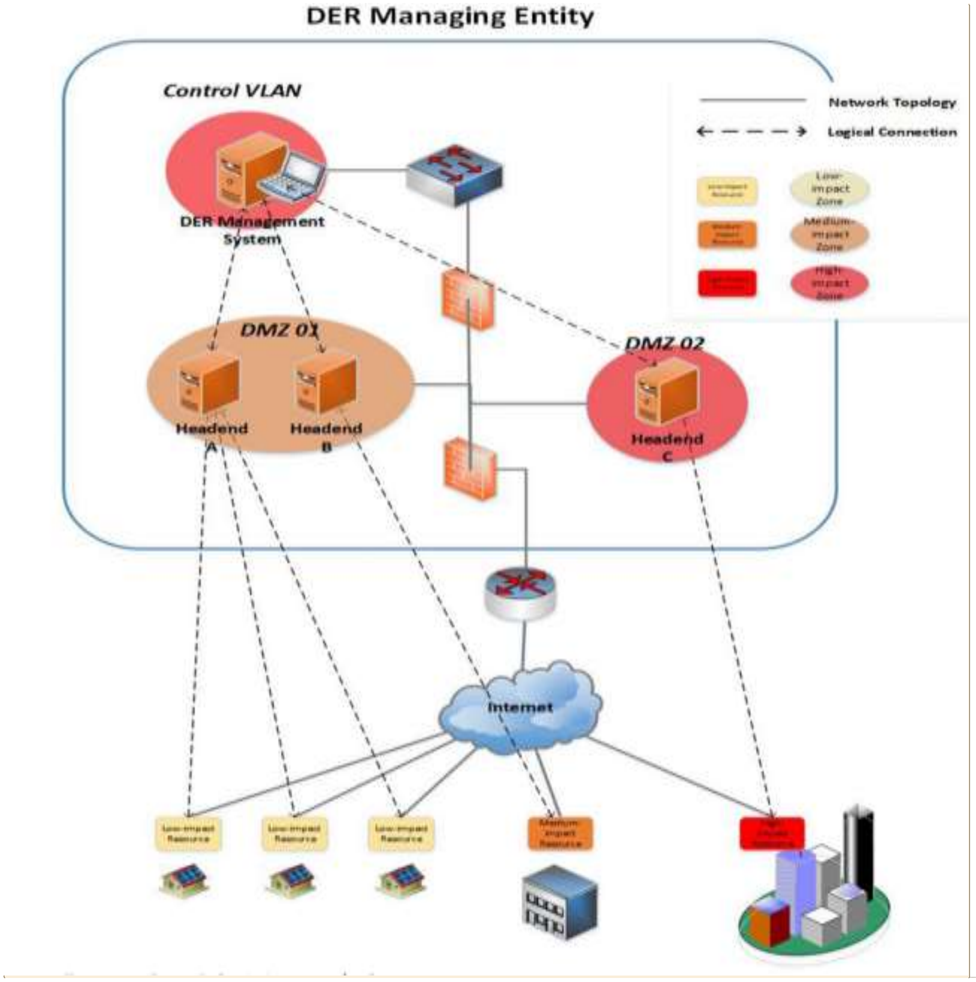


Figure 3~~2~~: Example DER Managing Utility Architecture [Source: EPRI]

In general, network and protocol security are~~is~~ fundamental to proper cybersecurity practices. As such, the types of threats and adversary tactics they mitigate are diverse and numerous.

Internal Network Security Monitoring

Commented [SB66]: Three comments on this drawing:

1. Is it necessary to label as the "Internet" rather than calling it the "Network" or "DER aggregation network"?

2. What is the difference in the solid vs dashed lines? Is the implication that there are two comm pathways from the aggregator to the edge devices?

3. To reflect what is done in practice, we could make an edit to this illustration to show the gateways just above the DER at the system edge.

4. Need larger font sizes.

Commented [JS67R66]: Cannot update as source figure unavailable from EPRI contributors. Increased size to try and improve readability

Formatted: Centered

Commented [XF68]: One important aspect of this architecture is that it recognizes different impact thresholds of a DER warrant isolation within different network segments - not sure if that is explained in the text preceding this image. It doesn't just stop at network segmentation - more advanced or robust security controls may be warranted for "high-impact" DER vs "low-impact" - the required set of security controls should usually be commensurate to the level of risk/impact of the DER or groups of DER. Currently, there is no criteria or guidelines on how to qualify high vs low impact DER and the associated security controls for each category. Reading further down, the issue of "aggregate" impact to BES is identified discussed.

Commented [JS69R68]: Thank you, this paper discusses this in the NERC Reliability Standards section

Commented [KM70]: are

Commented [JS71R70]: Change made as proposed

Formatted: Normal

Internal network security monitoring (INSM) controls are available for all networks involved, potentially includingowners of the DER ~~owner's~~ network,[22] the ~~DER Aggregator~~DER aggregator's network, a ~~utilities~~utility'~~s~~~~iesutilities~~ network, ~~and~~ or an OEM's network. INSM monitors the traffic flowing internal ~~to~~ throughout the network and provides alerts when suspect traffic is detected~~ and takes action to mitigate the threat~~. These ~~actions included~~solutions include network mapping, vulnerability management, anomaly detection,~~edincluded~~ logging and alerting when malicious traffic is detected. Some INSM implementation may also block network communications to and from suspected compromised nodes. Proper patching and updates to malicious code signatures or heuristic detection schemes is critical to assure effectiveness of these network-~~-~~based security controls.

Monitoring and logging ~~controls~~ are a prerequisite for any automated prevention or response-~~–~~based controls including access control lists (ACL), endpoint security, and security orchestration tools. In addition, the monitoring controls and their associated logs and reports facilitate security event triage and are a key component[23] of security incident response activities. Their monitoring and alert data can also be piped to SIEM solutions for SOC analysts and/or managed by MSSP providers.

Complete INSM solutions would be implemented for ~~full~~ greater network visibility, but limitations in architecture, bandwidth~~,~~ or device capabilities may preclude the monitoring of 100% of all network segments. The monitoring described here is analogous to the current and voltage relaying equipment[24] typically found on the electrical monitoring equipment in substations; however, these controls can take some automated action to mitigate against specific traffic. The following malicious activities can typically be detected by successful implementations of INSM~~internal network security monitoring~~:

- Active s~~S~~canning of networks by malicious actors
- Lateral movement between internal network nodes such as servers and workstations, DER endpoints, etc.
- Download of known malware
- Command and control traffic (C^2)
- Communications parameters and malformed packets
- New devices connecting to networks
- Weak and cleartext passwords
- Appliance usage and health logs

Commented [CR72]: What examples of logging controls fall under this?

Commented [JS73R72]: Clarified to reduce control as specific solutions weren't the focus but the broad category.

Commented [XF74]: In this footnote, we may want to specify the requirement pertains to Medium Impact assets and control centers in the bulk electric system, while identifying which CIP Standard.

Commented [JS75R74]: Added clarity

Commented [KM76]: Should we use 'greater'

Commented [JS77R76]: Change made as proposed

---

[22] It is not expected that residential DER owners would implement advanced controls beyond the default configuration at the time of their DER installation

[23] Due to their pivotal nature, these controls ~~are~~ will be required for ~~Medium H~~highHigh impact ~~or higher control centers~~or ~~M~~mediumMedium impact with external routable connectivity control centers in the NERC CIP standards per FERC Order 887. Text available here: https://www.ferc.gov/media/e-1-rm22-3-000

[24] As substation circuit breakers requires the voltage and current waveforms in order to isolate faults from the system. As such, more complex security solutions require monitoring and logging to perform their objective.

- Threat intelligence indicators of compromise (~~i.e.~~e.g., malicious IP addresses)

In general, INSM defends against internal reconnaissance, lateral movement within the network, and malware deployment~~.~~ to reduce the severity from incidents and compromise.~~.~~ Additionally, should a malicious actor compromise a DER or ~~DER Aggregator~~DER aggregator network, INSM may be able to detect outbound command and control communications which is a prerequisite for a coordinated attack utilizing many compromised DER devices.

Formatted: Indent: Left: 0"

Interactive Remote Access Controls

Physical access to the DER site by the utility or ~~DER Aggregator~~DER aggregator is typically unlikely outside of routine meter reads and similar calls. Consequently, DER gateway communication interfaces will need to facilitate remote access capability to perform routine patching, firmware updates, or even the altering inverter settings. Any remote access[25], and the communications network required to facilitate it, introduces a credible attack vector to the DER, gateway, and ~~DER Aggregator~~DER aggregator ecosystem. ~~Non-existent~~ The absence of security controls, improperly configured and maintained security controls, ~~and~~ or vulnerabilities at the DER ~~device~~ site ~~level~~ or within a ~~DER Aggregator~~DER aggregator's network could be exploited. Securely implemented and maintained remote access ~~implementations are~~ is critical for ~~DER Aggregator~~DER aggregators, utilities, and OEMs to ~~be able to~~ service and manage DERs.

Commented [QC78]: could use additional small clarification on why this is unlikely. May seem obvious, but consider explaining why briefly

Commented [JS79R78]: added some context.

Commented [KM80]: Seems duplicative as the sentence starts with 'Securely implemented…'

Commented [JS81R80]: Made as proposed

Remote access may require software and certain functionality on both sides of the communication ~~stream~~link. Thus, security controls may exist on the utility network, ~~DER Aggregator~~DER aggregator network, ~~and / or~~or on the DER device or DER~~ER~~ gateway in order to provide remote access capability in a secure manner. A simple, ~~and~~ but inadequate, form of a security control are authentication credentials.[26] ~~; however,~~ M~~<m~~ore sophisticated remote access control mechanisms are needed. Secure remote access technologies include:

Commented [KM82]: Link?

Commented [JS83R82]: Change made as proposed

Commented [CR84]: Added footnote

Commented [JS85R84]: Made as proposed

- Virtual Private Networks (VPNs) using encrypted tunnels for network traffic
- Network Access Controls limiting device connections to authorized and accessed[27] devices
- Phishing-Resistant Multi-Factor Authentication (MFA)[28] for interactive remote access
- Certificate based authentication for programmatic application access or system-to-system access
- Zero Trust architectures requiring constant re-authentication and re-authorization
- Secure protocols

---

[25] Programmatic or interactive

[26] Another mitigation example is adding a timeout session of remote access.

[27] Assessed in this context means assessing the security posture of the device prior to it being allowed access to network resources. Security posture assessment may include firmware patch level, antivirus version, hardening level, MAC address, or other criteria used to assess the security 'health' of the device.

[28] *Implementing Phishing-Resistant MFA*. CISA: October 2022. https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

Formatted: Font: Italic

These ~~components~~ methods are of ~~high priority~~essential for securing remote access, a high demand function for our current digitalized landscape. With an increasing ~~amount~~ number of access points through remote DER connections, secure networks are paramount to facilitating DER adoption and management through DER aggregator and utility systems. While the implementation and specific functionality of a technology will determine the vulnerability to ~~specific~~ particular threats and attacks, secure remote access implementations can generally mitigate the following types of malicious activities:

- Unauthorized external remote access
- Man-in-the-middle attacks
- Remote system discovery and reconnaissance
- Compromised trust relationships

Any security controls improperly configured or unpatched systems ~~not patched~~ for vulnerabilities may allow attackers to circumvent remote access controls~~ to be circumvented~~. Thus, the above mitigations support proper cyber-hygiene and a defense-in-depth approach. Both are~~is~~ ~~critical~~ important to balance the need for remote access with the security risk~~.~~.~~ such access brings~~.

~~Regional Autonomy and Network Architecture~~

~~In the context of DER aggregations, security includes availability. The electric power system is designed with ability for given regions to isolate from surrounding regions for reliability purposes. For example, it may be possible for a given balancing authority to maintain service within its footprint when a blackout is occurring in adjacent areas. As DER become more common, there is increased potential for power system operability at local levels.~~

~~For regional power systems to operate, both the energy and the communication systems involved must be available. If aggregations of DER play a role of any significance, then the communication networks that manage DER must remain functional. This can be an issue for some communication architectures. As illustrated in Figure 0-3, grid equipment is integrated via networks that remain available when the local region (green shaded) is operating. But DER may not be available, even though they lie inside the region, if they are managed via systems or networks in some other location where operation has been interrupted. For example, if an aggregation of battery units is critical to grid operation, then it isn't practical for the associated control system to have dependencies in a different region or country.~~

Commented [KM86]: Methods?

Commented [JS87R86]: Made as proposed

Commented [KM88]: Essential?

Commented [JS89R88]: Made as proposed

Commented [QC90]: you don't describe what either of these terms would entail (might seem obvious, but it's not described for the reader)-- consider revising to say something like the above mitigations support proper cyber-hygiene and a defense-in-depth approach

Commented [JS91R90]: change made as proposed

Commented [KM92]: Consider either removing 'such assess brings.' and have a period at the end of risk. Or how about the following -

'to ensure remote access controls are commensurate with the security risks.'

Commented [JS93R92]: Change made as proposed

Formatted: Justified

Field Code Changed

~~**Figure 0-3**~~

Data Management and Access Controls

Data, particularly at the ~~DER Aggregator~~DER aggregator level, can ~~reach extreme quantities~~scale exponentially. Data management policies, which address storage, transit, use, and retention measures are essential to ensuring establishing a holistic data management program.[29] ~~Data management policies, including storage, use, transit, and retention measures need to be in place. This is where d~~Data~~data~~ management and access controls ~~aid~~ ~~in securing~~secure the access and management functions of data. ~~of corporate data~~. Applied to DER and ~~DER Aggregator~~DER aggregators, these controls limit the credentials of who can read, write, and transfer data from a particular entities network. At the DER device level, these functions are broad per 1547-2018, particularly Clause 10 language that allows for a broad read, write, and transfer capabilities inherent ~~built into~~~~in to~~~~into the~~in the DER equipment itself. Other device standards, like UL2941 are more specific in their requirement language for data storage and data transit. As stated ~~in sections~~ above, 1547-2018 requires that DER support necessary monitoring and management at the local interface and does not specify~~inherently apply~~ cybersecurity ~~protections~~ at this ~~local DER network~~interface.~~, so~~With this,~~, so~~ ~~DER Aggregator~~DER aggregators and DER owners ~~would~~ need to implement these cybersecurity controls on their respective networks.

The controls themselves reside in the privileges granted to users ~~in order~~ to read, write, extract, and otherwise alter the data on the DER, ~~DER Aggregator~~DER aggregator, or other entity's network. ~~Good security controls in this area also deal with~~ Best practice security controls include storage, extraction, and deletion policies for data. These practices are~~is~~ ~~is~~ particularly useful when exchanging equipment at the ~~DER Aggregator~~DER aggregator level that may have private information stored about the DER it controls, or even for DER owners that exchange devices to wipe the ~~confidential~~ private information stored locally ~~concerning the local DER network~~. Effective implementations ~~enhance~~ ensure the security and privacy of data, as well as mitigate against IT sourced attacks on OT equipment in this ~~space~~environment. Specific attacks mitigated by data management and access controls could include:

Commented [KM94]: Can scale exponentially.

Commented [JS95R94]: Change made as proposed

Commented [KM96]: Data management policies, which address storage, transit, use, and retention measures are essential to ensuring establishing a wholistic data management program.

Commented [JS97R96]: Change made as proposed

Commented [KM98]: Not clear on the context of this sentence.

Commented [JS99R98]: clarified

Commented [CR100]: In UL 2941 requirements are more specific about data in transit and data stored on device.

Commented [JS101R100]: Added sentence

Commented [SB102]: Does the responsibility lie with the aggregator, not the DER owner.

Commented [XF103R102]: A footnote may be required here to acknowledge that most DER owners may not have the cyber security maturity or knowledge to adequately address cyber. Likely this responsibility will be offloaded to a managed services or perhaps the DER manufacturer/OEM. Reading further down, there is a sentence acknowledging this fact in the R-DER vs. U-DER.

Commented [MOU104]: Could this section include a basic comment on cloud security if data is stored in cloud for DER or is that out of scope for the goal of this paper?

Commented [JS105R104]: Added footnote on the concept here and added a section later.

Commented [KM106]: Best practice security controls include storage extraction, ……

Commented [JS107R106]: Change made as proposed

Commented [CR108]: Recommend discussing device decommissioning processes or factory resets here on a policy level instead of just leaving as a deletion policy.

Commented [QC109R108]: Also, 'good security controls' is subjective and should be clarified-- perhaps instead best practice?

Commented [QC110]: what is particularly useful? needs clarification

Commented [JS111R110]: clarified

Commented [KM112]: We use confidential information in the same sentence so should we be consistent and call it confidential information here too?

Commented [JS113R112]: Altered to private

Commented [SB114]: I don't understand what this is referring to. The DER, per 1547-2018, does not have information regarding the DER network.

Commented [JS115R114]: Altered sentence.

Commented [KM116]: ensure

Commented [JS117R116]: made as proposed

Commented [KM118]: change made as proposed

---

[29] Some data management policies allow for off-site, on-site, or hybrid approaches to manage data. Cloud security practices are important once data management and access controls include off-site or hybrid data management solutions.

- Credential Harvesting or Access
- Privilege Escalation
- Account Manipulation
- Data deletion, encoding, obfuscation, or manipulation
- Cryptographic (private) key exfiltration

Data management controls can further mitigate against data exfiltration or ransomware by a malicious actor. Privilege escalation is a common technique in the cyber criminal's toolbox, allowing the individual or malware to overcome a number of inhibiting controls to access data. C~~However, c~~ontrols such as data loss prevention (DLP), IDS/IPS, and endpoint security ~~may help~~provide a greater assurance to detect or ~~outright~~ prevent the exfiltration or malicious encryption of ~~said~~ data.

Commented [KM119]: Provide a greater assurance to detect....

Commented [JS120R119]: Made as proposed

Commented [KM121]: 'provides a greater assurance to detect or prevent the exfiltration or malicious encryption of data.

Commented [JS122R121]: Made as proposed

Key Takeaway:
Although endpoint controls may be applied to the DER to accomplish security objectives, these controls are not guaranteed to be adequately maintained over their lifetimes and existing, legacy DER may not be technically equipped to accommodate them. DER Gateways are required to mitigate the lack of endpoint controls on the DER devices and to ensure secure interoperability with upstream managing entities. ~~themselves.~~ Alternatively, endpoint controls on the DER devices may accomplish some of the same security objectives~~ accomplished through a~~

DER Gateways

~~**Key Takeaway:**~~
~~DER Gateways mitigate the lack of endpoint controls on the DER devices themselves. Alternatively, endpoint controls on the DER devices may accomplish some of the same security objectives accomplished through a DER Gateway.~~

DERs face a ~~variety~~ broad range of local threats and vulnerabilities which are ~~likely~~ presently outside of utility responsibility and control. For example, a~~the~~ DER ~~itself~~ can ~~be exposed to~~have a variety of ~~different~~ interfaces in addition to the ~~utility's~~ standardized ~~connection~~one~~connection~~, including those used for aggregators~~aggregator~~, owners, and OEM management. Each of these interfaces present a potential backdoor to the DER, ~~its~~ any local networks~~network~~, and the upstream managing entity's systems. IEEE 1547-2018 requires one open standard interface but does not prohibit these other interfaces. There are currently no specifications or requirements that apply to other DER interfaces. IEEE 1547-2018 does not specify cybersecurity requirements for DER and its local ~~networks~~ interfaces because they are generally untrusted systems to the DER managing entity[30] due to these risk exposures.

Furthermore, current compliance and certification frameworks are limited in their scope of enforcement[31] to ensure that necessary security controls are adequately met among owners of DER. In the absence of enforceable requirements at all DER interfaces, managing entities cannot establish assurances that critical security controls used for secure communications, including certificate management, private key protection, firewall policies, user access control, and other device-specific security features are routinely reviewed and maintained over the DER's lifetime. This gap presents a challenge for managing entities where integrity and availability of data and functionalities cannot be fully established for communications to the DER, ~~and~~ where risk exposures[32] are ~~most significant~~much broader. This gap~~This~~ exposes all interfacing parties to a variety of attack scenarios against communications critical for grid interoperability, including:

- Man-in-the-Middle – Data that is supposed to flow only between a managing entity and the DER flows through a middle node that reads or modifies data before it is sent on its way~~.~~
- Denial of Service – A group of compromised DERs deliberately overload upstream managing systems with useless traffic and the resource-exhausted network or managing system cannot perform its functions. Alternatively, a certificate expires on the DER and prevent the managing system from access. In both cases, this could impact a power system operator trying to control the power system~~.~~
- Replay – A command being sent from the managing entity to the DER is copied by an attacker. This command is then used at some other time to cause unexpected actions performed by the DER~~.~~
- Malware – An attacker adds malware to a DER, allowing it to propagate upstream to the managing entity.

Formatted: List Paragraph, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Commented [MOU123]: Would move this to the top as mentioned

Commented [QC124]: worht mentioning UL2941 here?

Commented [JS125R124]: No change made

Commented [SB126]: Similar to a previous comment, I'm confused about what is envisioned as a DER owner responsibility. I am not aware of any movement toward requiring DER owners to do anything.

Commented [JS127R126]: Added clarity to footnote

Commented [QC128]: what does significant mean in this context? could use additional clarification

Commented [JS129R128]: added clarity

Commented [QC130]: what is 'this' referring to here?

Commented [JS131R130]: Added clarity

Commented [QC132]: could consider revising to adversary or person in the middle

Commented [JS133R132]: no change made.

---

[30] The special case exception to this is when the DER managing entity is also the DER manufacturer.

[31] Due to the voluntary nature of the IEEE Standards, and the varying nature of the regulatory framework for the local distribution of energy. Further, it is not feasible to require action at the DER Owner level for their networks.

[32] This is especially true for cases where DERs integrate using public, internet-based networks.

DER gateways can serve as local platforms housing features and functions important to the DER managing entity, but they can also perform several important perimeter security functions that prevent~~s~~ ~~against~~ these attack scenarios. This local platform physically resides at the ~~local~~ DER site and, as defined by IEEE 1547, includes a wired, physical interface that establishes a private connection to the DER ~~only~~ through the gateway though the definition is still under revision in IEEE.

Commented [QC134]: based on conversations happening in the 1547.10 stakeholder meetings, this definition may change, just an fyi

Commented [JS135R134]: added clarifier

Placing ~~S~~security requirements for DER gateways assumes that there are deficiencies in DERs and establish a higher degree of trust in the communications to and from DER sites to protect critical utility systems, such as DERMS and Advanced Distribution Management System (ADMS~~,~~), from internal and external threats. These requirements include~~s~~ translating the DER's untrusted communication to trusted TLS-based communications, implementing data access rights through role-based controls, configuring network access control and segmentation through firewall policy, performing network and application-layer monitoring for threats, and verifying firmware updates through signature-based methods. Because these and other security features are implemented on a gateway that is owned, implemented, maintained, and certified by the managing entity rather than the DER-owner or manufacturer, managing entities can ensure secure integration over public, untrusted networks with its DERMS or other management software operations.

Commented [QC136]: Which requirements? are you talking about a specific standard or proposed requirements? Either way. needs clarification

Commented [JS137R136]: Clarity added

Formatted: Font color: Text 1

Firmware updates are necessary to maintain security. For example, mobile phones, browsers, and computer operating systems are engineered with great attention to security, and yet frequently updated due to discovered vulnerabilities. It is not practical to expect that a DER managing entity could or would update firmware in a customer's DER for several reasons:

- The system is made up of a broad diversity of makes, models and vintages
- Only the manufacturers of each DER can produce a new/patched code
- The manufacturer of DER's may not be in business or supporting the models in the field and are not required by interconnection agreements to provide future updates
- Manufacturers may not have a network path or connection to reach the DER to perform an update.
- There may be risk of harming (brick-ing) a device when updating its code

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

However, DER managing entities may readily maintain the firmware of DER gateways which may be of consistent design and under their direct control. For example, firmware updates are commonly pushed to thousands of utility SCADA radios, millions of AMI meters, etc. Further, complete systems of DER gateways and the communication networks they use can be retired and replaced when necessary but it is not practical to force the retirement of a customer's DER.

A new IEEE ~~implementation guideline~~recommended practice, the *IEEE P1547.10 Recommended Practice for Distributed Energy Resources (DER) Gateway Platforms*[33], is currently under development with contributions of ~~different~~ several stakeholder groups (e.g., DER and DER gateway developers, owners, and operators, software producers, distribution and transmission system planners and operators, certification providers, etc.). The purpose of this project is to maintain coherency between the family of P1547.x and P2030.x standards, and other related projects for DER and Distributed Energy Resources Management

Commented [SB138]: Could shorten this section a bit.

---

[33] PAR available at https://development.standards.ieee.org/myproject-web/app - viewpar/13494/9866

Systems (DERMS) within the evolving smart grid interoperability reference model with a focus on Distributed Energy Resources (DER) Gateway Platforms. The recommended practices within P1547.10 will~~practice~~ enable~~s~~ utilities deploying DERMS and other DER integration systems to integrate DER with grid edge intelligence, while allowing DER devices to serve their core functions, focused~~ing focusing~~ on simplicity, interoperability, and long-term stability. The scope of IEEE P1547.10 includes g~~G~~ateway platform functions and communications, including operational procedures and data collection recommendations. Additionally, recommended procedures for cybersecurity, centralized manageability, monitoring, grid edge intelligence and control, multiple entities management, error detection and mitigation, events tracking, and notification, communication protocol translation, and communication network performance monitoring. **Figure 4~~Figure 3~~** illustrates the use of DER gateways. As indicated by the dashed lines, the gateways are physically at the DER site, but as shown by the coloring, are part of the aggregation/management system. ~~shows the location of where a DER Gateway sites between networks in the latest efforts for IEEE implementation guideline~~.

Commented [QC139]: for consistency, I believe this should be lower case

Formatted: Cross Reference Char

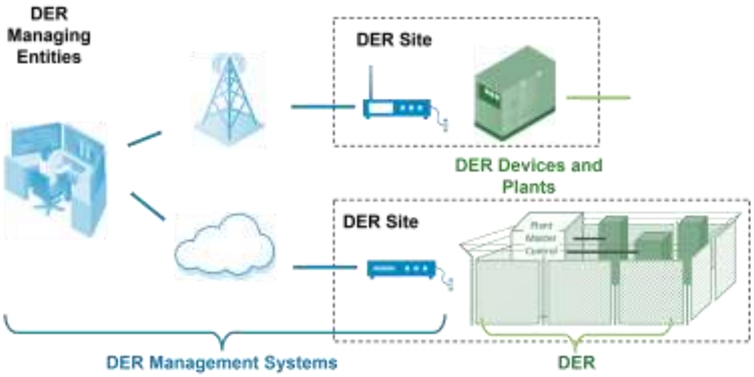


Figure 4~~3~~: Example DER Gateway interface [Source: EPRI]

Carrier Controls Inherent in Communication

Many of the communications channels anticipated for information sharing between DER and DER Aggregators may traverse fiber networks using TCP/IP protocols. Devices (e.g., DER inverters or DER Aggregator control centers) using routable protocols over fiber networks, including some private fiber networks, will have a carrier entity install and maintain these communication lines. Entities should ensure business agreements with third party carriers of these fiber networks ensure security controls are implemented. ~~Many of the communications channels anticipated for information sharing between DER and DER Aggregators will likely traverse some fiber network and likely uses TCP/IP protocols. In unique circumstances, this may be different, yet the underlying assumption is that the traffic will need to be routable to the intended device (e.g., DER inverter or DER Aggregator control center). As many of these fiber networks, including some private fiber networks, will have a carrier entity install and maintain these communication lines, the carrier of these fiber networks inherently have some security controls in the way~~

Commented [KM140]: May traverse fiber networks using TCP/IP protocols.

~~they handle communication on their network. It should not be assumed that carriers of these networks will provide the security controls necessary to thwart OT cyber criminals., but Rrather, acknowledgingesrather acknowledges that carriers of the networks may be helpful in implementing a strong security posture of the electric ecosystem that includes DER and DER Aggregators.~~

Current Distribution Security Landscape of DER and DER Aggregators

As evidenced in recent presentations[34] to SPIDERWG and SITES, the distribution landscape is primarily supported by equipment standardization with little to no standard design criteria about specific hardware, technologies, and engineering. This practice is in an effort to ensure that non-engineering technicians can install cost-effective solutions geared towards~~to~~ mitigating commonly-reported customer ~~-reported~~ problems within~~in~~ ~~that~~ the affected portion of the distribution system. ~~In~~ From the lens of cyber~~-~~security, this may seem like an unknown world of major interoperability challenges that would need solid endpoint controls to limit ~~the~~ access to the centralized ecosystem. ~~This~~Specific security requirements, however, ~~is~~ are left up to each distribution entity's regulatory and corporate bodies to enable specific security controls for~~on~~ DER. Additionally, FERC Order 2222 does not ~~have~~ require any specific security protections ~~required~~ to enable the participation of DER in the wholesale ISO/RTO markets. Thus, the SPIDERWG and SITES reviewed ~~the~~ all available information ~~it had available~~ on the distribution system and characterized a few main points, summarized below.

Telecommunications Networks: Distribution utilities use a combination of private fiber connections, public internet fiber connections, and radio communication interfaces for their monitoring and switching action. Utility-~~-~~level DERs are more likely to emulate BPS architectures, using private networks for communication back to their shared locally geographic control centers. Most concerning, however, are geographically decentralized residential and commercial DERs utilizing public networks, i.e., the internet. Commonly, these connections do not use the IEEE 1547-2018 specified interface, but a variety of other interfaces for which there is presently no requirements at all. Accordingly, adding cyber security requirements to the IEEE 1547-2018 standard interface would have no effect.

Public internet access for DERs is utilizing ~~wi-fi~~Wi-Fi and cellular 4G/5G wireless networks which are susceptible to interception and require strong encryption and authentication, or wired ~~ethernet~~Ethernet and fiber-optic networks potentially compromised through physical access or device vulnerabilities at the site of the DER endpoint. In some ~~of~~ cases, private networks between the DER aggregator and their controlled DERs are achieved over the internet through the use of VPNs, offering increased security if properly terminating the remote session. Regardless of the medium for access, the use of public internet leaves both DERs and DER aggregators' control systems more exposed to remote attacks from anywhere on the globe. To ensure the resilience and stability of residential and commercial DER ecosystems, it is crucial to implement comprehensive security measures tailored to the specific requirements of each telecommunication network.

Commented [QC141]: it is not obvious what kinds of inherent security controls this might include. Consider adding an example

Commented [QC142]: helpful in what ways? should this be enforced through contracts? How do you envision these carriers 'helping'?

Commented [KM143]: Consider this edit -

Many of the communications channels anticipated for information sharing between DER and DER Aggregators may traverse fiber networks using TCP/IP protocols. Device (e.g., DER inverter or DER Aggregator control center) using routable protocols over fiber networks, including some private fiber networks, will have a carrier entity install and maintain these communication lines. Entities should ensure business agreements with third party carriers of these fiber networks ensure security controls are implemented.

Commented [JS144R143]: Made as proposed

Commented [QC145]: this, as in the lack of standardization?

Commented [JS146R145]: clarified

Commented [QC147]: is 'that portion' the distribution portion? this is unclear

Commented [JS148R147]: added clarity

Commented [QC149]: think this is missing a word major interoperability challenges? Consider re-wording for clarity

Commented [JS150R149]: added as proposed

Commented [QC151]: what is left to regulatory and corporate bodies? Responsibility for specific security controls for DERs?

Commented [JS152R151]: Clarity added

Commented [CR153]: Some of these open connections may have open ports or remote sessions that are not properly terminated and such. Suggest mentioning the impact here.

Commented [JS154R153]: Added to sentence

---

[34] In particular the presentations at the SPIDERWG February 2023 meeting. Available here: https://www.nerc.com/comm/RSTC/SPIDERWG/SPIDERWG_Presentations.pdf

Electrical Protection Measures: It is still a common practice for protection in most distribution networks to use fuse-based protection while some distribution entities may use more advanced solid state relay protection. In those instances, however, the protection seeks to limit backfeed to the transmission system or to enhance a secondary area network scheme's ability to recover from fault. The distribution system is thus much more fuse-based which provides physics-based protections that are not present in the same ways or same densities on the transmission grid.

Distribution entities rely on equipment standardization: With the need to lower cost to their consumers, distribution companies rely on turnkey solutions based on standard designs when upgrading or fixing a circuit. This allows the distribution system to be reconfigured by non-engineering staff and field crews while still maintaining high levels of reliability (e.g., using proven designs to limit SAIFI and SAIDI)

Security is not integrated in distribution system design: Rather than installing security protections, distribution companies rely on well-run line crews to recover the system and restore damaged equipment using local spare equipment. As distribution poles and associated equipment is relatively cheap, some perceive this as a cost effective solution to the security challenge posed by overhead distribution. However, the proliferation of DER, the upward trends of cyber attacks against both internet of things (IoT) and industrial control systems (ICS), and the potential for aggregate attack against DER ecosystems are changing these perspectives.

The common distribution system does not currently have a robust set of security requirements and controls to protect it from malicious activity. Rather, the system is currently designed around quick response to equipment damage (e.g., due to tree limbs, downed distribution poles, or other faults) and reconfiguration to maintain a high degree of reliability to their system. Current research and scenario development[35] to secure the distribution system and DERs at large is progressing rapidly, especially by review of equipment standards and implementing security controls. This research is assisting and developing equipment level standards to aid distribution entities to be able to use standard equipment when integrating DERs into their system. For example, UL Solutions is seeking to investigate at an equipment level a way to certify the functional requirements of secure communication to limit the impact of a security compromise of a single DER. These updates to equipment standards and certification of distribution equipment are anticipated to maintain the current distribution paradigm and enhance it to support a strong security posture.

~~As the other main points may allude to, security is an afterthought for most distribution system upgrades or alterations. Rather than installing security protections, distribution companies rely on well-run line crews to recover the system and restore damaged equipment using local spare equipment. As distribution poles and associated equipment is relatively cheap, some perceive this as a~~ cost- effective ~~solution to the security challenge posed by overhead distribution. However, the proliferation of DER, the upward trends of cyber attackscyber-attacks against both internet of things (IoT) and industrial control systems (ICS), and the potential for aggregate attack against DER ecosystems are changing these perspectives.~~

Commented [CR155]: Cybersecurity is not a profit space, it is almost always a profit sink as well. Under resourced vendors/utilities with no means of having effective cyber programs may result in attack vectors.

Commented [JS156R155]: Thank you for your comment.

---

[35] One example of the research into recommendations and test cases for cybersecurity scenarios pertaining to DERs is available here: https://www.osti.gov/biblio/1832209

~~These main points are not to say that the distribution systems across NERC are under consistent malicious threat and are a critical nature, but rather that the common distribution system does not have a robust set of controls to protect it from all malicious activity. Rather, the system is currently designed around quick response to equipment damage (e.g., due to tree limbs, downed distribution poles, or other faults) and reconfiguration to maintain a high degree of reliability to their system. Current research and scenario development[36] to secure the distribution system and DERs at large is progressing rapidly, especially by review of equipment standards and implementing security controls. This research is feeding and developing equipment level standards to aid distribution entities to be able to use standard equipment when integrating DERs into their system. For example, Underwriter Laboratories[37] is seeking to investigate at an equipment level a way to certify the functional requirements of secure communication to limit the impact of a security compromise of a single DER. These updates to equipment standards and certification of distribution equipment are anticipated to maintain the current distribution paradigm and enhance it to support a strong security posture.~~

Differentiation of Utility-scale DER versus Retail-scale DER landscape

The security posture between utility-scale DER (U-DER) and retail-scale DER (R-DER) can differ. The retail-scale ~~will likely~~may not have a private fiber connection to the utility itself and ~~will likely~~can use public networks for communication. Further, the DER o~~O~~wners of R-DER are not able to practically acquire, implement, and maintain the above security controls and as such have no requirements to do so. In the utility-scale side there is a higher ~~chance~~ likelihood that the connection will be over a private network to the utility and may already have a small attack surface and stronger security controls inherent to the design. These end-use devices will then move towards having ~~lesser~~ fewer recommended additional controls for managers of U-DER ~~only opposed to~~than for management of R-DER devices. Namely, R-DER devices are assumed untrustworthy as a default~~.~~. These categorizations do not alter the current distribution landscape, however, as the same equipment standardization will likely be used to electrically connect both U-DER and R-DER to the distribution system. These categorizations are important when considering the “trustworthiness” of a type of communication and in producing standardized design to incorporate U-DER, R-DER, or a combination of both into the distribution system. ~~DER Aggregator~~DER aggregators in particular should ~~contain~~ implement and maintain security controls that allow a strong protection against attack through the DER it controls, regardless of U-DER or R-DER classification.

Distribution Management Systems and Emerging Distribution Landscape Considerations

Currently, efforts are ongoing to implement Distributed Energy Resource Management Systems (DERMS) at various entities. These systems have functional specifications housed in the IEEE 2030.11-2021,[38] which is a guide that houses the various configurations and required functions of such a management system. Such a guide allows the functions of the DERMS to exist within an entity’s premises, off-site at a cloud-based system, or a hybrid solution that interplays between the two. As stated in the guide, “it is possible to deploy a DERMS in an off-site location where the infrastructure is provided by a third-party computer hosting

---

~~[36] One example of the research into recommendations and test cases for cybersecurity scenarios pertaining to DERs is available here: https://www.osti.gov/biblio/1832209~~

~~[37] Specifically UL2941, available here: https://www.shopulstandards.com/ProductDetail.aspx?productId=UL2941_1_O_20230113~~

[38] Available here: https://ieeexplore.ieee.org/document/9447316

Commented [QC157]: I believe they are now called UL Solutions

Commented [KM158]: Consider this proposed edit.

Rather than installing security protections, distribution companies rely on well-run line crews to recover the system and restore damaged equipment using local spare equipment. As distribution poles and associated equipment is relatively cheap, some perceive this as a cost effective solution to the security challenge posed by overhead distribution. However, the proliferation of DER, the upward trends of cyber attacks against both internet of things (IoT) and industrial control systems (ICS), and the potential for aggregate attack against DER ecosystems are changing these perspectives.

The common distribution system does not currently have a robust set of security requirements and controls to protect it from malicious activity. Rather, the system is currently designed around quick response to equipment damage (e.g., due to tree limbs, downed distribution poles, or other faults) and reconfiguration to maintain a high degree of reliability to their system. Current research and scenario development to secure the distribution system and DERs at large is progressing rapidly, especially by review of equipment standards and implementing security controls. This research is assisting and developing equipment level standards to aid distribution entities to be able to use standard equipment when integrating DERs into their system. For example, Underwriter Laboratories is seeking to investigate at an equipment level a way to certify the functional requirements of secure communication to limit the impact of a security compromise of a single DER. These updates to equipment standards and certification of distribution equipment are anticipated to maintain the current distribution paradigm and enhance it to support a strong security posture.

Commented [JS159R158]: Made as proposed

Commented [CR160]: Nor will R-DER homeowners be required or mandated to do anything. Vendors are responsible for maintaining the security of this, but don’t fall under many standard jurisdiction.

Commented [JS161R160]: Thank you for your comment. The group agrees.

Commented [CR162]: As such they may represent an attractive attack vector even if the vendors enterprise security is good, the device level may be lacking such that it can be used to gain access.

Commented [JS163R162]: Thank you, no change made based on this comment.

Commented [QC164]: are these the authors' opinions or based on observations from interactions with utilities or does this require a citation? Alternatively, you could get around this by using 'may' or 'can', or 'most' to describe what you feel is a likely scenario

Commented [JS165R164]: clarity added.

Formatted: Heading 2

provider." While 2030.11 lists the various common communication protocols and concepts required to be addressed, it does not directly address the cybersecurity requirements of a DERMS. Rather, the guide provided other referenced material (e.g., IEEE C37.240-2014[39]) and allows the integrator of a DERMS to determine the exact cybersecurity requirements. The guide lists that the security of data in such deployments should be reviewed and include the following:

- Security of data in transit between on-site and off-site locations
- Security of data at the off-site locations
- Security of requests sent from the off-side location to the external internet
- Backups of off-site data
- Hosting service availability

Formatted: List Bullet

In such instances, the ongoing implementation of a DERMS will have direct tie-ins to the ongoing evaluation of cloud-hosted services and the security requirements of such applications. It is assumed that most utilities at this time do not have a DERMS and are likely not able to have sufficient infrastructure to fully own all infrastructure used by a DERMS if the utility decides to implement a DERMS. Utilities looking to implement a DERMS in order to manage and dispatch DERs should have stringent specification for cybersecurity requirements when using off-site hosting services as part of their DERMS. Further, DER aggregators are assumed to require a DERMS or similar infrastructure in order to accomplish their goal and should also require stringent cybersecurity requirements when implementing any functions of a DERMS off-site. As a first step, requiring strong cybersecurity controls as part of their service agreements with the off-site hosting service can initiate a bilateral agreement with the off-site hosting service in order to secure the DERMS from malicious interaction.

---

[39] Available here: https://standards.ieee.org/ieee/C37.240/5029/

Security posture of DER Aggregators

DER aggregators are relatively new entity to the ecosystem of aggregate control of multiple end-use devices to participate in the wholesale ISO/RTO markets. ~~DER Aggregators are different~~ unique ~~as they are a relatively new entity to this ecosystem that aggregate control of multiple end-use devices to participate in the wholesale ISO/RTO markets.~~ The ISO/RTOs consist of the PCs, BAs, and RCs of the transmission system while the ~~DER Aggregator~~DER aggregator is a middle entity (or entities) that constitute a pathway for previously independently controlled DER assets are under command from this middle entity. A DER aggregator currently does not have security requirements relative to the risk-impact it has on the bulk system, nor does it have OT security requirements outside of those required by regulators over the DER aggregator~~A DER Aggregator currently does not have known security requirements relative to the risk-impact is~~it~~sis has on the bulk system, nor does it have known OT security requirements outside of those required by regulators over the DER Aggregator~~. As such, the NERC SPIDERWG and SITES have assumed the following with respect to the ~~DER Aggregator~~DER aggregator:

~~2.~~1. The ~~DER Aggregator~~DER aggregator will act to protect itself against common IT attacks targeting personal data required to award bids

~~3.~~2. The protections on a ~~DER Aggregator~~DER aggregator's ~~has on its~~ IT software will not allow OT compromise by an IT intrusion

3. The ~~DER Aggregator~~DER aggregator has minimal OT security and relies on the utility (i.e., ISO/RTOs) to dictate the required security controls on ~~it~~ the aggregator and the DER it controls.

4. The DER aggregator will use cloud solutions for their DER management due to the amount of data to process.

Confidentiality of Data at the DER and DER Aggregator

In order to conduct a proper study of the electrical impact of DER and ~~DER Aggregator~~DER aggregators, specific electrical models ~~would~~ need to be developed and shared to represent the aggregate impact DER have on the bulk system. The SPIDERWG has multiple reliability guidelines associated with the model development of aggregate DER; however, the representation of a ~~DER Aggregator~~DER aggregator can vary and should be able to be represented in the impact it has on loadflow and transient stability of the bulk system. As with bulk-connected resources, some information may be tied to confidential agreements between OEMs or owners and data sharing of that confidential data is not allowed. This requirement to represent the end-use electrical equipment to study impact of aggregate DER[40] does not require the type of data typically secured under confidential and private agreements between the DER owner, manufacturer, ~~DER Aggregator~~DER aggregator, or the utility. Entities handling DER information (e.g., TPs, PCs, and DPs) should ensure that the security controls they have in place include proper data management and access controls to ensure the sharing of required modeling data can occur while maintaining a high level of confidence in the privacy-protective treatment of ~~private~~ end-user data.

NERC Reliability Standards Relationships

Commented [KM166]: DER Aggregators are relatively new entity to the ecosystem of aggregate control of multiple end-use devices to participate in the wholesale ISO/RTO markets.

Commented [JS167R166]: Made as proposed

Commented [KM168]: A DER Aggregator currently does not have security requirements relative to the risk-impact it has on the bulk system, nor does it have OT security requirements outside of those required by regulators over the DER Aggregator

Commented [JS169R168]: Made as proposed

Commented [XF170]: Is it also safe to make an assumption that aggregators are likely to use the cloud for DER management and call that out as a bullet here? If so, there may be a whole section on cloud recommendations that should be included in this paper.

Commented [JS171R170]: Made as proposed and added a small section on this below

Commented [KM172]: Is it a 'will' or a 'must'?

Commented [JS173R172]: Added clarity. Assumption was on what action the DER Aggregator will take in cybersecurity. Assumed only IT.

Commented [KM174]: The protections on a DER Aggregator's IT software will not allow OT compromise by an IT intrusion

Commented [JS175R174]: Made as proposed

Commented [KM176]: delete

Commented [JS177R176]: altered text

Commented [CR178]: Additionally what security measures are they enforcing on their vendors? What about foreign vendors? Do they have a documented supply chain vendor list?

Commented [JS179R178]: Thank you for your comment. While the group agrees with the questions, no change made to the assumption that they will apply the ISO/RTO dictated controls.

Commented [KM180]: delete

Commented [QC181]: privacy-protective treatment maybe?

Commented [JS182R181]: Made as proposed

Commented [JS183]: Took out comments related to DER networks for integration. Not identified as separate entity but rather part of the DER facility (lower f).

---

[40] Operated under a DER Aggregator or in independent operation

As both ~~DER Aggregator~~DER aggregators and DERs do not have a NERC registered ~~function~~ entity category that directly covers their applicability to NERC Reliability Standards, SPIDERWG and SITES identified ~~any~~ similarities ~~to~~ where the privacy and security practices of DERs and ~~DER Aggregator~~DER aggregators may need to be examined ~~in order~~ to determine any future applicability to NERC Reliability Standards. In particular, if DER or ~~DER Aggregator~~DER aggregators provide BES Reliability Operating Services (BROS).~~).~~ These services, as seen in **Table 1**, are typically assessed for any impact over a 15 minute time frame. The following table is from CIP-002-5.1a[41], which can help relate the electrical function provided by a registered entity and what has been identified to have a grid reliability impact. SPIDERWG and SITES note that the ~~DER Aggregator~~DER aggregator in particular can, in some instances, provide some of these functions for the DER it controls; however, the capacity of the ~~DER Aggregator~~DER aggregator in a particular area can determine if the service has impact to BROS.

Table 1: Impact of Registered Entity and Associated Reliability Functions

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

In Order No. 2222 Paragraph 130, FERC specified that RTO/ISOs must “…~~“~~allow distributed energy resources to provide all services that they are technically capable of providing through aggregation.” If capable, DER Aggregations may begin providing services that resemble BES Reliability Operating Services. To determine whether ~~DER Aggregator~~DER aggregator’s Cyber Assets meet the definition of a BES Cyber Asset, new and improved models for simulating a ~~DER Aggregator~~DER aggregator’s impact on the Bulk Electric System will be required. Without accurate development of electrical models[42] that represent the control behavior pertinent to the functions above, completing the impact test of whether the control of the asset may materially impact the bulk system requires engineering judgement. For instance, if ~~DER Aggregator~~DER aggregators are providing Frequency Regulation – balancing supply and demand on the electric system by changing energy injection or energy withdrawal within seconds – then the impact of rendering the DER aggregation Cyber Asset “unavailable, degraded, or misused” within 15 minutes on the Balancing Authority Area should be carefully studied. A ~~DER Aggregator~~DER aggregator providing 1 MW of Frequency Regulation

Commented [KM184]: Includes?

Commented [JS185R184]: No change made.

Formatted: Cross Reference Char

---

[41] CIP-002-5.1a is available here: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf

[42] These models can take on a variety of data sources, the most common software platforms that represent the Bulk Electric System are positive sequence models. Models here include loadflow and transient dynamic representations of the behavior exhibited by DER and DER Aggregator actions. Current SPIDERWG modeling documents exist for DER operating independently of a DER Aggregator, available here: https://www.nerc.com/comm/Pages/Reliability-and-Security-Guidelines.aspx

compared to a ~~DER Aggregator~~DER aggregator providing 100 MW of Frequency Regulation will ~~simply~~ clearly have a different level of impact to the Bulk Electric System (i.e., to Area Control Error).

BES Cyber Asset

The definition of a NES Cyber Asset is ~~A~~aA Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

Key Takeaway:
The DER Aggregator should be registered for NERC Reliability Standards applicability when it owns an asset that acts as a BES Cyber Asset and thus can impact the reliable operation of the BES.

Limitations on Assessment and Applicability of DER, DER Aggregators, or other Distribution Entities

The NERC Rules of Procedure Appendix 5B's material impact test[43] defines the way in which a potentially compromised asset in the generation, transmission, or distribution of energy can ~~have an~~ impact ~~on~~ the BES. The materials impact test's questions are reproduced here:

~~2.~~1. Is the entity specifically identified in the emergency operation plans and/or restoration plans of an associated Reliability Coordinator, Balancing Authority, Generator Operator or Transmission Operator?

~~3.~~2. Will intentional or inadvertent removal of an Element owned or operated by the entity, or a common mode failure of two Elements as identified in the Reliability Standards (for example, loss of two Elements as a result of a breaker failure), lead to a reliability issue on another entity's system (such as a neighboring entity's Element exceeding an applicable rating, or loss of non-consequential load due to a single contingency)? Conversely, will such contingencies on a neighboring entity's system result in issues for Reliability Standards compliance on the system of the entity in question? Appendix 5B – Statement of Compliance Registry Criteria (Revision 7) 8

~~4.~~3. Can the normal operation, misoperation or malicious use of the entity's cyber assets cause a detrimental impact (e.g., by limiting the operational alternatives) on the operational reliability of an associated Balancing Authority, Generator Operator or Transmission Operator?

~~5.~~4. Can the normal operation, misoperation, or malicious use of the entity's Protection Systems (including UFLS, UVLS, Special Protection System, Remedial Action Schemes and other Protection Systems protecting BES Facilities) cause an adverse impact on the operational reliability of any associated Balancing Authority, Generator Operator or Transmission Operator, or the automatic load shedding programs of a PC or TP (UFLS, UVLS)?

---

[43] Available here: https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix%205B.pdf

As seen by the language above, ~~the way~~ NERC identifies the material impact to the bulk system ~~is identified is~~ through an element's ability to affect the operational state and functions performed by a BA, GOP, or TOP. A few other questions focus on distribution enabled relaying (i.e., UFLS and UVLS), which DER and ~~DER Aggregator~~DER aggregators may have a stronger impact depending on feeder configuration and specific implementation[44] of a PC's UFLS program. Many of these questions do not currently apply to OEM interactions for proprietary connections to the asset~~,~~ but instead deal with the element's electric impact to the bulk system. Proprietary connections are allowable per 1547-2018 at the local DER interface, which can allow for the DER device to be compromised and lead to misoperation or malicious use if unprotected. Thus, it is important ~~for the ability~~ to represent the potential impact of these devices in studies that assess the performance of the bulk system, including the applicable level these assets reach in NERC's Reliability Standard CIP-002-5.1a. These devices should be appropriately categorized based on the impact test, which requires a thorough understanding of the interaction of DERs, ~~DER Aggregator~~DER aggregators, and utility systems.

BES Impact Test and Meaning

~~DER Aggregator~~DER aggregators may potentially meet the material impact test as per the "BES Cyber Asset" definition as part of the NERC Glossary of Terms[45] and through the understanding of the control of assets the ~~DER Aggregator~~DER aggregator has in its system. SPIDERWG and SITES do not anticipate that any one DER outage will have the size and impact that can adversely affect the ~~impact or~~ operational reliability of any associated BA, GOP, TOP, RC, or other NERC entity. Rather, the aggregate impact of DERs onto the bulk system ~~are found in~~can affect the performance of the bulk system during grid disturbances. SPID~~R~~ERWG~~SPIDREWG~~ has developed reliability guidelines[46] to address the modeling and verification of DERs in bulk system studies, and is currently drafting guidance[47] on the studies performed that incorporate these aggregate models. Further, the SITES has also identified[48] that the individual DER under malicious control has a different impact than the ~~DER Aggregator~~DER aggregator. Depending on the size[49] and control mechanisms in place, a ~~DER Aggregator~~DER aggregator may reach a level of BES impact. The SPIDERWG and SITES recommend further analysis in this area to determine the impact of a ~~DER Aggregator~~DER aggregator (or similar entity) has on the bulk system.

Security Standards, Frameworks, or Alternatives in this Area

Outside of the NERC CIP standards, other governmental and national labs have provided frameworks to categorize multiple aspects of a strong security posture for the electric ecosystem. Other cybersecurity forums have also provided certification, tests, and other communication protocols that enhance the

---

[44] SPIDERWG has drafted a reliability guideline on this topic, which is available here: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Recommended_Approaches_for_UFLS_Program_Design_with_Increasing_Penetrations_of_DERs.pdf

[45] Glossary of terms here: https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf

[46] The SPIDERWG reliability guidelines are available here: https://www.nerc.com/comm/Pages/Reliability-and-Security-Guidelines.aspx

[47] See SPIDERWG Work Plan, available here: https://www.nerc.com/comm/RSTC/SPIDERWG/SPIDERWG%20Work%20Plan.pdf

[48] Identified in *Cyber Security for Distributed Energy Resources and DER Aggregators*, available here: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_Cybersecurity_for%20DERs_and_DER_Aggregators.pdf

[49] For reference, the CIP-002-5.1a Medium impact threshold for generator control centers is 1,500 MW of active power resources and 1,000 MVAR of reactive power resources

efficacy of modern security controls. In some instances, these alternatives can include resilience focused projects that do not fully rely on security controls, akin to how many distribution companies have "hot swappable" equipment. Some of these alternatives include:

~~2.~~1. The Cybersecurity Capability Maturity Model[50] (C2M2), which is a tool for organizations to evaluate cybersecurity capabilities for IT and OT environments.

~~3.~~2. The Distributed Energy Resource Cybersecurity Framework[51] by NREL, which is a tool designed specifically to evaluate the cybersecurity posture of DERs for the U.S. federal government.

~~4.~~3. Idaho National Lab's Standards to Secure Energy Infrastructure[52] that allows for quick searches of applicable standards or guidance material in this area

~~5.~~4. Underwriter Laboratory Cybersecurity Assurance Program[53] (UL CAP), which offers a suite of tools, testing, and certifications (e.g., UL 2941[54]) to manage and apply commercially available cybersecurity capabilities

~~6.~~5. Sunspec's Cybersecurity Certification Program[55] that also seeks to certify functions for DERs, particularly for compliance to IEEE 2030.5.

~~7.~~6. Sandia National Lab's Recommendations for Distributed Energy Resource Access Control,[56] which provides a framework to minimize the risk of unauthorized access to DER systems.

~~8.~~7. The National Institute of Standards and Technology's set of protocol[57] standards, which define information system security practices.

Many of these alternatives are self-answered questionnaires that highlight areas of improvement for an organization to build new capabilities or leverage existing technology to improve their cybersecurity postures. As such, the SPIDERWG and SITES encourage DER owners, ~~DER Aggregator~~DER aggregators, and similar entities to leverage these more exhaustive tools in addition to the recommendations found in this paper.

Market rules may also offer an avenue for enhanced cybersecurity measures for DERs as they dictate the participation requirements for each participant in the energy market. It is outside the scope of this paper to evaluate particular markets for their structure or adequacy in meeting cybersecurity objectives; however, market rules that specify heightened cyber security postures for all participants may be an avenue to ensure

---

[50] Available here: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

[51] Available here: https://dercf.nrel.gov/

[52] Available as part of the Office of Cybersecurity, Energy Security, and Emergency Response here: https://energyicsstandards.inl.gov/

[53] Available here: https://www.ul.com/services/ul-cybersecurity-assurance-program-ul-cap

[54] Standard available here: https://www.shopulstandards.com/ProductDetail.aspx?productId=UL2941_1_O_20230113

[55] Available here: https://sunspec.org/sunspec-cybersecurity-certification-work-group/

[56] Available here: https://www.osti.gov/biblio/1765273

[57] Primarily NIST's *Security and Privacy Controls for Information Systems and Organizations*, available at https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final, and their Technical Note 2182, available at https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2182.pdf.

DERs and ~~DER Aggregator~~DER aggregators maintain cyber security practices in both the IT and OT environments. ISOs and RTOs are encouraged to incorporate reliability-focused security practices in their rules such that the reliable operation of the bulk power system is not compromised by latent or unknown security threat by the participants of the electric market. Utilities are likewise recommended to ensure proper cybersecurity hygiene when integrating command and control over DERs into their distribution control centers or DER Management Systems[58] (DERMS).

Sponsored certification programs reach a sort of standardization depending on the test bed and protocol. One example from the National Renewable Energy Laboratory (NREL) aims to provide testing and certification procedures[59] for common cybersecurity controls. Additionally, NREL is also working to identify a framework[60] that comprehensively identifies the common threats against DERs in order to standardize incident response and other key players in securing the DER landscape.

National and International Lessons Learned

Current efforts to aggregate the control and dispatch of DERs include the PG&E VPP pilot project[61] with Tesla to leverage distribution-connected Battery Energy Storage Systems during times of high peak demand. These efforts have led to many thousands of end-users supplying a peak power output of, at the time of this paper, nearly 30 MW of generation during times of high strain on the grid. Internationally, Vehicle to Grid (V2G) initiatives that aggregate the ability for electric vehicles to discharge when called upon by the system operator have had some success in the European Union (EU). One EU program's V2G VPP currently is looking at a pilot project[62] to provide short-term frequency response to grid disturbances using strong collaboration between the grid operator and the VPP operator. These pilot projects have the same structural compositions seen by ~~DER Aggregator~~DER aggregators.

Further, it is known that many cybersecurity recommendations, standards, and frameworks speak to a limited scope of applicable assets, threats, and known threat actors. In areas like DER and the distribution system security landscape, many of these frameworks are vague in their applicability to the threats facing DER, ~~DER Aggregator~~DER aggregators, and the distribution system at large. This is largely due to inherent assumptions, lack of threat information sharing, and assumed minimal threat of distribution facilities. Entities in this space have learned that where these functions lack, technical design specifications and framework adaptations to threats facing the distribution system readily improve the overall reliability and security posture of the electric ecosystem. Current advancements in this area include specifying technical security requirements[63] that historically have not existed for DERs.

---

[58] A DER Management System is identified in the IEEE 2030.X family of standards. Particularly 2030.11-2021, which can be found here: https://standards.ieee.org/ieee/2030.11/7259/

[59] Available here: https://www.nrel.gov/docs/fy22osti/80581.pdf

[60] Available here: https://www.nrel.gov/docs/fy20osti/75044.pdf~~—~~. Other work by NREL includes supply chain concerns (https://www.nrel.gov/docs/fy23osti/84752.pdf), and measuring framework compliance by an emulated environment (https://www.nrel.gov/docs/fy23osti/84079.pdf)

[61] Information related to this pilot program can be found on PG&E's website for the Emergency Load Reduction Program. Available here: https://elrp.olivineinc.com/

[62] Information for this one particular project is available here: https://www.next-kraftwerke.com/products/balancing-energy. For this pilot, available lessons learned can be found at the integrating German utility, available here: https://www.amprion.net/

[63] One example of these specifications comes from NREL. Their report on functional specifications is available here: https://www.nrel.gov/docs/fy22osti/79974.pdf

Commented [CR186]: Not to only call out papers I have written, but NREL in addition are addressing supply chain cybersecurity concerns in DER addressed by this paper: https://www.nrel.gov/docs/fy23osti/84752.pdf

And to measure the compliance from the framework that is developed and implement that in an emulated environment outlined in this paper:https://www.nrel.gov/docs/fy23osti/84079.pdf

Commented [JS187R186]: Added to footnote

Commented [QC188]: may be worth explaining why these frameworks are vague (is it the lack of threat information sharing? Something else?)

Commented [JS189R188]: added sentence

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Default Paragraph Font, Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Formatted: Font: 9 pt

Conclusions and Recommendations to DER and DER Aggregators

While there are a variety of security controls available to the ~~DER Aggregator~~DER aggregator and DER owners, there are some controls that are better suited at the end-user device (i.e., the DER) or at the entity that controls and aggregate amount of DER (e.g., ~~DER Aggregator~~DER aggregator or VPP). The types of security controls, types of mitigated attack, implementation notes and recommended entity for these security controls are summarized in Table ~~X.X~~2. This table is a summary of the information contained in the above sections. Further, DER aggregators implementing a DERMS, all or in-part, at an off-site hosting service should ensure strong cybersecurity requirements are in the service agreement, including similar or greater protection than at their own premesis.

Formatted: Cross Reference Char

Formatted: Highlight

Table 2: Security Control Recommendations

Security Control	Types of Attacks Mitigated by Proper Control Implementation	Applicable Entitles	Implementation Notes
Internal Network Security Monitoring	Phishing, Active Scanning, Gathering Victim network or organization information, Malware Deployment	~~DER Aggregator~~DER aggregators	INSM alerts and logs maybe inputs for other activities such as automated responses, forensics, or incident response~~Some controls do not automatically use the reports. These may be prerequisite for other security controls~~
DER Gateways	Man in the middle, malware deployment, Denial of Service, and Replay attacks	~~DER Aggregator~~DER aggregators**	DER Gateways are currently under development for technical specification and may alter per IEEE P1547.10 outcomes
Remote Access Controls	Unauthorized External Remote Access, Trusted Relationship compromises, Remote System discovery, and most forms of Reconnaissance	All Entities*	~~DER Aggregator~~DER aggregators in particular should enable strong remote access security controls on the DER it controls
Data Management and Access Controls	Credential Harvesting or Access, Privilege Escalation, Account manipulation; and a broad set of data deletion, encoding, obfuscation, or manipulation	~~DER Aggregator~~DER aggregator**	These controls can also be used to mitigate privacy concerns by end-users as well as their intended security function
Network and Protocol Security	A majority of current and future cybersecurity threats.	~~DER Aggregator~~DER aggregator	Certain endpoints in the chosen ~~DER Aggregator~~DER aggregator's environment may not support all desired protocols. The implementation of these controls may be software-based, specifically for cloud implemented controls.

* denotes that a DER owners implementation of the control doesn't need to be as sophisticated as ~~DER Aggregator~~DER aggregators or utilities
** denotes that while ~~DER Aggregator~~DER aggregators are applicable, the control may require DER owner coordination to implement

The SPIDERWG and SITES joint team has developed recommendations for the ISO/RTOs (collectively registered as BAs and RCs), ~~DER Aggregator~~DER aggregators, and DERs in order to enhance the security posture of the electric ecosystem. Cyber attacks utilizing simple social engineering or other low-level tactics can readily compromise credentials, making security controls based on credentials alone insufficient. DERs constitute a large attack surface with potentially thousands of entry points into a network. That is, the compromise of any one side of a communications network can allow for interconnected networks to also become compromised potentially ~~and~~ facilitating malware propagation and malicious actor lateral movement~~and propagate~~ (e.g., DER devices, ~~DER Aggregator~~DER aggregator networks, and utility networks). With an ever increasing number of DER access points, robust security controls are of high priority to ensure the security of the electric ecosystem.

To that end, SPIDERWG and SITES jointly developed the following high-level recommendations for the ISO/RTOs:

1. ISOs/RTOs should ensure that their market rules do not prohibit entities ~~to~~ from enhancing~~enhance~~ their cyber~~-~~security posture beyond a minimum level of protection.
2. ISOs/RTOs should also explore and consider market rule enhancements ~~such that~~encouraging participants to incorporate cybersecurity best practices and that do not impose a risk to the reliable operation of the BES. ~~In general, this~~This is part of proper cyber hygiene for entities.

SPIDERWG and SITES also jointly developed the following high-level recommendations for ~~DER Aggregator~~DER aggregators:

1. ~~DER Aggregator~~DER aggregators should implement proper data management and access controls for its network in order to assure confidentiality of private data as well as mitigate against specific cyber attacks. DER aggregators should start by performing a privacy impact assessment[64] and implement the necessary data management and access controls identified as needed from the assessment.
2. ~~DER Aggregator~~DER aggregators should implement strong network access controls, particularly for remote access, and require MFA for remote access of their network and applications.
3. ~~DER Aggregator~~DER aggregators should implement strong ~~external perimeter~~internal controls, such as intrusion detection systems, such that they are notified of a compromise and can take proper actions to mitigate the intrusion.
4. ~~DER Aggregator~~DER aggregators should ensure endpoint controls, such as through DER g~~G~~ateways, are deployed at the DER sites and deploy endpoint controls where a gap exists.

Formatted: Numbering Bullet 1, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Numbering Bullet 1, No bullets or numbering

Commented [QC190]: redundant (ie best practices and proper cyber hygiene) consider removing this sentence

Commented [JS191R190]: Thank you for your comment. The repetition is used for emphasis. Edits made.

Formatted: Numbering Bullet 1, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Commented [XF192]: I suggest this should be preceded with aggregators performing a "privacy impact assessment" PIA to determine whether data exchanges or storage of data hold personally identifiable information (PII) or energy consumption/production data that may infer customer behaviors/characteristics that some DER owners may deem as confidential . The PIA will determine risk level of private data which will, in turn, determine the necessary data management and access control required.

Commented [JS193R192]: Added to this recommendation.

Formatted: Numbering Bullet 1, No bullets or numbering

---

[64] These assessments evaluate the data exchange and storage that may potentially hold energy consumption data that infers customer behaviors or personally identifiable information. Common assessment tools also include follow-up recommendations based on the identified risk exposure in the assessment.

Furthermore, SPIDERWG and SITES jointly developed the following high-level recommendations for DERs:

1. DER owners should ensure they wipe personal information from old hardware and, to the degree possible, implement data management and access control to their network. In particular, U-DERs should implement strong access controls.

~~1.~~2. DER owners should ~~ensure~~understand agreements with DER aggregators including the~~e~~include criteria for the proper use and handling of their personal data ~~as to not exchange data~~including data exchanged with third-parties ~~without the~~ and requirements related to the DER owner's prior consent.

~~2.~~3. U-DERs, to the extent possible, should implement network access controls, particularly for remote access. For ~~programatic~~programmatic remote access, PKIs through a DERMS or other management system by the utility should be enabled.

State Coordination of Implementation of Recommendations

~~**Key Takeaway:**~~
~~The DER Aggregator should register for NERC Reliability Standards applicability when it acts as a BES Cyber Asset and thus can impact the reliable operation of the BES.~~

FERC Order 2222 does not specify requirement for cybersecurity and data privacy. Rather the order recommends that "… ~~"~~that RTOs/ISOs coordinate with distribution utilities and relevant electric retail regulatory authorities (e.g., state PUCs) to establish protocols for sharing metering and telemetry data, and that such protocols minimize costs and other burdens and address concerns raised with respect to privacy and cybersecurity." Due to the various jurisdictions on utility procedures and security measures, strong collaboration and coordination among transmission and distribution entities is highly recommended.

The overall security posture of the bulk system can be impacted by the potential security risks~~risk~~ associated with DER or ~~DER Aggregator~~DER aggregators, and the SPIDERWG and SITES recommend that ~~DER Aggregator~~DER aggregators register for NERC standards applicability when they act as a BES Cyber Asset and thus can impact the reliability of the BES. The recommendations above should be coordinated with appropriate and open stakeholder engagement where the security measures and controls are agreed on for the local distribution system. These entities can assist in building the design basis threat or other risk assessment that prioritize the most effective security controls to mitigate their anticipated threats. State coordination is a high priority where DER-site specific physical security measures are identified.

In general, the key risk considerations ~~which should be considered~~ in this broader coordination effort[65] include 1) data privacy, including both personal and market data, 2) data integrity among entities, and 3) data availability.

Commented [XF194]: Continuing on with the issue of privacy… DER owners should ensure agreements with aggregators include criteria for the proper use and handling of their personal data (such as not exchange data with third-parties without prior consent - for example, to prevent from a similar incident to the Facebook/Cambridge Analytics breach).

Commented [JS195R194]: Added to list of recommendations

Formatted: Numbering Bullet 1, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Numbering Bullet 1, No bullets or numbering

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

---

[65] Additional resources on how this participation in markets can be influenced by DER Aggregators is available at:
EPRI, DER Aggregation Participation in Electricity Markets: EPRI Collaborative Forum Final Report and FERC Order 2222 Roadmap, Palo Alto, 3002020599

Data Confidentiality

Per FERC Order 2222, RTO/ISO must revise their tariffs such that DERAs provide "a list of the individual resources in its aggregation, necessary information that must be submitted for individual DERS, and retain performance data for individual DERs." Entities participating in energy markets must be aware of data privacy regulations, understand the potential impact to customer privacy in the event of data-loss-events, and ensure both technical and procedural controls are implemented to ensure both transparencies in how data is used and adequate protections for consumer data. The recommended coordination should identify these and similar confidentiality requirements, especially as they relate to protecting against a widespread compromise of DERs.

Formatted: Font: Not Italic

Data Integrity

Entities should coordinate development of cybersecurity criteria for DER systems and communication protocols used for interoperability and data exchanges, includes NIST-approved cryptographic suites and protocols to protect against data manipulation, as well as establish protocols to ensure adequacy of security control implementations. Testing standards for DER systems and communication protocols should also be included in the implementation of recommendations.

Data Availability

Creation of risk assessment methodologies is needed to evaluate a grid entity's role in the electric sector and their associated security control and redundancy measures these roles must adopt and maintain. These measures can account for various financial, safety, reliability, privacy considerations resulting from cyber attacks against the entity's systems and data.

Contributors

NERC wishes to thank the following SMEs for contributing to this document. NERC also wishes to thank NREL and EPRI for their contributions and review of the white paper.

Name	Entity
John Biasi	Burns and McDonnell
Dan Kopin	VELCO
Jens Boemer	EPRI
Jose Cordova	EPRI
Xavier Francia	EPRI
Abrez Mondal	EPRI
John Schmall (SPIDERWG vice chair)	ERCOT
Shayan Rizvi (SPIDERWG chair)	NPCC
Shannon Mickens	SPP
Morgan King	WECC
Nick Hatton	WECC
Sam Chanoski	INL
Karl Perman	CIP Corps
Jordan Petersen	NREL
Danish Salem	NREL
Ryan Cyar	NREL
Tom Hofstetter	NERC
Dan Goodlett	NERC
Larry Collier (SITES Coordinator)	NERC
JP Skeath (SPIDERWG Coordinator)	NERC

Formatted Table

Formatted Table

Formatted Table

Agenda Item 13
RSTC Meeting
September 20, 2023

Standard Authorization Request (SAR) for Revisions to EOP-004 Standard

Action

Endorse

Background

Recent large-scale disturbances (e.g., the August 2019 disturbance in the United Kingdom)[1] have demonstrated that unexpected loss of distributed energy resources (DER) during BPS faults can compromise reliable operation of the BPS. Despite potential impact to reliable operation, EOP-004-4 does not currently require reporting by Balancing Authorities (BA) and Reliability Coordinators (RC) of the loss of aggregate DERs to NERC. The purpose of EOP-004-4[2] is to "improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities." Further, NERC disturbance analysis have demonstrated net load jumps that have been attributed to DER tripping yet there is no reflection in EOP-004-4 as to the treatment of this type of event in the categories in Attachment 1. Clarity on which Event Type in Attachment 1 as well as the establishment of a threshold for reporting of loss of aggregate DER support the purpose of EOP-004 in reporting of large grid disturbances.

Summary

This SAR has been through the Event Analysis Subcommittee and the Performance Analysis Subcommittee for their comments, which is included in the draft SAR. The SAR has also gone through the new RSTC SAR industry comment posting and the comments have been incorporated. Redlines and a clean version of the SAR are provided in the meeting package in addition to the comment responses by SPIDERWG members.

Furthermore, the SPIDERWG members had a minority opinion that the SPIDERWG should request RSTC to remove this item from their work plan due to many of the comments not indicating their support of the SAR.

The SPIDERWG is requesting RSTC endorsement of the SAR and submitting it next to the Standards Committee. Additionally, the SPIDERWG is not requesting at this time that the RSTC remove the item from its work plan.

---

[1] Available: https://www.ofgem.gov.uk/publications/investigation-9-august-2019-power-outage

[2] EOP-00404 available here: https://www.nerc.com/pa/Stand/Reliability%20Standards/EOP-004-4.pdf

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the NERC Help Desk. Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	Reporting of Aggregate loss of DER during Grid Disturbances in EOP-004		
Date Submitted:	MM/DD/2023		
SAR Requester			
Name:	Shayan Rizvi, NPCC (NERC SPIDERWG Chair) John Schmall , ERCOT (NERC SPIDERWG Vice-Chair)		
Organization:	The NERC System Planning Impacts of DER Working Group (SPIDERWG)		
Telephone:	Shayan – 212-840-1070 John – 512-248-4243	Email:	Shayan – srizvi@nppc.org John – john.schmall@ercot.com
SAR Type (Check as many as apply)			
☐ New Standard ☒ Revision to Existing Standard ☐ Add, Modify or Retire a Glossary Term ☐ Withdraw/retire an Existing Standard		☐ Imminent Action/ Confidential Issue (SPM Section 10) ☐ Variance development or revision ☐ Other (Please specify)	
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☐ Regulatory Initiation ☐ Emerging Risk (Reliability Issues Steering Committee) Identified ☐ Reliability Standard Development Plan		☒ NERC Standing Committee Identified ☐ Enhanced Periodic Review Initiated ☒ Industry Stakeholder Identified	
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
Recent large-scale disturbances (e.g., the August 2019 disturbance in the United Kingdom[1] or the April and May 2018 disturbances in the United States[2]) have demonstrated that unexpected loss of DERs[3] as part of the entire set of generation assets participating during BPS faults can further compromise reliable			

---

[1] Available: https://www.ofgem.gov.uk/publications/investigation-9-august-2019-power-outage

[2] Available: https://www.nerc.com/pa/rrm/ea/April_May_2018_Fault_Induced_Solar_PV_Resource_Int/April_May_2018_Solar_PV_Disturbance_Report.pdf

[3] Used throughout this SAR, the term DER refers to "any Source of Electric Power located on the Distribution System" from SPIDERWG's terms and definitions document: https://www.nerc.com/comm/RSTC/SPIDERWG/SPIDERWG%20Terms%20and%20Definitions%20Working%20Document.pdf
Similar definitions are underway in Project 2022-02 with the intention of mirroring the concepts in the SPIDERWG document while not needing to add many terms to the glossary.

Requested information

operation of the BPS. Despite potential impact to reliable operation, EOP-004-4 does not currently require reporting by Balancing Authorities (BAs) and Reliability Coordinators (RCs) of the loss of aggregate DERs to NERC. The purpose of EOP-004-4[4] is to "improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities." Further, NERC disturbance analysis have demonstrated net load jumps that have been attributed to DER tripping yet there is no reflection in EOP-004-4 as to the treatment of this type of event in the categories in Attachment 1. Clarity on which Event Type in Attachment 1 as well as the establishment of a threshold for reporting of loss of aggregate DER support the purpose of EOP-004 in reporting of large grid disturbances.

Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):

Some of NERC's objective in the Rules of Procedure[5] identify that the Reliability Assessment and Performance Analysis Program are to "analyze off-normal events on the Bulk Power System" and "identify the root causes of events that may be precursors of potentially more serious events". Event analysis for major events is part of the NERC's process following these disturbances, but requires a notification process to determine if a grid disturbance meets the criteria for a major event. The notification of disturbances, including both minor and major disturbances that impact the bulk power system, is required in order for the ERO Event Analysis program to perform their procedures. The proposed project provides clarity for the attribution (i.e., Event Type in EOP-004) of tripping of aggregate DER and establishes a threshold for which loss of aggregate DER warrants notice to the ERO. Both objectives provide the event analysis process the information needed to conduct their reliability-focused objective.

Project Scope (Define the parameters of the proposed project):

The scope of the project is to modify EOP-004 to account for loss of aggregate DER during grid disturbances. At a minimum, the standard team should clarify how loss of aggregate DER and loss of firm load are accounted so they are not canceled by netting the two. The standard drafting team should also define a threshold for reporting of events where the loss of aggregate DER exceed such threshold. Further, as Attachment 2 specifies that the DOE OE-417 report can be submitted in lieu of the EOP-004 report, the SDT should align the forms for such instances to ensure the OE-417 form submissions cover events where aggregate amounts of DER trip above the threshold the SDT establishes.

---

[4] EOP-00404 available here: https://www.nerc.com/pa/Stand/Reliability%20Standards/EOP-004-4.pdf

[5] Quotations are from NERC Rules of Procedure, available here: https://www.nerc.com/AboutNERC/RulesOfProcedure/NERC%20ROP%20effective%2020220825_no%20appendicies.pdf

Requested information
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification[6] which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.,* research paper) to guide development of the Standard or definition):
DERs are generation resources that are on the distribution system, and they sometimes are netted with load. As such, the loss of aggregate DER on the system can be interpreted to fill both generation loss and firm load shedding categories of Attachment 1 of EOP-004, so clarity is needed to account for DER in the reporting form. Further, the linkage of EOP-004 to OE-417 reporting should also be considered for Attachment 2 such that loss of aggregate DER reported on the DOE's OE-417 report that is accepted in lieu of EOP-004 also covers the identified threshold of aggregate DER loss in the proposed revisions. SPIDERWG recommends that a standard drafting team review and revise EOP-004-4 to require reporting, including the threshold and timing for reporting, of the loss of aggregate DERs to NERC. These are accomplished by: 1) Requiring of reporting of loss of aggregate DERs by applicable entities. The SDT should ensure that the chosen registered entities applicability does not prevent notification of the loss of aggregate DER to the ERO during grid disturbances. The SDT should consider both wide-area and local (e.g., transmission to distribution interfaces) applicability when determining its chosen entities. 2) Establishing a monitored threshold[7] that would indicate a loss of aggregate DER has occurred. The SDT should ensure their threshold and timing of reporting does not dramatically increase the number of extraneous events reported by the applicable entities. 3) Ensuring consistency of reporting by the forms accepted for this reporting in the Attachments of the Reliability Standard. 4) Determining if the DER loss event type above should exist independent of other EOP-004 event types, or be explicitly included in one of the current event types. The SDT should ensure that this event type is clear as it relates to the generation and load event types already listed. Monitoring of net load quantities can attribute the trajectory to load or DER contributions. The SDT should ensure and allow reporting of "potential" DER loss as part of their changes rather than require a certainty that such performance was 100% DER or 100% load. The SDT should identify other event types for the chosen applicable entities in 1) to determine if a separate event type improves or degrades clarity in the EOP-004 Reporting Form in Attachment 2 for gross load and DER interactions.

---

[6] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

[7] The SDT can consider monitoring net load (that includes loss of aggregate DER and increases in gross load) at a transmission to distribution interface to measure against the established threshold. The aggregate of such interfaces for an applicable entity is intended to be the monitored value for the SDT determined threshold. The SDT can also consider regional variations in establishing the loss of aggregate DER thresholds akin to other established EOP-004-4 thresholds.

Requested information
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
The material costs are unknown. This project requires the reporting of loss of aggregate DER, which may require additional staffing should bulk disturbances result in wide-spread tripping of aggregate DER. However, net loading quantities currently tracked by BAs, RCs, and TOPs to run their Operating Planning Assessments, Real-Time Assessments, and real-time monitoring of their area are able to track loss of aggregate DER, so additional metering is unlikely to be needed[8] to meet the scope of changes of this SAR. The metering of T-D Interfaces as net load here can capture the response of gross load and aggregate DER output for that interface.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
There are no required alterations to BES Facilities based on this project. The project focuses on reporting requirements of entities, which are not BES Facilities.
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g.*, Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Impacted: Reliability Coordinator (RC), Balancing Authority (BA), and Distribution Provider (DP) Potentially Impacted: Transmission Owner (TO) and Transmission Operator (TOP)
Do you know of any consensus building activities[9] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
This SAR has been submitted through the RSTC and has been vetted by the SPIDERWG membership. The SPIDERWG membership includes BAs, RCs, TOs, TPs, TOPs, PCs, and DPs. The SAR drafting has been circulated to the Event Analysis Subcommittee and the Performance Analysis Subcommittee under the RSTC. The SPIDERWG recommended this standard be revised in *White Paper: SPIDERWG NERC Reliability Standards Review*.[10]
Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?

---

[8] Major jumps in this metered net load can indicate DER tripping.

[9] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

[10] Paper available here: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Whitepaper_SPIDERWG_Standards_Review.pdf

Requested information

This SAR is covering the aggregate loss of DER and the development of a threshold to notify the ERO when such losses exceed the threshold. The Inverter-Based Resources Subcommittee has recently submitted an EOP-004 SAR that covers bulk-connected equipment, which is currently approved and progressing under Project 2023-01.[11] While different scopes and risks, the projects are covering the same Reliability Standard and complement each other. The Standards Committee can coordinate teams working on the same Reliability Standard, and even place both SARs in the same project should that be feasible.

This SAR also uses the term "DER" that is being defined in the Project 2022-02[12] team for the NERC Glossary of Terms used in Reliability Standards. The team for this SAR should use Project 2022-02's definition for any changes to standard language to clarify reporting of DERs.

Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.

The SPIDERWG considered Standards revisions alongside compliance implementation guidance and reliability guidelines. Neither compliance implementation guidance nor reliability guidelines were determined to be sufficient for the risk identified by SPIDERWG in their consensus-based white paper above. Reliability guidelines or compliance implementation guidance are not able to add the clarity if DER should be handled as a separate reporting category entirely, as part of the generation category of EOP-004 (or a subpart of current thresholds), or as a potential to reduce the firm load shedding threshold. Such ambiguity is further enhanced SPIDERWG guidance in the white paper identified reliability guideline for state-of-the-art detection is planned, but does not cover the needed clarity in the notice to the ERO for contributing factors of a disturbance as identified in the SAR. Such guidance and practices are to include improved monitoring of aggregate DER outside of the current capabilities identified above.

Reliability Principles

Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.

☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☒	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.

---

[11] Project page available here: https://www.nerc.com/pa/Stand/Pages/Project-2023-01-EOP-004-IBR-Event-Reporting.aspx

[12] Project page available here: https://www.nerc.com/pa/Stand/Pages/Project2022-02ModificationstoTPL-001-5-1andMOD-032-1.aspx

Reliability Principles	
☐	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☐	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
None	N/A

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).	
☐ Draft SAR reviewed by NERC Staff ☐ Draft SAR presented to SC for acceptance ☐ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking

1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the NERC Help Desk. Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	Reporting of Aggregate loss of DER during Grid Disturbances in EOP-004		
Date Submitted:	MM/DD/2023		
SAR Requester			
Name:	Shayan Rizvi, NPCC (NERC SPIDERWG Chair) John Schmall , ERCOT (NERC SPIDERWG Vice-Chair)		
Organization:	The NERC System Planning Impacts of DER Working Group (SPIDERWG)		
Telephone:	Shayan – 212-840-1070 John – 512-248-4243	Email:	Shayan – srizvi@nppc.org John – john.schmall@ercot.com
SAR Type (Check as many as apply)			
☐ New Standard ☒ Revision to Existing Standard ☐ Add, Modify or Retire a Glossary Term ☐ Withdraw/retire an Existing Standard		☐ Imminent Action/ Confidential Issue (SPM Section 10) ☐ Variance development or revision ☐ Other (Please specify)	
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☐ Regulatory Initiation ☐ Emerging Risk (Reliability Issues Steering Committee) Identified ☐ Reliability Standard Development Plan		☒ NERC Standing Committee Identified ☐ Enhanced Periodic Review Initiated ☒ Industry Stakeholder Identified	
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
Recent large-scale disturbances (e.g., the August 2019 disturbance in the United Kingdom~~)~~[1] or the April and May 2018 disturbances in the United States[2]) have demonstrated that unexpected loss of DERs[3] as part of the entire set of generation assets participating during BPS faults can further compromise reliable			

---

[1] Available: https://www.ofgem.gov.uk/publications/investigation-9-august-2019-power-outage

[2] Available: https://www.nerc.com/pa/rrm/ea/April_May_2018_Fault_Induced_Solar_PV_Resource_Int/April_May_2018_Solar_PV_Disturbance_Report.pdf

[3] Used throughout this SAR, the term DER refers to "any Source of Electric Power located on the Distribution System" from SPIDERWG's terms and definitions document: https://www.nerc.com/comm/RSTC/SPIDERWG/SPIDERWG%20Terms%20and%20Definitions%20Working%20Document.pdf
Similar definitions are underway in Project 2022-02 with the intention of mirroring the concepts in the SPIDERWG document while not needing to add many terms to the glossary.

Requested information
operation of the BPS. ~~Recent large-scale disturbances (e.g., the August 2019 disturbance in the United Kingdom)[4] have demonstrated that unexpected loss of DERs during BPS faults can compromise reliable operation of the BPS.~~ Despite potential impact to reliable operation, EOP-004-4 does not currently require reporting by Balancing Authorities (BAs) and Reliability Coordinators (RCs) of the loss of aggregate DERs to NERC. The purpose of EOP-004-4[5] is to "improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities." Further, NERC disturbance analysis have demonstrated net load jumps that have been attributed to DER tripping yet there is no reflection in EOP-004-4 as to the treatment of this type of event in the categories in Attachment 1. Clarity on which Event Type in Attachment 1 as well as the establishment of a threshold for reporting of loss of aggregate DER support the purpose of EOP-004 in reporting of large grid disturbances.
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):
Some of NERC's objective in the Rules of Procedure[6] identify that the Reliability Assessment and Performance Analysis Program are to "analyze off-normal events on the Bulk Power System" and "identify the root causes of events that may be precursors of potentially more serious events". Event analysis for major events is part of the NERC's process following these disturbances, but requires a notification process to determine if a grid disturbance meets the criteria for a major event. The notification of disturbances, including both minor and major disturbances that impact the bulk power system, is required in order for the ERO Event Analysis program to perform their procedures. The proposed project provides clarity for the attribution (i.e., Event Type in EOP-004) of tripping of aggregate DER and establishes a threshold for which loss of aggregate DER warrants notice to the ERO. Both objectives provide the event analysis process the information needed to conduct their reliability-focused objective.
Project Scope (Define the parameters of the proposed project):
The scope of the project is to modify EOP-004 to account for loss of aggregate DER during grid disturbances. At a minimum, the standard team should clarify how loss of aggregate DER and loss of firm load are accounted so they are not canceled by netting the two. The standard drafting team should also define a threshold for reporting of events where the loss of aggregate DER exceed such threshold. Further, as Attachment 2 specifies that the DOE OE-417 report can be submitted in lieu of the EOP-004 report, the SDT should align the forms for such instances to ensure the OE-417 form submissions cover events where aggregate amounts of DER trip above the threshold the SDT establishes.

~~[4] Available: https://www.ofgem.gov.uk/publications/investigation-9-august-2019-power-outage~~

[5] EOP-00404 available here: https://www.nerc.com/pa/Stand/Reliability%20Standards/EOP-004-4.pdf

[6] Quotations are from NERC Rules of Procedure, available here: https://www.nerc.com/AboutNERC/RulesOfProcedure/NERC%20ROP%20effective%2020220825_no%20appendicies.pdf

Requested information

Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification[7] which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.,* research paper) to guide development of the Standard or definition):

DERs are generation resources that are on the distribution system, and they sometimes are netted with load. As such, the loss of aggregate DER on the system can be interpreted to fill both generation loss and firm load shedding categories of Attachment 1 of EOP-004, so clarity is needed to account for DER in the reporting form. Further, the linkage of EOP-004 to OE-417 reporting should also be considered for Attachment 2 such that loss of aggregate DER reported on the DOE's OE-417 report that is accepted in lieu of EOP-004 also covers the identified threshold of aggregate DER loss in the proposed revisions.

SPIDERWG recommends that a standard drafting team review and revise EOP-004-4 to require reporting, including the threshold and timing for reporting, of the loss of aggregate DERs to NERC. These are accomplished by:

~~2)~~1) Requiring of reporting of loss of aggregate DERs by applicable entities. The SDT should ensure that the chosen registered entities applicability does not prevent notification of the loss of aggregate DER to the ERO during grid disturbances. The SDT should consider both wide-area and local (e.g., transmission to distribution interfaces) applicability when determining its chosen entities.

~~3)~~2) Establishing a monitored threshold[8] that would indicate a loss of aggregate DER has occurred. The SDT should ensure their threshold and timing of reporting does not dramatically increase the number of extraneous events reported by the applicable entities.

3) Ensuring consistency of reporting by the forms accepted for this reporting in the Attachments of the Reliability Standard.

4) Determining if the DER loss event type above should exist independent of other EOP-004 event types, or be explicitly included in one of the current event types. The SDT should ensure that this event type is clear as it relates to the generation and load event types already listed. Monitoring of net load quantities can attribute the trajectory to load or DER contributions. The SDT should ensure and allow reporting of "potential" DER loss as part of their changes rather than require a certainty that such performance was 100% DER or 100% load. The SDT should identify other event types ~~identified~~ for the chosen applicable entities in 1) to determine if a separate event type

Formatted: Normal, No bullets or numbering

---

[7] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

[8] The SDT can consider monitoring net load ~~that can include~~(that includes loss of aggregate DER and ~~increasing~~ increases in gross load) at a transmission to distribution interface to measure against the established threshold. The aggregate of such interfaces for an applicable entity is intended to be the monitored value for the SDT determined threshold. -The SDT can also consider regional variations in establishing the loss of aggregate DER thresholds akin to other established EOP-004-4 thresholds.

Requested information
improves or degrades clarity in the EOP-004 Reporting Form in Attachment 2 for gross load and DER interactions.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
The material costs are unknown. This project requires the reporting of loss of aggregate DER, which may require additional staffing should bulk disturbances result in wide-spread tripping of aggregate DER. However, net loading quantities currently tracked by BAs, RCs, and TOPs to run their Operating Planning Assessments, Real-Time Assessments, and real-time monitoring of their area are able to track loss of aggregate DER, so additional metering is unlikely to be needed[9] to meet the scope of changes of this SAR. The metering of T-D Interfaces as net load here can capture the response of gross load and aggregate DER output for that interface.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
There are no required alterations to BES Facilities based on this project. The project focuses on reporting requirements of entities, which are not BES Facilities.
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g.*, Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Impacted: Reliability Coordinator (RC), Balancing Authority (BA), and Distribution Provider (DP) Potentially Impacted: Transmission Owner (TO) and Transmission Operator (TOP)
Do you know of any consensus building activities[10] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
This SAR has been submitted through the RSTC and has been vetted by the SPIDERWG membership. The SPIDERWG membership includes BAs, RCs, TOs, TPs, TOPs, PCs, and DPs. The SAR drafting has been circulated to the Event Analysis Subcommittee and the Performance Analysis Subcommittee under the RSTC. The SPIDERWG recommended this standard be revised in *White Paper: SPIDERWG NERC Reliability Standards Review*.[11]

Formatted: Justified

Formatted: Justified

---

[9] Major jumps in this metered net load can indicate DER tripping.

[10] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

[11] Paper available here: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Whitepaper_SPIDERWG_Standards_Review.pdf ~~e~~

Requested information

Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so, which standard(s) or project number(s)?

This SAR is covering the aggregate loss of DER and the development of a threshold to notify the ERO when such losses exceed the threshold. The Inverter-Based Resources Subcommittee has recently submitted an EOP-004 SAR that covers bulk-connected equipment, which is currently approved and progressing under Project 2023-01.[12] While different scopes and risks, the projects are covering the same Reliability Standard and complement each other. The ~~creation of standards projects~~Standards Committee can coordinate teams working on the same Reliability Standard, and even place both SARs in the same project should that be feasible.

This SAR also uses the term “DER” that is being defined in the Project 2022-02[13] team for the NERC Glossary of Terms used in Reliability Standards. The team for this SAR should use Project 2022-02’s definition for any changes to standard language to clarify reporting of DERs.

Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.

The SPIDERWG considered Standards revisions alongside compliance implementation guidance and reliability guidelines. Neither compliance implementation guidance nor reliability guidelines were determined to be sufficient for the risk identified by SPIDERWG in their consensus-based white paper above. Reliability guidelines or compliance implementation guidance are not able to add the clarity if DER should be handled as a separate reporting category entirely, as part of the generation category of EOP-004 (or a subpart of current thresholds), or as a potential to reduce the firm load shedding threshold. Such ambiguity is further enhanced SPIDERWG guidance in the white paper identified reliability guideline for state-of-the-art detection is planned, but does not cover the ~~items~~ needed clarity in the notice to the ERO for contributing factors of a disturbance as identified in the SAR. Such guidance and practices are to include ~~direct~~improved monitoring of aggregate DER ~~of output~~ outside of the current capabilities identified above.

Reliability Principles

Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.

☒	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.

---

[12] Project page available here: https://www.nerc.com/pa/Stand/Pages/Project-2023-01-EOP-004-IBR-Event-Reporting.aspx

[13] Project page available here: https://www.nerc.com/pa/Stand/Pages/Project2022-02ModificationstoTPL-001-5-1andMOD-032-1.aspx

Reliability Principles	
☒	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☐	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☐	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
None	N/A

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).	
☐ Draft SAR reviewed by NERC Staff ☐ Draft SAR presented to SC for acceptance ☐ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer

Agenda Item 14
RSTC Meeting
September 20, 2023

Support Study: Reviewing Fuel Availability for Regional Flexible Resources to Support System Variability

Action

Approve

Summary

As North America increases its reliance on variable energy resources, so too will the grid's need for firm flexible generation to support and accommodate the intermittent generation. During this transition, flexible generation and the availability of fuel, primarily natural gas, will play a critical role in maintaining reliability and providing essential reliability services, specifically ramping capability.

The EGWG membership has the knowledge and the desire to support this much-needed study on an as-needed basis and seeks approval of the RSTC to add it to its upcoming work plan.

Concept Paper for Potential Phase I Study: Reviewing Fuel Availability for Regional Flexible Resources to Support System Variability

April 3, 2023

Federal, regional, and state policies, combined with industry commitments and investment in new technologies driven by economics, are providing a pathway to reach the stated goals of relying more on non-carbon resources to produce electricity. As we transition to greater reliance on more intermittent electricity generating resources, maintaining grid reliability will be affected by two critical components: (1) building new transmission delivery capacity that expands the use of intermittent energy to all parts of the country and (2) ensuring adequate generating resources are available to support increasing levels of variable energy resources. Firm flexible generation resources will be increasingly relied upon to accommodate higher levels of variability, and we must also ensure that the associated backstop fuels those flexible resources relied upon are readily available to accommodate new energy usage patterns such as steeper ramping requirements.

It is anticipated that significant advancements and expanded application of new technologies, such as battery storage, could allow these technologies to increasingly provide the system flexibility needed to reliably support these changes to the energy grid. Yet, during the transition, regions will continue to rely on existing flexible resources for providing services like ramping, frequency response, and inertia, in addition to demand response tools that can offset some of these requirements. Additionally, in most instances, regional assessments have not examined whether there is sufficient fuel availability and flexibility to support flexible generation resources, especially in those instances in which faster, more frequent, less certain, and steeper ramping requests are required of them. We must make sure that not only do we have adequate and diverse flexible resources in place but also that the fuels supporting those resources are readily available to support them. There are a number of types of flexible resources that the grid can rely upon but natural gas units in particular must have sufficient natural gas infrastructure in place for gas units to have the ability to quickly ramp since natural gas is not stored on location. Similarly, other fuels may have upstream issues that impact their ability to provide the flexibility required. Since the availability of fuel to support flexible resources through the transition is uncertain yet an essential component of maintaining reliability, this study is intended to fill that gap.

The energy transition is already underway yet these uncertainties regarding potential reliability risks persist. Therefore, our broad group of government and industry participants believe it is critical to expeditiously embark on a thorough examination of whether each region has sufficient flexible resources and fuel availability to support these units, especially during these early years of transition. Because of the critical importance of maintaining reliability through the transition, we believe this study must be performed using the most credible unbiased information and data available to provide a realistic assessment of potential outcomes.[1] Due to the large scope of such a study, it is more realistic to initially undertake this study in phases and prioritize regions based on those that may be

---

[1] Given that each region of the country has its own resource mix and pace of transition, analysis of balancing resource capabilities must be done at the regional level or even sub-regional levels when appropriate.

most at risk for potential gaps in resource capabilities and sufficient fuel capability to support them. On the following page, we have listed the general steps that would likely be necessary for Phase I of this analysis.

General Conceptual Parameters of Assessment:

(1) **Select Best Region(s) for Phase I of Study**. Once the group performing the study is selected, they will work with the stakeholders to determine the best region(s) to be studied in Phase I based on modeling capabilities and consideration of the region(s) that may benefit the most from filling this gap in whether there is sufficient fuel capabilities to support system ramping needs.

(2) **Examine Fuel Availability to Support Flexible Resources and Other Upstream Hindrances that Could Impact a Flexible Resources' Performance**. Using a three-to-five-year out timeframe, assess whether there are any impediments that could impact the ability of the needed flexible resources to perform as instructed.[2] **How much additional supply, transport, and delivery natural gas capacity is needed to serve all natural gas customers (to ensure electric reliability; NOT only to serve firm customers)?** Mainly, are there any upstream obstacles that could impair their ability to operate such as adequate fuel availability/fuel infrastructure? Also it may be helpful to consider the impact of emissions restrictions or bans. Some examples of areas that should be assessed include:
   a. For gas generation used for quick-ramping capabilities, examine whether there is sufficient pipeline and underground storage capacity available to accommodate expected

---

[2] In order to establish a baseline for examining the fuel requirements in a region, modelers will first need to establish a baseline of the level and mix of regional resources and an accurate estimate of the flexible resources that will be available to support increased system variability. Those steps are outlined below.

(1) **Current and Future (3 to 5 years out) Regional Resources**. Relying on studies already performed by ISO-RTOs and other regional assessments to the extent possible and credible data available from other resources, the study will document the existing resources in the region.
   a. This assessment should reflect the current level of generation resources as well as the resources needed three to five years from the date of the study during "normal" conditions. Normal conditions generally refer to peak and net-peak day for summer and winter or an entire year of operations under several scenarios that may occur under normal operating conditions. Hypothetical extreme scenarios will be explored as specific scenarios as outlined in step 3.
   b. This analysis should be as granular as possible using at least hourly assessments so that modelers can determine the usage patterns for upstream fuel (sub-hourly is preferable but recognizing that matching to natural gas availability may limit granularity to hourly).

(2) **Flexible Generation and Other Resources Used to Support System Variability.** Based on the findings in #1 above, (looking currently and 3 to 5 years out), the study will document a subset of regional resources that are or will be expected to be available and capable of providing balancing, ramping, frequency response and inertia to maintain reliability with increasing levels of variable resources on the system, based on mandated NERC performance standard.
   a. The most credible data available should be used to estimate the potential for battery storage to displace other flexible generation resources that are relied upon for balancing the system's needs.
   b. The assessment should also reflect any demand flexibility increases through formal and informal demand response actions as well as self-supply that would reduce demand and thereby decrease the need for flexible resources.
   c. If there are any shortfalls in flexible resources, the study will provide estimates of frequency, duration and scale/magnitude that may be required to address that shortfall.

more frequent ramping requirements. To what extent does the intra-day "dynamic ramping" requirements increase total natural gas infrastructure needs (e.g., additional pipeline, compression, storage).

   b. While this study is primarily focused on whether there is sufficient natural gas infrastructure to support system ramping requirements, the study will assess the risk of other upstream issues that may impact the ability to provide needed flexibility. For example:
      i. Coal supply and delivery constraints or shortfalls
      ii. Water constraints and drought conditions impacting hydro capabilities
      iii. Policy restrictions, such as emissions limitations, that may result in a limited ability of balancing resources to perform as needed

(3) **Run Other Important Sensitivities in Model to Assess Risks in Phase I.**
   a. Stressing the system to understand sufficiency of pipeline and underground storage during severe weather and other extreme conditions (large pipeline or storage out of service).
   b. Evaluate "peak ramping" requirements and the natural gas system implications during those periods (usually several hours).
   c. For the 3–5-year time period— run a scenario that assumes more-than-expected generation retirements to assess the difference between low and high generation retirements.

(4) **Develop a Model that Can Readily Assist Policymakers**. To the extent possible, federal, and state policymakers should have the ability to request modeling of specific scenarios in order to enhance their awareness of any potential reliability risks that needs to be considered.

(5) **Maintain Impartiality and Credibility by Relying on Diverse Input and Oversight**. The study should allow for the diverse group supporting the development of this concept paper to also assume the role as the lead advisory group for the study to ensure impartiality and credibility regardless of funding source.

(6) **Consider Phase II.** Based on what is learned in Phase I, the group performing the study will assess whether continued efforts should be undertaken to review other regions and adjust as needed based on best practices in Phase I.

(7) **Additional Considerations.** This study is not intended to go further than providing an assessment of whether there are reliability risks associated with insufficient fuel to meet balancing needs. However, we expect that policymakers will be able to use the results of this study as a key piece of knowledge to assess what policies should be in place to manage any reliability risks.

Agenda Item 15
RSTC Meeting
September 20, 2023

Reliability Guideline: Fuel Assurance and Fuel-Related Reliability Risk Analysis for the Bulk Power System

Action

Approve

Background

The Electric Gas Working Group (EGWG) presents to the Reliability and Security Technical Committee the following Guideline for approval.

- Reliability Guideline: Fuel Assurance and Fuel-Related Reliability Risk Analysis for the Bulk Power System (September 2023)

The rapid advancement of renewable generation, retirement of coal- and oil-fired generation, and increased use of natural gas have necessitated the need to re-evaluate the methods that the industry has historically utilized to analyze and maintain bulk power system reliability. Specifically, the increased reliance on just-in-time dispatchable generation, in particular, natural gas, to back up variable generation. This reliance requires an examination of the potential for compounded fuel/energy supply challenges and exemplifies the increased importance of thoroughly characterizing cross-sector interdependencies.

The 2020 edition of the Reliability Guideline was reviewed and updated by the EGWG.

Summary

The purpose of this reliability guideline is to ensure registered entities have relevant information to plan for the procurement of sufficient fuel to serve load and have modeled contingencies for both short-term operational horizons to long-term planning timeframes. In addition, the guideline will help registered entities to fully understand fuel supply chain risks, and offer additional conditions and constraints, especially during extreme events, to consider when performing studies. In addition, this reliability guideline may inform potential scenario analyses - e.g., loss of fuel, compressor outages, etc., but it is not intended to provide the environmental conditions contemplated under those studies.

This guideline has been posted for 45-day industry comment and includes the response to those comments.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Guideline

Fuel Assurance and Fuel-Related Reliability Risk Analysis for the Bulk Power System

~~March 2020~~

September 2023

Style Definition: Comment Text

Formatted: Left: 0.22", Right: 0.22"

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

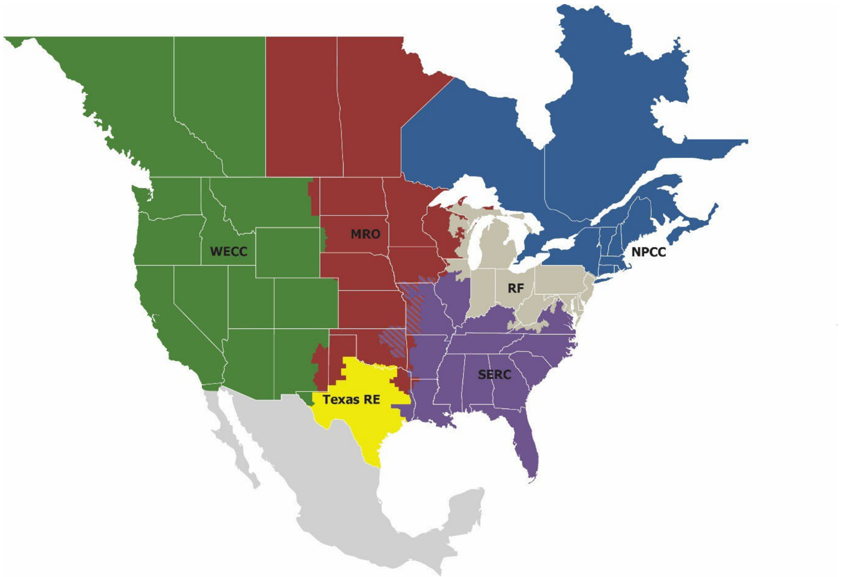
Formatted: Left: 0.22", Right: 0.22"

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

~~Preamble~~

NERC, as the Federal Energy Regulatory Commission (FERC) certified ERO,[2] is responsible for the reliability of the BES and has a suite of tools to accomplish this responsibility, including but not limited to the following:

- Lessons learned
- Reliability and security guidelines
- Assessments and reports
- The Event Analysis program
- The Compliance Monitoring and Enforcement program
- Mandatory Reliability Standards

It is in the public interest for NERC to develop reliability guidelines that are useful for maintaining and enhancing the reliability of the Bulk Electric System (BES). Reliability guidelines establish a voluntary code of practice on a particular topic for consideration and use by BES users, owners, and operators. The NERC Reliability and Security Technical Committee (RSTC), through its subcommittees and working groups, develops and triennially reviews and, as necessary, updates reliability guidelines in accordance with the procedures set forth in the RSTC Charter~~.[1]~~.[1]

Each entity registered in the NERC compliance registry is responsible and accountable for maintaining reliability and compliance with applicable mandatory Reliability Standards. Reliability guidelines include the collective experience, expertise, and judgment of the industry on matters that impact BPS operations, planning, and security. Reliability guidelines provide key practices, guidance, and information on specific issues critical to promote and maintain a highly reliable and secure BES. Reliability guidelines are not to be used to provide binding norms or create parameters by which compliance to NERC Reliability Standards are monitored or enforced. Entities are encouraged to review these guidelines in detail and in conjunction with evaluations of their internal processes and procedures. While the incorporation of guideline practices is strictly voluntary, reviewing, revising, or developing a program using these practices is highly encouraged to promote and maintain BES reliability.

Formatted: Indent: Left: 0.5", Right: 0.48", Space Before: 2.8 pt

Formatted: Font: 11 pt

~~[1] https://www.nerc.com/comm/RSTC/RelatedFiles/RSTC_Charter_Board_Approved_Nov_4_2021.pdf~~

~~[2] http://www.ferc.gov/whats-new/comm-meet/072006/E-5.pdf~~

---

[1] https://www.nerc.com/comm/RSTC/RelatedFiles/RSTC_Charter_Board_Approved_Nov_4_2021.pdf

~~Introduction~~

~~The *2019 ERO Risk Priorities Report* highlights a wide array of pertinent risks to the reliable operation of the BPS that merit attention and recommends actions that align with those risks.[3] Among the diverse risks identified in the report, utilities, generators, and other suppliers are experiencing a number of factors that increase the likelihood of fuel/energy supply challenges that exemplify the increased importance of thoroughly characterizing cross-sector interdependencies.~~

~~The rapid advancement of renewable generation, retirement of coal fired generation, and increased use of natural gas have necessitated the need to re- evaluate the methods that the industry has historically utilized to analyze and maintain BPS reliability. Increased reliance on natural gas-fired generation in various parts of North America will have increased by an estimated 55% over the period 2010–2020. This document will provide entities guidance on how to evaluate such risk factors within their own portfolios to address potential impacts on the BPS.~~

~~While this guideline addresses present concerns related to natural gas, it offers a broader perspective on the definition of "fuel assurance" in **Chapter 1** and takes a cursory look at all major fuel sources used to supply electric generation in **Chapter 2**. As each fuel type possesses a variety of limiting factors that affect its reliable delivery through its entire supply chain, **Chapter 3** describes specifically what those limiting factors may be and provides guidance to further equip planners with the requisite knowledge to assist in the development of credible fuel supply risks to analyze.~~

~~There have been a number of relevant studies performed—especially by regional transmission organizations, independent system operators (RTO/ISO), and other organizations[4] to analyze and assess generator fuel-related concerns. This guideline combines the experience gained from these studies and outlines a framework in **Chapter 4** that may be applied across all NERC Regions for effectively evaluating potential reliability risks to the BPS at all times through the lens of fuel assurance. Applying this framework for a given area will uncover where credible risks to reliability exist in terms of fuel delivery and will highlight those risks for further analysis and consideration.~~

Formatted: Font: 11 pt

Formatted: Justified, Indent: Left: 0.5", Right: 0.48", Space Before: 0 pt

Field Code Changed

Formatted: Font: 10.5 pt

Purpose

The purpose of this reliability guideline is to ensure registered entities have relevant information to (i) plan for sufficient fuel to serve load ~~plus~~and have modelled contingencies for both short-term operational horizons to long-term planning timeframes, (ii) fully understand fuel supply chain risks, and (iii) offer ~~planners~~ additional conditions and constraints, especially during extreme events, to consider when performing studies. ~~More specifically, this reliability guideline is intended to educate, inform, and provide context when entities are performing studies NERC required under current planning and operational studies.~~ This reliability guideline may inform potential scenario analyses - e.g., loss of fuel, compressor outages, etc., but it is not intended to provide the environmental conditions contemplated under those studies.

Background

The rapid advancement of renewable generation, retirement of coal-fired generation, and increased use of natural gas have necessitated the need to re-evaluate the methods that the industry has historically utilized to analyze and maintain BPS reliability. Specifically, the increased reliance on just-in-time dispatchable generation, in particular, natural gas, to back up variable generation. This reliance requires an examination of the potential for compounded fuel/energy supply challenges, and exemplifies the increased importance of thoroughly characterizing cross-sector interdependencies.

In November 2017, NERC published the *Special Reliability Assessment: Potential Bulk Power System Impacts Due to Severe Disruptions on the Natural Gas System* (*2017 NERC Special Assessment*).[5] In that report, NERC made numerous recommendations for assessing disruptions to natural gas infrastructure and related impacts to the reliable operation

~~Introduction~~

of the BPS in planning studies, several of which were assigned to the NERC ~~PC.~~

Planning Committee (PC), a predecessor to the Reliability and Security Technical Committee (RSTC). In July 2018, the PC convened a workshop to highlight ongoing "fuel assurance" discussions and studies and to convene experts from across industries to develop a plan for action. ~~Based on reactions from some workshop attendees, it was clear that some entities desired guidance around establishing "contingency selection" and other assumptions to be used for studying the impact on the BPS from fuel unavailability as well as fuel system disturbances. Transmission Planners (TPs) also desired guidance in identifying potential transmission impacts and how to evaluate the level of risk to the BPS, including the ability to serve load they should be willing to accept.~~ In November 2018, the NERC Board approved a set of recommendations developed by the PC to address issues raised in concerns from the *2017 NERC Special Assessment*. One such recommendation was the development of this reliability guideline, which that was assigned by the PC to the newly formed Electric Gas Working Group. The initial guideline was approved by the RSTC in March 2020. This document is the first revision to the March 2020 guideline and will provide entities guidance on how to evaluate such risk factors, ascertain potential impacts on the BPS, and potentially mitigate the risks.

Formatted: Justified, Indent: Left: 0.5", Right: 0.48", Space Before: 0 pt

This guideline offers a definition of "fuel assurance" in **Chapter 1** and takes a cursory look at all major fuel sources used to supply electric generation in **Chapter 2**. As each fuel type possesses a variety of physical and commercial characteristics that affect its delivery through its entire supply chain, **Chapter 3** describes specifically what those characteristics may be and provides guidance to assist planners and system operators in the development of fuel security analyses. Appendix [] includes a design basis that was approved by the RSTC in October 2022 for a potential future electric-gas study.

Formatted: Font: 11 pt

Formatted: Justified, Indent: Left: 0.5", Right: 0.48", Space Before: 0 pt

Field Code Changed

There have been a number of relevant studies performed—especially by regional transmission organizations, independent system operators (RTO/ISO), and other organizations[4] to analyze and assess generator fuel-related considerations. This guideline combines the experience gained from these studies and post-event analyses to outlines a framework in **Chapter 4** that may be applied across all NERC Regions for effectively evaluating potential reliability risks to the BPS through the lens of fuel assurance. Applying this framework for a given area will provide indications of where credible risks to reliability exist and will highlight areas for further analysis and consideration.

Though this guideline discusses planning, commonalities in the assessment techniques, processes, and procedures discussed are applicable to all time frames and may be adopted by more than just Transmission Planners and Planning Coordinators. Terms like "planner," "generator owner/operator," and "fuel supplier" are not capitalized intentionally so that the concepts presented may be considered and applied in the broadest sense as they pertain to the BES.~~In November 2018, the NERC Board approved a set of recommendations developed by the PC to address concerns from the *2017 NERC Special Assessment*. One such recommendation was the development of this reliability guideline that was assigned by the PC to the newly formed Electric Gas Working Group.~~

In accordance with Section 8 of the RSTC charter, approved Reliability Guidelines or Technical Reference Document shall be reviewed for continued applicability by the RSTC at a minimum of every third year since the last revision. The contents of this guideline encompass updates developed by the Electric Gas Working Group during its 2023 triennial review[2] that include insights and recommendations taken from the *FERC-NERC-Regional Entity Staff Report: The February 2021 Cold Weather Outages in Texas and the South Central United States*.[3] The EGWG will continue to work with NERC to gauge the effectiveness of this reliability guideline and support efforts for continued improvement and opportunities for education and information sharing.

Formatted: Normal, Left, Indent: Left: 0", Right: 0"

---

[2] INSERT RSTC APPROVAL & DATE

[3] https://www.nerc.com/pa/rrm/ea/Documents/February_2021_Cold_Weather_Report.pdf

---

[3] https://www.nerc.com/comm/RISC/Related%20Files%20DL/RISC%20ERO%20Priorities%20Report_Board_Accpeted_November_5_2019.pdf

[4] E.g., *The Eastern Interconnection Planning Collaborative Gas-Electric Interface Study* performed under the DOE grant and completed in June 2015

[5] https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_SPOD_11142017_Final.pdf

Formatted: Centered, Indent: Left: 1.58", Right: 1.57", Space Before: 2.05 pt

Formatted: Font: Bold

~~In Appendix E of the *2017 NERC Special Assessment*, NERC evaluated existing natural gas infrastructure disruption studies conducted by the industry to gain an understanding of existing planning approaches and to highlight and promote best practices. As a result of this assessment, NERC presented steps for Planning Coordinators to take when performing future analysis (see below). This guideline is intended to expand upon methods to implement these recommendations.~~

~~*2017 NERC Special Assessment* **Appendix E Recommendations**~~

~~Identify potential natural gas system contingencies and their likelihood of occurrence~~

~~Assess the impacts for each of the identified contingencies in terms of duration and amount of natural gas supply disrupted~~

~~Apply the contingency disruptions to the natural gas supply capabilities to calculate the impact on total natural gas supplies and, more specifically, the amount of natural gas available to electric generators~~

~~Determine the transmission systems ability to transport power to load under these extreme conditions~~

~~Though this guideline discusses planning, commonalities in the assessment techniques, processes, and procedures discussed are applicable to all time frames and may be adopted by more than just TPs and Planning Coordinators.~~

~~Terms like “planner,” “generator owner/operator,” and “fuel supplier” are not capitalized intentionally so that the concepts presented may be considered and applied in the broadest sense as they pertain to the BES.~~

~~The processes identified within this guide may also be applied to those organizations whose resource mix includes entitlement and bilateral transactions that have resource contingencies. Entities with such arrangements can also benefit from recognizing when limitations may potentially impact their grid operations.~~

~~The Electric Gas Working Group will work with NERC to gauge the effectiveness of this reliability guideline and support efforts for continued improvement and opportunities for education and information sharing.~~

Formatted: Left: 0.22", Right: 0.22"

Formatted: Indent: Left: 0", First line: 0", Right: 0"

Formatted: Font: Tahoma, 14 pt, Bold

Chapter 1: Fuel Assurance

~~Fuel assurance is a term that has been utilized in many forums to date but has yet to be given a formal definition. As this guideline directly relates to the conversation taking place across the industry regarding concerns with the rapidly transitioning BPS generation fleet, it is appropriate and timely for NERC to establish its definition for “fuel assurance.” Defining this term will ensure consistency and alignment with statements within this guideline and also provide clarity to the industry going forward on the most appropriate areas of focus related to fuel supply elements facing generators supporting the BPS.~~

For the purposes of this guideline, “fuel assurance” will be defined as follows:

> ***Fuel Assurance:*** *proactively taking steps to identify fuel arrangements or other alternatives that would provide confidence such that fuel interruptions are minimized to maintain reliable BPS performance during both normal operations and credible disruptive events*

Fuel Assurance is critical across all planning time horizons and continuing on to real-time operations.[4] The criteria to establish the level of confidence referenced in the definition is unique to respective planning areas and is established by planners, system operators, and/or generator owners/operators based on internal assessments, situational awareness, contractual supply arrangements, and understanding of ~~their~~ asset characteristics. ~~The role of the regional planner in addressing fuel assurance is related to but separate from actions of individual generator owners to assure fuel assurance for their units.~~ The regional planner’s focus is to assess the vulnerabilities of the entire region to withstand fuel disruptions that could impact multiple generators and impact reliable BPS performance. ~~A lack of fuel assurance to a particular generator may affect that unit’s ability to receive revenues from the market or otherwise meet their obligations to their customers but not necessarily impact the provision of reliable service to the entire region.~~The role of the system operator demands significant situational awareness and system operators would benefit from utilizing all relevant public and non-speculative non-public information available in order to facilitate reliable delivery of fuel in the operational horizon. Generator Owners/Operators should communicate timely to the system operators how the terms of their fuel and transportation contracts may impact their unit specific performance parameters and operations and whether they reasonably foresee fuel availability issues. As the fuel mix of generation and wholesale electricity market structures can vary greatly across reliability areas, this guideline does not and cannot prescribe a single approach to the process.

NERC encourages planners to proactively model, evaluate and consider specific BPS impacts based on credible events that could compromise the provision of reliable service to all or part of the region within the regional planner’s area of responsibility and to develop strategies to mitigate credible risks. Regional planners may consider modeling extreme fuel disruptions to better understand the impact of catastrophic events so that they may prepare for such emergencies. Recognizing that there is no way to anticipate or measure all potential threats and catastrophic scenarios, stakeholders and ~~regional planners~~system operators should focus on effective measures that will maintain reliable and fuel- secure BPS operations during credible events. While the individual unit owners are ultimately responsible for effectively managing the fuel ~~assurance~~needs of particular units, the ~~regional planners~~system operators, in advance of an actual contingency, should understand the risk and consequences of losing critical generators ~~and take~~. They should consider the steps necessary to limit the reliability impact of such ~~a loss should a loss of fuel delivery at a particular unit threaten reliability~~losses and select other sources of supply in advance if the risk is unacceptable.

Formatted: Left, Indent: Left: 0", First line: 0", Right: 0", Space Before: 0.3 pt

Formatted: Font: Tahoma, 8.5 pt, Bold

Formatted: Not Expanded by / Condensed by

Formatted: Not Expanded by / Condensed by

Formatted: Not Expanded by / Condensed by

Formatted: Not Expanded by / Condensed by

Formatted: Not Expanded by / Condensed by

Formatted: Not Expanded by / Condensed by

Formatted: Not Expanded by / Condensed by

Formatted: Not Expanded by / Condensed by

Formatted: Not Expanded by / Condensed by

Formatted: Not Expanded by / Condensed by

Formatted: Not Expanded by / Condensed by

Formatted: Not Expanded by / Condensed by

---

[4] Time_Horizons.pdf (nerc.com)

~~[6] https://www.pjm.com/-/media/library/reports-notices/fuel-security/2018-fuel-security-analysis.ashx?la=en~~

~~FUEL SECURITY ANALYSIS: A PJM RESILIENCE INITIATIVE~~~~[7]~~

~~In 2018, PJM performed a fuel security analysis which was designed to stress-test the PJM grid and the fuel delivery systems serving generation in PJM under a series of extreme but plausible future events (using 2023/2024 as the study year). As in any stress test, the analysis was intended to discover the point at which the PJM system begins to be impacted (i.e., when system operators initiate emergency actions) and to identify key drivers of risk. In PJM's phased approach to addressing the Fuel Assurance issue, Phase 1 involved the fuel security analysis. In Phase 2, which began in 2019, the analysis results are being used to inform PJM's stakeholder process, which will help to define fuel security attributes for PJM, location and magnitude of how many fuel secure resources or megawatts are needed, as well as determine how to value fuel secure resources. PJM may also use the results of the study to determine how best to incorporate fuel security into other aspects of its operations, markets and planning. The final Phase 3 is a cooperative effort between PJM and United States (U.S.) federal agencies to define and analyze further scenarios based on classified information about credible risks to fuel security that could have impacts on the power grid.~~

Formatted: Font: 11 pt

Formatted: Justified, Indent: Left: 0.5", Right: 0.48", Space Before: 0.05 pt

Fuel Assurance Principles

While each reliability area is unique, there are common principles for fuel assurance that may be applied more broadly to assist planners and system operators in their assessments of fuel supply reliability. Below are some examples of actions that various entities may perform to advance fuel assurance initiatives.

Formatted: Font: 10.5 pt

Formatted: Space Before: 0.5 pt

~~Markets~~

~~RTOs/ISOs that have not already done so could consider additional mechanisms for generators to meet their obligations during reserve shortages—these could be market (e.g., capacity market reforms) or out-of-market solutions while attempting to avoid out of market solutions where possible or only as a temporary measure while a market-based approach is developed. Such market rules and mechanisms would incentivize generators to maintain or enhance fuel delivery contracts. Additionally, adopting more detailed and timely procedures for communications to members when near-term fuel shortages/reliability concerns arise (e.g., upcoming shortages, disruptive weather) will allow time for generators to assess and react to fuel supply needs. RTOs/ISOs should also consider other mechanisms that would facilitate greater certainty that generators have reliable fuel options regardless of market structure (i.e., restructured or vertically integrated).~~

Formatted: Font: 11 pt

Formatted: Justified, Indent: Left: 0.5", Right: 0.48", Space Before: 0 pt

~~Generator Owners/Operators~~

~~Generator owners/operators should seek reliable delivery solutions from a transportation, commodity, and commodity procurement perspective. Monitor and evaluate risks associated with varying levels of transportation or delivery options associated with the different types of transportation (e.g., interruptible transportation, firm transportation). This evaluation must include pipeline scheduling, flow rule and constraint realities. Consider and evaluate a diverse portfolio of products that can be utilized to deliver fuel both reliably and cost-effectively; examples of these are as follows:~~

Formatted: Not Expanded by / Condensed by

- ~~Delivered bundled products~~
- ~~Firm call options for periods of heightened fuel uncertainty~~
- ~~Asset management arrangements~~
- ~~Potential purchases from suppliers with firm capabilities~~

~~[7] Id.~~

- ~~Enhanced infrastructure considerations~~
- ~~Storage capacity~~
- ~~Liquefied natural gas (LNG) options~~
- ~~Dual-fuel capability~~
- ~~Interconnection with more than one pipeline~~
- ~~On-site fuel reserves.~~

~~Generator owners/operators should consider credible fuel-related contingencies that impact their facilities and provide fuel-related facility outage concerns as necessary to the reliability authority. Lastly, where fuel delivery constraints are routinely evident, generator owners/operators should consider and investigate whether new options for fuel deliveries to a specific facility or their fleet are available.~~

Transmission Planners/Planning Coordinators

Planners should consider using steps outlined in **Chapter 4:** of this guideline to develop credible fuel-related contingencies that may be used in planning studies, including (but not limited to) Reliability Standard TPL-001 (Transmission System Planning Performance Requirements).[8] Any identified fuel-related contingencies should be evaluated for reliability risks, and planners should determine what (if any) mitigation should be put in place. Planners might consider conducting generator fuel-related surveys to determine potential risks to the fuel supply of the generators. Using the survey data, planners may perform fuel-related reliability risk analyses as described in **Chapter 4**~~:.~~. Planners should also seek and use experts familiar with regional markets and practices to help interpret and analyze the survey data.

System Operators

System gas requirements and availability are influenced by locational electrical demands and constraints and when unit commitment are made. This suggests the need for a centrally situated party to maintain a high-level of situational awareness. System operators should consider how to work voluntarily with as many stakeholders as possible through non-disclosure agreements or other mechanisms to receive non-public information that would assist their detailed understanding of grid demands and challenges and to maintain this utmost situational awareness. FERC Order 787, for example, allows interstate gas pipelines and electric transmission operators to share, on a voluntary basis, non-public operational information with each other to promote grid reliability and operational planning. System operators should consider how they can maximize the use of public and non-public information, how to best coordinate with all parties while preserving the confidentiality of the non-public information, and make decisions that facilitate the proper utilization of gas infrastructure, leverage the value of precedent transportation arrangements, and respect the pipeline operational constraints.

Generator Owners/Operators

Generator owners/operators should seek reliable delivery solutions from a transportation, commodity, and commodity procurement perspective. BES reliability risks associated with emissions limits, fuel availability, transportation or delivery options should be monitored and evaluated. For example, with regard to use of natural gas, consider the "firmness" of the transportation agreement to include policies, processes or tariff provisions which could restrict gas flow (e.g., NAESB pipeline scheduling timeline), flow rule and constraint realities; and the commodity availability at the relevant trading hub.

Generator owners/operators should consider credible fuel-related contingencies that may impact their facilities and provide fuel-related facility outage concerns as necessary to the relevant reliability authority. Planning for credible fuel-related contingencies strengthens a generator's ability to ensure it can run when called upon during critical events. Lastly, where fuel delivery constraints are routinely evident, generator owners/operators should consider and investigate whether new options for fuel deliveries to a specific facility or their fleet are available.

Formatted: Font: 10 pt

Formatted: Body Text, Line spacing: Multiple 0.06 li

Formatted: Left: 0.22", Right: 0.22"

Formatted: Not Expanded by / Condensed by

Formatted: Font: 11 pt

Formatted: Justified, Indent: Left: 0.5", Right: 0.48"

Formatted: Font: 11 pt

Formatted: Justified, Indent: Left: 0.5", Right: 0.48", Space Before: 0 pt

Formatted: Not Expanded by / Condensed by

Formatted: Font: 10 pt

Formatted: Body Text, Line spacing: Multiple 0.06 li

Formatted: Font: 10 pt

Formatted: Body Text, Line spacing: Multiple 0.06 li

---

[8] See NERC Standard TPL-001-4 – Transmission Planning Performance Requirements, Table 1 –Steady State & Stability Performance Extreme Events, 3.a.i.

Formatted: Font: 10 pt

Formatted: Body Text, Line spacing: Multiple 0.06 li

Chapter 2: Electric Generation Fuel Supply Primer

This section describes the supply chain of each major generator fuel supply type at a high level. It describes illustrative challenges that may be encountered between production and consumption as well as other viable considerations specific to each fuel type. These considerations will assist planners in forming realistic assumptions when developing their own fuel assurance and reliability risk analysis.

Natural Gas

Over the last ~~[10]~~18 years~~,~~ domestic production of natural gas has ~~increased tremendously~~doubled[5], mostly due to new well development techniques that have lowered production costs and allowed extraction in previously uneconomic or technologically inaccessible fields. The relative economics of natural gas, coupled with ~~tighter~~tightening environmental regulations on other fuel types, ~~has~~ led to the ~~proliferation~~increased development of new gas-fired generation~~.~~ in some regions. Additionally, gas-fired combustion turbines and reciprocating engines have relatively fast-start times and ramping capabilities that complement the variable ~~generation~~nature of wind and solar resources that are being developed in many parts of the United States at accelerating rates. Consequently, ~~with increased renewable penetration, and the retirement of nuclear and coal in certain bulk electric regions, the bulk electric system is becoming more dependent on the natural gas system from well-head to burner tip. NERC has previously reported in its *2017 Special Assessment*, that disruptions to natural gas delivery may occur resulting from adverse events, such as line breaks, well freeze-offs, hurricanes, floods, storage facility outages, or infrastructure attacks.[17] Similarly, the pipeline system can be impacted by events that occur on the electric system (e.g., loss of electric motor driven compressors).[18] From the perspective of gas-fired electric generators, there are two distinct natural gas reliability risks associated with natural gas supply: unavailability and curtailment. Unavailability, the inability of a gas-fired generator to schedule gas deliveries to their location, may occur for a number of reasons, but ultimately results in no flow of gas. Interruption, the condition when a gas-fired generator scheduled gas but less than the scheduled quantity was shipped, may also occur for several reasons. Therefore, a fundamental understanding of the natural gas supply chain is necessary to understand how they may affect electric reliability.~~ the bulk electric system increasingly relies on the gas industry to deliver more natural gas with greater flexibility.

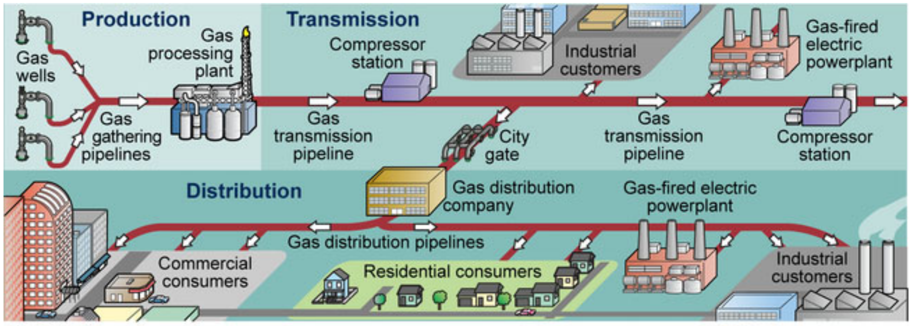
These increased new demands on the natural gas industry are highlighting issues that planners and system operators may not have had to grapple with previously but which are becoming more important to ensuring electric reliability. The physical differences between systems that convey compressed pipeline quality gas and electricity drive operational and administrative differences, which manifest through fundamental differences in scheduling and operational flexibility. Clearly, the throughput capacity of the natural gas system is of paramount importance; however, the timing that shippers nominate fuel and how that fuel must be taken is of equal importance and might, in many circumstances, impact their ability to run when called upon. Pipeline operators' nomination and scheduling systems, and ultimately flow, are timed to ensure gas system reliability. Unlike the electric grid, pipeline operators require time to configure their systems in advance, and constrained conditions may limit system operators' ability to call on gas-fired generators if fuel has not been nominated in accordance with pipeline tariff nomination deadlines and flow rules. Additionally when pipelines are flowing at near or maximum capacity, pipeline operational flexibility that is typically provided on a best efforts basis and supports non-spinning Operating Reserves may not be available. Both conditions require planners and system operators to examine the scheduling constraint timelines and the physical realities of the gas systems when performing studies and constructing day ahead operating plans, especially during stressed conditions. However, the limitations and constrained conditions may not exist universally and requires a careful, regional analysis of the natural gas supply chain. This section breaks the natural gas supply chain into segments, describes their function at a high level, and identifies areas of potential risk.

---

[5] https://www.eia.gov/dnav/ng/hist/n9070us2A.htm

The natural gas supply and delivery chain includes three major segments, listed below:

- **Production and Processing**
- **Transmission and Storage**
- **Distribution**



Source: GAO analysis of Energy Information Administration and Natural Gas Council documents. | GAO-20-658

The rest of the section describes the characteristics of each segment and considerations relevant to the electric industry.

Production and Processing

Natural gas is primarily found in reservoir pools and shale rock formations in the earth and brought to the surface through production wells ~~by processing plants that heavily rely on electric power to operate.~~. Unprocessed natural gas withdrawn from natural gas or crude oil wells ~~may~~ is usually “wet” natural gas because, along with methane, it contains natural gas liquids (NGL)—ethane, propane, butane, and pentane—and water vapor. Since methane, the primary constituent of pipeline-quality gas, remains in its gas phase down to -260 deg F, wellheads are more susceptible to “freeze-offs” when the wells have relatively high fractions of water vapor, which freezes in the wellhead or gathering system blocking the flow of gas. While the most effective method of preventing wellheads from freezing is to remove the water, this is not always cost-effective or possible. Another common method is to inject methanol into the gas stream for later removal. Producers may also be able to increase production in other areas or rely on using supplies ~~of~~they have natural gas in storage.[16] Some wellhead natural gas is sufficiently dry, and less prone to “freeze-offs~~,”~~.” Additionally, electrically-driven equipment, including compressors and ~~satisfies pipeline transportation standards without~~ processing~~.~~ facilities, used in the natural gas supply chain should be reviewed to ensure that it is on a critical circuit and would not be cut during manual load shedding, or that coordination occurs with operators of these facilities with sufficient time to facilitate switching to co-located non-electrically driven equipment or on-site backup power generation. It is imperative that both planners and system operators understand ~~where locally consumed fuel is produced~~the diversity of production sources, what risks fuel producers face, and how those producers ~~face, and how the producers~~ may ~~be mitigating the~~mitigate those risks.

From the wellhead, natural gas is sent to processing plants where water vapor and nonhydrocarbon compounds are removed and NGLs are separated from the wet gas and sold separately. ~~Historically,~~ Like any other type of operations in the gas and power sector, processing ~~facilities have [NOT?] materially affected~~plant operations can be impacted during critical events, and natural gas ~~supply chain risks been a bottleneck in the natural~~must be processed in order to meet interstate gas ~~supply chain…~~pipeline quality specifications. The processed natural gas is called dry, consumer-grade, or pipeline-quality natural gas. If the natural gas is not processed, and a pipeline cannot blend the gas, in most instances it will not be accepted into the interstate gas pipeline system. The processed natural gas is then transported via gathering systems into either intra- or interstate gas pipelines.~~-~~

~~Natural gas procurement is integral to this production and processing discussion. Specifically, timely fuel procurement that complies with pipeline nomination cycles, flow rules and transacted at locations such that, then effective, pipeline constraints will not impede delivery are as important to electric generation supporting a reliable BPS as the production and processing details, discussed above.~~

Formatted: Indent: Left: 0"

Transmission and Storage

Large-diameter interstate and intrastate pipeline transmission systems transport processed natural gas to large-volume customers (e.g., local distribution companies (LDCs), natural gas-fired power generation, industrial users, gas marketers). Processed natural gas is also transported to various storage facilities for future consumption. Compressor stations are located along the pipelines and storage network to maintain pressure at serviceable levels. In most cases, compressor units are powered by the natural gas in the pipelines. ~~Some~~However, some compressor stations may have both natural gas and electric or even diesel-driven compressor units, and; others may rely solely on electric power. As mentioned above, it's important that pipeline operators identify their electric compressors and communicate those sites to the ISO/RTO so that, should an event warrant load shedding, those units are prioritized and curtailed last and restored first.

While the natural gas transmission system may continue to operate even with the failure of as many as half of the compressors, the pressure may not remain high enough to meet the specific pressure requirements of each power generator interconnected to the pipeline~~.[10] Many~~, which can range from around 100 psi up to more than 1,000 psi for some turbine models.[6] To add redundancy, many gas-fired generators have on-site boost compression that ~~is capable of increasing~~increases the pressure of the pipeline~~-~~-delivered natural gas to the combustion inlet pressure required by the unit. ~~It is important to identify which generation~~Generation facilities that do not have boost compression ~~and~~ may be more susceptible to outage under certain pipeline operating conditions.

Typically, limited supply and transportation disruptions can be managed through substitution, transportation rerouting, on site peaking supply, third-party delivered supply contracts, and storage services (though such infrastructure redundancy is much more limited in certain portions of North America, such as the Northeast). However, unlike electricity through a transmission line, gas flows much more slowly through a pipeline, which also necessitates more advance planning by shippers and end users. Pipeline operators carefully manage the flows into and out of their pipelines, especially when demand on the pipeline is expected to be high, through scheduling procedures, alerts, notices, operational flow orders (OFOs~~),~~)[7], and ultimately imposing over-run penalties restricting withdrawals if the shipper disregards the OFO~~.~~ A fundamental understanding of pipeline operations and ~~commercial~~market constructs is ~~helpful to~~necessaryto understand how gas scheduling may impact electric reliability ~~under certain conditions~~.

~~The Federal Energy Regulatory Commission (FERC or "Commission") regulates interstate natural gas transportation and storage, and requires pipeline and storage operators to post a significant amount of public data on their websites, including information about pipeline operating and operationally available capacity by receipt and delivery point, critical and non-critical notices, identification of firm pipeline shippers, capacity release information, shipper-specific data, etc. Additionally, certain entities that have electric reliability responsibility may also receive non-public data from interstate pipeline and storage operators, as well as LDCs, (and vice versa) per FERC Order 787 to maintain and enhance grid reliability[8]. Intrastate pipelines are typically under the jurisdiction of state regulatory authorities and the publicly available information publicly available varies widely from state-to-state.~~

---

[6] https://gasturbineworld.com/shop/performance-specs/2022-performance-specs-38th-edition/

[7] An Operational Flow Order is a mechanism to protect the operational integrity of the pipeline. It requires shippers to balance their gas supply with their usage on a hourly and/or daily basis, within a specified balance, per the tariff's requirements. It is not a curtailment.

~~[8] Add cite~~

Formatted: Indent: Left: 0.5", Right: 0.48"

~~The interstate pipeline industry is contract-based. Pipeline and storage companies contract with customers (or "shippers") in accordance with the terms of FERC-approved agreements and tariffs. Shippers select transportation (for e.g., firm, no notice, or interruptible, park and loan) and storage services based on the level of certainty and reliability desired. Firm transportation ("FT") is a reservation of capacity on the pipeline from the origin ("receipt point specified ") to the designated facility ("delivery point"). Pipelines are required to honor all firm service contract nominations, provided the force majeure conditions do not impact the shipper tenders the natural gas supply, the natural gas pipeline capacity remains available (assuming that another firm transportation shipper has not subscribed in an earlier NAESB cycle to the point), and there are no service disruptions on the pipeline, such as a force majeure event, impacting the pipeline's ability to deliver.[9] Most interstate pipelines also offer no-notice firm transportation, where the pipeline must stand ready to serve the shipper at any time during the Gas Day. These services typically require the shipper to nominate (and the shipper to have the natural gas supply) and also require the shipper to transport gas ratably. Interruptible transportation ("IT") service is offered as residual capacity after firm shippers are served and is usually purchased in daily increments. During periods of high usage and system constraints, pipelines may not be able to schedule interruptible customers because firm capacity is being fully utilized.~~

~~Pipeline shippers or potential shippers can also attempt to purchase pipeline or storage capacity on the secondary market through shipper capacity release, assuming a willing firm pipeline shipper is willing to release its capacity, or directly from a gas marketer who holds firm transportation service on the pipeline.~~

~~NAESB has developed uniform nomination windows for shippers to "nominate" gas prior to and during the gas day, which currently runs from 9:00am – 9:00am CCT. While shippers may nominate during any nomination cycle, per FERC policy FT shippers may "bump" scheduled IT shippers up to the Intraday 3 cycle (7:00pm CCT intraday). Another important consideration is that pipeline operators are not obligated to flow the gas until after the nomination cycle ends. In some cases, this delay from the nomination cycle closing until gas is allowed to flow to the shipper is up to 4 hours. The flow lag is dependent upon the specific pipeline, and planners and system operators should consult the specific pipeline tariffs for more information. Contracting firm transportation capacity alone does not guarantee delivery of natural gas supplies at a specific location and time. Firm supply delivery must also consider pipeline nomination cycles, flow rules and then effective constraints.~~

~~In order to maintain their own, and their shippers' operational reliability, particularly during high demand periods, pipeline operators may issue OFOs to require shippers to take gas "ratably," per the tariff's requirement." This means that shippers must flow its daily scheduled quantity of gas in 1/24th hourly increments, with some small percentage of hourly imbalances but getting back in balance by the end of the day. Should a shipper disregard the OFO, significant penalties may accrue for non-compliance.~~

Formatted: Indent: Left: 0.5", Right: 0.48"

~~However, some pipelines also offer "enhanced" transportation services, which functions like FT coupled with storage. This service allows shippers to call on gas "non-ratably" and generally shortens the flow lag from normal FT or IT service. Enhanced service should not be mistaken for "no-notice" or on-demand service. Consequently, current recourse pipeline services may not be well-suited to serve non-spinning Operating Reserves, which require electricity to be generated with little or no advance notice and gas at large rates to be delivered non-uniformly.~~

~~In addition to transportation services, customers also purchase the physical commodity directly from a gas producer or from a gas marketer to receive natural gas at contracted points into the applicable transportation agreements and/or at other points of delivery at their respective interconnection points or market center. Larger volume customers (e.g., LDCs and electric generation facilities) may also purchase natural gas upstream at or near the point of production and contract for pipeline service to transport the commodity to the point of delivery. In addition, based on market conditions, these entities and other market participants may purchase natural gas at a market center and contract for transportation from that point to a delivery point(s). Also, market participants may purchase a bundled commodity and transportation package from marketers, who deliver the natural gas using the pipeline capacity for which they have contracted or through utilization of the established secondary bilateral market for capacity and commodity.~~

Formatted: Not Expanded by / Condensed by

Distribution

Intrastate transportation, balancing, storage, and distribution of natural gas by LDCs is subject to state regulation. LDCs are regulated by most states as local natural gas utilities that have an obligation to serve ~~their firm core customers—~~the customers for which the system is built to serve reliably (e.g., residential and commercial heating

---

~~[9] *See* 18 C.F.R. § 284.7(a) (3).~~

customers). ~~Similar to interstate pipeline operations, during periods of high usage and system constraints, LDCs may call on interruptible customers to cease gas usage temporarily.~~ State statutes and public utility regulations may allow ~~an LDC~~intrastate pipelines and LDCs to curtail services to some industrial or non-core customers, possibly including power generators, during emergencies to maintain the operational integrity of the system and/or maintain natural gas service to designated high-priority customers. Historically, these state regulatory requirements give the highest priority to residential (essential human need) and small commercial customers without short-term alternatives.

Pipeline Tariffs and Contracting Arrangements

The interstate pipeline industry is contract-based

~~Certain characteristics of the natural gas system contribute to its reliability and resilience. The natural gas transportation network is composed of an extensive network of interconnected pipelines that offer multiple pathways for rerouting deliveries in the unlikely event of a physical disruption. Each customer's ability to use such alternate pathways and capacity to maintain natural gas delivery will depend upon the rights specified in the customer's transportation contract.[11] In addition, pipeline capacity is often increased by installing two or more parallel pipelines in the same right-of-way (called pipeline loops), making it possible to shut off one loop while keeping the other in service.[12] In the event of one or more compressor failures, natural gas pipelines can usually continue to operate at pressures necessary to maintain deliveries to pipeline customers (at least outside the affected segment) subject to the constraints that some power generators may experience due to location and pressure requirements as noted above.[13] "Line pack" in the pipelines is routinely used as necessary to provide some additional operational flexibility.[14] It can facilitate non-ratable flows and support pipeline reliability as~~

~~***Line pack*** *is the usable volume of natural gas contained within the pipeline network at any given time. It allows natural gas received in one area of a pipeline system to be delivered simultaneously elsewhere on the system.*~~

~~***Line pack*** *is the usable volume of natural gas contained within the pipeline network at any given time. It allows natural gas received in one area of a pipeline system to be delivered simultaneously elsewhere on the system.*~~

~~[10] Massachusetts Institute of Technology, Lincoln Laboratory, "Interdependence of the Electricity Generation System and the Natural Gas System and Implications for Energy Security," May 15, 2013.~~

~~[11] NGC, *Natural Gas Systems: Reliable & Resilient* at p. 10 (July 2017).~~

~~[12] *Id.*~~

~~[13] *Id.*~~

~~[14] *Id.*~~

Formatted: Justified, Indent: Left: 0.5", Right: 0.48"

Formatted: Font: 11 pt

Formatted: Justified, Indent: Left: 0.5", Right: 0.48", Space Before: 0 pt

Formatted: Indent: Left: 0.5", Right: 0.48"

~~a temporary buffer for imbalances. However, line pack must be kept reasonably stable throughout the system to preserve delivery pressure and system capacity. Thus, line pack neither creates incremental capacity nor is it a substitute for appropriate transportation contracts, however, it can support sustained operation in the short termshort-term following a disruption.~~

~~Further, the existence of geographically dispersed production and storage and their locations acrosson different parts of the pipeline and distribution system also provide flexibility to maintain service in the event of a disruption on parts of the transportation and distribution system.~~~~[15]~~

, and understanding the supply and transportation fuel arrangements requires having a basic knowledge of these contract terms and conditions. Shippers that are interconnected directly to interstate facilities contract with the pipeline and storage operators in accordance with the terms of FERC-approved agreements and tariffs. Gas-fired generators purchase bundled commodity supply and transportation services from a third-party marketer or an exchange, or enter into commodity and transportation contracts separately. Marketers either hold the transportation service outright or offer capacity released by other shippers with firm entitlement rights under an asset management agreement. The entitlement holder may not need all of its capacity at all times and allow marketers to re-sell released capacity to offset the entitlement holder's fixed reservation cost. However, it is important to note that the volume and liquidity of this secondary market moves inversely to the demands of firm shippers. That is, when gas demand is highest, shippers that have not made prior arrangements may not be able to obtain the bundled fuel and transportation in the secondary market. Shippers that are interconnected to intrastate pipelines or to LDCs will have contracting arrangements unique to the jurisdiction and the contracting parties; users are advised to consult the facility-specific contracts for additional details.

Interstate shippers may select transportation and storage services based on the level of certainty and reliability desired. Some gas-fired generators contract for firm transportation ("FT"), which is a reservation of capacity on the pipeline from the origin ("receipt point specified") to the designated delivery point. The delivery point is usually a city gate (if the generator is connected to the LDC), an interconnecting pipeline, or the gas meter at the generator's facility. The receipt points may vary and a few examples include generators holding FT:

- only on a short lateral that interconnects to an interstate pipeline;
- on segments of an interstate pipeline that are known to be constrained; or
- to a liquid trading hub or a dedicated storage facility;

Other generators that are interconnected to a main pipeline within a liquid trading hub may not enter into a transportation contracts. On the other hand, some generators may contract for FT and storage, which may be classified as "enhanced" transportation services. This contracted service allows shippers to call on gas "non-ratably" and generally shortens the flow lag from normal FT or IT service. Enhanced service should not be mistaken for "no-notice" or on-demand service, which is a premium service in which the pipeline commits to serve the shipper when called upon, yet typically is ratable service. Consequently, current FT recourse pipeline services may not be well-suited to serve non-spinning Operating Reserves, which require electricity to be generated with little or no advance notice and gas at large rates to be delivered non-uniformly. The intent is not to enumerate every possible contracting combination but to illustrate that the contracting arrangements are extremely varied and may not be the primary determinant of gas availability.

Contracting firm transportation capacity alone does not guarantee delivery of natural gas supplies at a specific location and time. Firm delivery must also consider a purchase of fuel (sufficiently in advance of when needed), pipeline nomination cycles, flow rules, and then-effective pipeline constraints. The North American Energy Standards Board ("NAESB") has developed uniform nomination windows for shippers to "nominate" gas prior to and during the gas day, which currently runs from 9:00am – 9:00am Central Clock Time ("CCT"). While shippers may nominate during any nomination cycle, during high demand periods most gas deliveries are nominated and scheduled at the Timely Nomination Cycle. Therefore, it is important for a shipper to nominate at the earliest cycle

Formatted: Font: 10 pt

Formatted: Body Text, Line spacing: Multiple 0.06 li

Formatted: Left: 0.22", Right: 0.22"

Formatted: Font: 10 pt

Formatted: Body Text, Line spacing: Multiple 0.06 li

to ensure that it has secured its delivery point. There typically is less capacity available later in the nomination cycles. This is especially true if the receipt point is relatively illiquid or the transportation path follows segments that are known to often be constrained. Moreover, firm shippers may "bump" scheduled interruptible shippers up to the Intraday 3 cycle (7:00pm CCT intraday) per FERC policy.

Another important consideration is that pipeline operators are not obligated to flow the gas until the flow time specified in the NAESB nomination timeline approved by FERC. In some cases, this delay from the end of the nomination cycle until gas is allowed to flow to the shipper is up to 4 hours. However, many pipelines have tariff authority and often use best efforts to allow a generator gas to flow sooner than the flow time specified in the NAESB timeline. It is important to note that when gas demand is high, this operational flexibility should not be assumed. In fact, planners should make allowances for these constraints in their modelling efforts and system operators and generators should communicate frequently with the pipeline operators, and review pipeline critical notices, to understand how much flexibility, if any, may be afforded under stressed conditions.

An additional complexity is that pipeline operators may also issue OFOs which to require shippers to stay within certain daily and/or hourly imbalance tolerances per the pipeline tariff. These OFOs may be necessary to maintain the pipeline's, and their shippers', operational reliability and integrity, particularly during extremely (high or low) demand periods. For example during a ratable OFO, this means that shippers must flow their daily scheduled quantity of gas in 1/24th hourly increments, with some small percentage of hourly imbalances, but returning back within balance by the end of the gas day. Should a shipper disregard the OFO, significant penalties may accrue for non-compliance. If an OFO is issued, affected generators may need to modify their minimum or maximum run times; and reduce their ability to follow load. Synchronized generators, operating under a ratable OFO, may need to reduce their regulation ranges and operating reserve capabilities. Pipeline operators are required to post all critical and non-critical notices on their respective Electronic Bulletin Boards ("EBB"), including the specifics, duration, and geographic location of any OFO. Finally, it is important to know whether shippers have contractual entitlement to have gas delivered to a "primary delivery point." If a pipeline calls a primary delivery point restriction it is important to understand whether the generator has delivery at that primary delivery point. under constrained conditions, when firm transportation shippers are using their full contractual entitlements and there is not excess capacity, a pipeline operator may the pipeline operators restrict delivery to "primary delivery points." U ", unless the shipper's location is a "primary delivery point" it would not be able to schedule gas to the facility and thus be unavailable.

While we cannot understate the complexity of understating how a large number of shippers and pipeline operators may interact under certain scenarios, most of the information necessary to develop reasonable judgments is publicly available. FERC requires pipeline and storage operators to post a significant amount of data on their EBBs, including information about pipeline design, operating and operationally available capacity by receipt and delivery point, critical and non-critical notices, identification of firm pipeline shippers, and capacity release information. Additionally, interstate pipelines and storage operators may communicate non-public information, on a voluntary basis, to grid operators and vice versa to facilitate the reliable operation of their respective grids, per FERC Order 787. Intrastate pipelines are typically under the jurisdiction of state regulatory authorities, and the amount of publicly available information varies widely from state-to-state. While FERC Order 787 only covers pipeline and storage operators and grid operators, it does not prevent grid operators from requesting and receiving non-public data from intrastate pipeline operators and LDCs under non-disclosure agreements.

In addition to transportation services, customers also purchase the physical commodity directly from a gas producer or from a gas marketer to receive natural gas at contracted points into the applicable transportation system agreements and/or at other points of delivery at their respective interconnection points or market center. Larger volume customers (e.g., LDCs and electric generation facilities) may also purchase natural gas upstream at or near the point of production and contract for pipeline service to transport the commodity to the point of delivery. In addition, based on market conditions, these entities and other market participants may purchase natural gas at a market center and contract for transportation from that point to a delivery point(s). While commodity

Formatted: Font: 10 pt

Formatted: Body Text, Line spacing: Multiple 0.06 li

Formatted: Indent: Left: 0.5", Right: 0.48"

Formatted: Not Expanded by / Condensed by

Formatted: Font: 10 pt

Formatted: Body Text, Line spacing: Multiple 0.06 li

Formatted: Font: 10 pt

Formatted: Body Text, Line spacing: Multiple 0.06 li

arrangements may be as varied as transportation arrangements, the generators that are typically used for grid balancing – i.e., gas peakers, typically do not have enough operational certainty to enter into forward contracts for the commodity. If these particular generators do not receive unit commitments with sufficient advanced notice, they may not be able to source the commodity during the operating day under constrained conditions, and especially at more thinly traded hubs. A reasonable proxy for liquidity may be the volume of transaction for a particular point on Intercontinental Exchange, Inc. (“ICE”).

In summary, gas-fired generators’ contractual arrangements offer insight into how gas may be transported to facilities; however, other factors influence generators ability to effectuate gas deliveries. These conditions may be crudely grouped as “transportation constraints.” Another important consideration, especially for gas peakers, is the relative natural gas supply liquidity during periods of high demand of the shipper’s trading hub. If the supply/trading hub is relatively illiquid and the generator does not usually receive unit commitments day ahead, the risk that these generators may not be able to source the commodity during peak demand days increases. Obviously, both transportation and commodity are required to ensure fuel can be delivered. Some generators may be uniquely positioned or have sufficiently mitigated performance risk through transportation and commodity contracts to be at low risk if of non-performance. Conversely, other generators may be poorly positioned and have high transportation and commodity risk. While still others may have either heightened transportation or commodity risk, but not both. It may be necessary planners examine historical pipeline critical notices and trading hub history in addition to historical generator performance to determine fuel availability risk.

Formatted: Font: 11 pt

Formatted: Justified, Indent: Left: 0.5", Right: 0.48", Space Before: 0 pt

Oil

Fuel oil is obtained from the petroleum distillation process as either a distillate or a residual and is then distributed to regional bulk terminals for distribution to end users. Transportation to generation sites is typically by pipeline, barge, truck, or a combination of the three methods where it is off-loaded into on-site fuel tanks. Each power plant ~~site~~ with storage tanks will have unloading facilities that frequently limit the ability to replenish the on-site storage tanks. Each generator with oil as either the primary or back-up fuel must ~~decide the maximum capacity of the on-site storage tanks as well as~~ the amount of fuel oil that will be kept in inventory~~. Key factors in how much fuel oil to~~ or reserved for other uses such as maintenance or black start service obligations. Aside from any emissions limitations, facilities typically do not have ~~on site~~sufficient replenishment capability to run continuous at maximum output for long durations. Replenishment rates are ~~the proximity of the regional terminal, the regional terminal capacity, expected run-time,~~dependent on availability of transport tankers (maritime or over-the-road~~),~~) and pipelines, and expected transportation constraints ~~(~~ e.g., competition with resupply of home heating oil, dearth of licensed drivers, roads impassable due to weather conditions ~~or~~, rivers impassable due to ice conditions~~).~~, etc. There are multiple types of fuel oil and generators are typically designed to operate on or switch to a specific type. A majority of oil combustion capable units in the NERC footprint fire distillate fuel oil #2, also known as home heating oil. Others primarily combust distillate fuel oil #1, which includes diesel, kerosene, and jet fuel, or one of the three residual “bunker” fuels #4, #5, and #6.

Formatted: Condensed by 0.35 pt

Coal

Four major types of coal are used to produce electric power, each of which varies in heat content and chemical composition:

- ~~**Anthracite:** The highest rank of coal. It is a hard, brittle, and shiny black coal (often referred to as hard coal). It contains a high percentage of fixed carbon and a low percentage of volatile matter.~~

---

[15] *Id.*
[16] *Id.*
[17] 2017 NERC Special Assessment at page 7
[18] *Id.*

Formatted: Font: 10 pt

Formatted: Body Text, Line spacing: Multiple 0.06 li

- **Bituminous:** Bituminous coal is a middle rank coal between subbituminous and anthracite~~.~~ containing 45%–86% carbon. Bituminous usually has a high heating (Btu) value (11,000 – 15,000 Btu/lb). and is the most common type of coal used in electricity generation in the United States. In 2021, bituminous accounted for about 45% of coal mined in the U.S., with a majority originating from mines in five states. Since 2020, all coal produced in Canada was sourced from bituminous seams.
- **Subbituminous:** Subbituminous coal is black and dull (not shiny) containing 35%–45% carbon and has a higher heating value (8,500 – 13,000 Btu/lb) than lignite. In 2021, subbituminous accounted for about 46% of coal mined in the U.S. with more than 85% coming from the Powder River Basin in Wyoming.
- **Lignite:** Lignite coal, aka brown coal, is the lowest grade coal with the least concentration of carbon (25%–35%) and the lowest heat content (4,000 – 8,000 Btu/lb). In 2021, lignite accounted for about 8% of coal mined in the U.S. with most going to electricity generators a short distance from the mine. Most lignite is produced and consumed in North Dakota and Texas.
- **Waste coal:** Usable material that is a byproduct of previous coal processing operations. Waste coal is usually composed of mixed coal, soil, and rock (mine waste), often called gob or culm. Most waste coal is burned as-is in unconventional fluidized-bed combustors with the fuel source co-located with or near to the generator. The heat and carbon content of waste coal is highly variable and is often blended with higher grade coals to ensure a minimum combustor heat input. Most waste coal combusting facilities are located near former mine sites and were purpose built for reclamation.

Coal is extracted from surface and underground mines in various regions around the United States~~ and the world.~~. The United states has over 250 years of remaining coal reserves. It is then crushed and washed in preparation for transport to power plants. Transportation is typically by rail, barge, ~~or truck.~~truck, or conveyor belts; the latter used at what are called mine-mouth power plants. Coal may be delivered directly to a power plant or to a nearby unloading terminal from which it proceeds to the power plant by truck or a conveyance system. At the plant, coal is stored on-site in piles to be used as needed for generation, typically in an amount sufficient for several weeks to several months of operation. ~~Coal can be transported by rail using tariff rates shipment-by-shipment or under customer-specific short- or long-term rail contracts. Contracts may provide discounts when compared to the tariff rates but require volume commitments over a specified period of time~~ Long-term supply contracts are used to ensure high levels of reliable coal deliveries. Equally as important, coal plants require certain reagents to scrub the flue gas – e.g., any of a number of forms of lime, aqueous or anhydrous ammonia, activated carbon, etc. and chemicals to support ongoing operations – e.g., water treatment chemicals. These reagents and chemicals are typically transported via truck and most facilities have storage sufficient for a few weeks operations.

Nuclear

Nuclear plants are refueled every 18–24 months. Required outages cannot normally be delayed~~.~~ due to costs and scheduling of specially trained labor. Nuclear plants need to maintain certain reactivity levels in nuclear fuel. At times, this reactivity requirement has led to units derating in shoulder months in order to conserve fuel and be available to operate 100% during peak months.

Four major processing steps must occur to make usable nuclear fuel: mining and milling, conversion, enrichment, and fuel fabrication. The uranium used in power plants comes from Kazakhstan, Canada, Australia, and several western states in the United States. Major commercial fuel enrichment facilities are in the United States, France, Germany, the Netherlands, the United Kingdom, and Russia.[19]

~~Fuel is~~Both fresh and spent fuel are typically stored on site at nuclear plants in specialized facilities, when not in the reactor, that are built to withstand significant physical events, including weather, seismic, and other types of natural disaster. Licensees must abide by robust security measures (e.g., armed security officers), physical barriers, and intrusion detection and surveillance systems.[20]

Formatted: Font: 10 pt

Formatted: Body Text, Line spacing: Multiple 0.06 li

Formatted: Right: 0.5"

Formatted: Font: 10 pt

Formatted: Body Text, Line spacing: Multiple 0.06 li

The Nuclear Regulatory Commission regulates nuclear facilities in the United States~~.~~ and the Nuclear Safety Commission regulates facilities in Canada. Nuclear power plants must show that they can defend against a set of adversary characteristics called the Design Basis Threat (DBT). DBT imposes security requirements on nuclear power plants based on analyses of various factors, such as the potential for a terrorist threat. The Nuclear Regulatory Commission regularly evaluates the DBT for updates and alignment with the threat environment.

Nuclear facilities use digital and analog systems to monitor, operate, control, and protect their plants. Digital assets critical to plant systems for performing safety and security functions are isolated from the external networks, including the internet. This separation provides protection from many cyber threats.

Hydro

An integrated hydro-electric system, like those found in the Pacific Northwest, is more frequently energy limited than capacity limited from its mix of storage and run-of-river projects. The storage projects fill and draft annually and tend to have a steady discharge. Fluctuations in discharge (generation) are usually driven by snow melt water content, flood control, maintenance of navigation channels, seasonal icing, and downstream water temperature objectives. The run-of-river projects more closely follow demand as the projects fill and draft daily. However, run of river projects have limited storage to meet demand because the water needs to be in the right place(s) at the right time(s). Hydro-electric generation also has many non-power objectives that can limit hydro- electric power production (e.g., lake/river level management, recreational use, stream flow speeds, etc.) Information sharing, communication, and coordination is critical across different hydro projects, utilities, states, and countries.

---

[19] https://www.nei.org/fundamentals/nuclear-fuel

[20] https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/security-enhancements.html and https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/cyber-security-bg.html

Formatted: Font: 10 pt

Formatted: Body Text, Line spacing: Multiple 0.06 li

Formatted: Right: 0.48", Space Before: 2.8 pt

Formatted: Font: 10 pt

Formatted: Body Text, Line spacing: Multiple 0.06 li

~~electric power production (e.g., lake level management, recreational use). Information sharing, communication, and coordination is critical across different hydro projects, utilities, states, and countries.~~

~~Solar, Wind, and Other Battery~~

Variable Energy Resources, Energy Storage ~~With many states adopting emissions reduction goals,~~, and Developing Technologies

Technologies like weather dependent BPS-connected solar photovoltaic and wind generation ~~and energy limited battery storage have~~ are being integrated at an accelerating ~~rate into many rapidly and will likely remain a part of the resource mix of the future resource portfolios. These resources inverter-based resources and battery energy storage are asynchronously connected to the grid and only interface with the BPS through power inverters. This rapid adoption of inverter-based resources and battery storage has presented new opportunities in terms of grid control and response to abnormal grid conditions and has necessitated the standardization of performance characteristics for inverter-based resources. NERC produced a reliability guideline for this purpose in late 2018.[21] The~~ pace, and the "fuel" for wind and solar generation are ~~the wind and sunlight that are~~ effectively limitless but are only available as weather conditions permits. For storage devices, including batteries, the energy they provide is dependent on some other electric energy producing resource. Therefore, storage devices are not electric generators but rather may time shift the consumption of electricity generated in a less constrained period to a more constrained period.

~~The weather dependency for these solar and wind resources and the planned storage of their renewable energy for shifting this energy to peak demand hours will present new challenges for planning and procuring fuels for flexible, swing generation such as natural gas generation in the future. On blue-sky winter days for east coast entities with high penetrations of solar resources large amounts of gas generation with large peak demand hourly gas demand may be needed through the morning and evening peak hours with very little hourly gas demand needed for mid-day hours when solar is at full output. Similarly, for entities with high penetrations of wind generation, during higher wind output hours, gas generation output could be minimal, yet when wind output drops off significantly, gas generation could need to come online and ramp up quickly to meet electricity demand. For an entity with significant battery storage, if planned to be primarily charged by solar and/or wind and those weather-dependent resources experience short term low capacity factors, gas generation could be relied upon to charge the storage for needed peaking capacity from the battery storage during peak demand hours. Examples shown below from the US Energy Information Administration (EIA.gov) charts of this impact to gas generation are already being realized on some systems with high penetrations of wind and solar. As higher penetrations of solar, wind, and battery storage occur, this impact will continue to grow and will need to be managed from a gas supply and procurement perspective.~~

~~*(May create generic charts for illustration)*~~

Operators and planners must ensure sufficient energy is available given the non-dispatch-limited controllable nature of solar and wind resources and the regulatory imposition of "must-take" requirements in many areas. In particular, peak demand hours will present new challenges for planning and procuring fuels for flexible, swing generation, such as natural gas generation, as the penetration of nature-controlled resources increase. Two primary concerns are emerging as penetrations increase. Many regions are using probabilistic analysis and capacity-based metrics, such as Effective Load Carrying Capability, to model the resource adequacy contribution of variable generation during extreme conditions, yet the actual generation during these conditions could vary widely in either direction across a planning footprint. Therefore, it is important to examine the distribution of possible variable generation outputs from the modelling efforts and select appropriately low tail probability generation scenarios to ensure there are sufficient back-up resources in the event these low probability generation conditions

Formatted: Font: 10 pt

Formatted: Body Text, Line spacing: Multiple 0.06 li

Formatted: Left: 0.22", Right: 0.22"

Formatted: Not Expanded by / Condensed by

Formatted: Font: 10 pt

Formatted: Body Text, Line spacing: Multiple 0.06 li

Formatted: Font: 10 pt

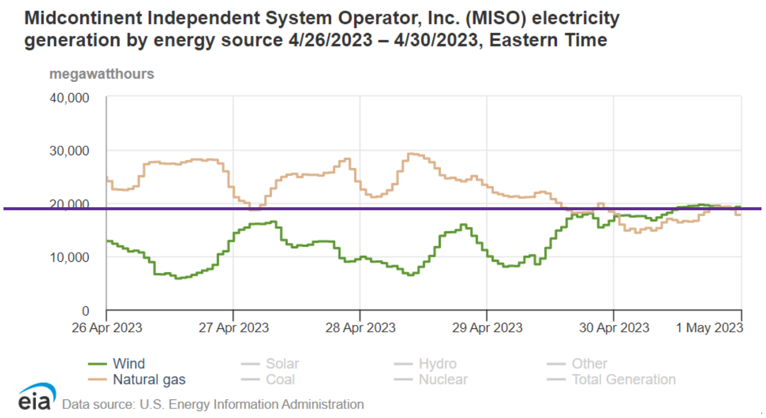
Formatted: Body Text, Line spacing: Multiple 0.06 li

occur. The second concern is to ensure that back-up resources may be both deliverable and able to respond in the operational horizon to changes in variable generation. There exists an inherent error between the forecasted variable generation and what is actual produced in the operating day. While the error may be small, there may be unique conditions that make this error much larger – e.g., icing of wind turbine blades, fog, smoke, temperature extremes, etc., and it is imperative to ensure there are sufficient back-up resources that are capable of responding during these outlier events. Moreover, theses issue may be compounded by the inherent increase of forecast risk across a weekend and holiday periods when gas typically trades for multiple days ahead of the Day Ahead electric market. These conditions highlight the importance of modelling low probability, or extreme scenarios, with respect to resource adequacy contribution and potential for generation forecast error, quantifying the potential need, and confirming that there is sufficient dispatchable generation is available and any temporal constraints that dispatchable generation may have due to fuel arrangements.

Other technologies (e.g., ~~battery~~energy storage) are still in early stages of development, and deployment of these technologies will require further evaluation and consideration as they mature. For instance, system operators and planners need to understand how co-located facilities with variable energy production and storage systems charge and discharge onto the grid. The charging and discharging behavior of energy storage devices may be responsive to regulatory demands and incentives, or ancillary service market price signals, and are not always conducive to assisting operators manage real time energy demand. For storage devices, including batteries, the energy they provide is dependent on some other electric energy producing resource. Therefore, storage devices are not electric generators but rather a mechanism for time shifting the production of electricity for later deployment, and offer fuel assurance only to the extent that they can shift energy generation from a less constrained period to a more constrained period. Additionally, many of today's energy storage technologies are subject to operational temperature limitations that may limit their ability to charge and discharge[9].

Formatted: Font: 11 pt

Formatted: Justified, Indent: Left: 0.5", Right: 0.48", Line spacing: Multiple 0.99 li



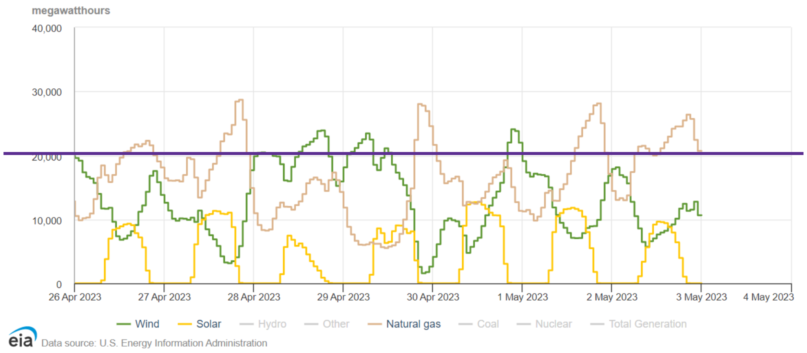
---

[9] https://batteryuniversity.com/article/bu-410-charging-at-high-and-low-temperatures

Formatted: Font: 10 pt

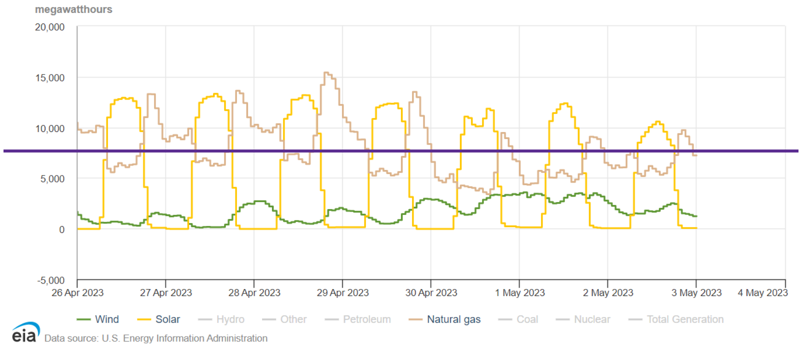
Formatted: Body Text, Line spacing: Multiple 0.06 li

Electric Reliability Council of Texas, Inc. (ERCO) electricity generation by energy source 4/26/2023 – 5/3/2023, Central Time



Data source: U.S. Energy Information Administration

California Independent System Operator (CISO) electricity generation by energy source 4/26/2023 – 5/3/2023, Pacific Time



Data source: U.S. Energy Information Administration

Formatted: Font: 10 pt

Formatted: Body Text, Line spacing: Multiple 0.06 li

Formatted: Font: 10 pt

Formatted: Body Text, Line spacing: Multiple 0.06 li

Formatted: Font: 10 pt

Formatted: Body Text, Line spacing: Multiple 0.06 li

~~[21]https://www.nerc.com/comm/OC_Reliability_Guidelines_DL/Inverter-Based_Resource_Performance_Guideline.pdf~~Hydrogen is another developing technology that will require close attention and coordination as it grows as a power generation fuel. If hydrogen utilizes the same transportation infrastructure as natural gas, it has 1/3rd the heating value on a volumetric basis, which will require significant build out to deliver the same energy. Today, most hydrogen is produced using natural gas reforming technologies and is primarily used in petroleum refining and chemical production. As hydrogen technologies advance and hydrogen use as a power generation fuel expands, it will be necessary for planners to consider many of the same concerns that exist today with the supply and procurement of natural gas in addition to coordinating with hydrogen producers relying on electrically intensive processes such as electrolyzers and hydrogen fueled generators to ensure that sufficient stocks and production are maintained during to ensure the availability of generation during extreme conditions.

Formatted: Font: 11 pt

Formatted: Body Text, Justified, Indent: Left: 0.5", Right: 0.48", Space Before: 0 pt

Formatted: Font: 10 pt

Formatted: Body Text, Line spacing: Multiple 0.06 li

Chapter 3: Fuel Supply Risk Analysis Consideration

Formatted: Left: 0.22", Right: 0.22"

At a high level, this chapter describes the supply chain considerations of each generator fuel supply type that will help planners form realistic assumptions when developing their own fuel-related reliability risk analyses.

Natural Gas

While the natural gas industry does not have a history of being susceptible to failure in general or to wide-spread failure from a single point of disruption because of the dispersion of production and storage,[22] redundancies due to the integrated pipeline and distribution network, and its low vulnerability to weather-related events, a temporary outage of a section of a single pipeline or a delivery point is a credible scenario to examine. When considering such a natural gas supply disruption within a given area, the examination would not just be limited to the loss of the natural gas supply but also the associated loss of electric generation and any ancillary needs, such as the loss of electric natural gas compression.

Planners should fully examine the credible reliability risks associated with the natural gas supplied to generators within the reliability footprint of the planner. Further, planners should view the system through an “all-hazards” lens and evaluate additional considerations, including weather, regional policies, and cyber-related risks. The following paragraphs outline the information that planners should seek to understand as a precursor to a more rigorous fuel assurance and reliability risk analysis.

To begin, planners should seek to understand the strategies employed regarding natural gas supply to each generator within their reliability footprint and any applicable regulatory requirements. This could include regular and emergency transportation/service agreements, call options, or other marketing arrangements being employed by the generator owners/operators to meet its resources capacity obligations. This examination could also include reviewing access to on-site fuel storage (e.g., fuel oil, propane, LNG, compressed natural gas), access to off-site storage,[23] access and availability of an alternate pipeline connection, and the availability of non-firm natural gas services and supply. Planners may also consider the alternative fuel capability of the generator, how any such alternatives are contracted and managed, and any environmental and regulatory requirements that may limit the use of the alternative fuel.

The PJM study “Fuel Security Analysis:[24] A PJM Resilience Initiative” investigated the two following natural gas “disruption” scenarios with different recovery expectations:

“Line Hit,” such as an excavating crew accident	“Other,” such as corrosion
This type of disruption is easily identified, isolated to a smaller area requiring repairs, and would only cause about a five-day disruption.	This could take longer as investigations are needed over a larger area and will likely be a more “sustained” type of outage.

Planners should examine each generator and its potential physical access to supply (including access to pipeline, distribution, and storage facilities), the amount of capacity subscribed and available at each supply facility, and the ability of the facility to meet daily and seasonal demand swings. In addition, planners should review potential curtailments to key supply points on their respective transportation agreements (e.g., LDCs needing to redirect supply to “essential human needs” if a severe supply disruption occurs). These details are important in order to formulate

---

[22] Although it is noted that prior to shale natural gas, hurricanes in the Gulf of Mexico caused large amounts of supply to be shut-in.

[23] Storage facilities are different in the various regions of the United States; therefore, understanding the configuration, operation, and services available in the different regions is recommended.

[24] https://www.pjm.com/-/media/library/reports-notices/fuel-security/2018-fuel-security-analysis.ashx?la=en

2020 9

Formatted: Left: 0.22", Right: 0.22"

supply alternatives to consider when examining a possible supply shortage or failure. While physically severing an interstate pipeline is very uncommon, it can occur in situations like third-party damage. Furthermore, a facility may need to be taken out of service for maintenance. Other considerations include specific pipeline resilience, geography, and potential state or federal restrictions on pipeline expansion, competition for supply with heating and industrial demands, and upstream demand that may impact the region.[25] Environmental permits, such as those that allow streambed alteration, may be required and will vary by repair required and specific location. Quick agreement on any environmental mitigation measures will speed obtaining those permits. As noted previously, the planner's role is to have specific knowledge of the fuel assurance of individual generators in order to be able to assess, over the planning area, whether any fuel assurance problems at a particular unit can impact the maintenance of reliability to the area as opposed to just impacting the deliverability of that particular unit. Planners need to recognize this distinction so as to avoid taking on management responsibilities that more appropriately lie with the individual unit owner.

In order to assess the forgoing, data can be obtained from certain public sources. FERC regulations and the business practice standards of the Wholesale Gas Quadrant of the North American Energy Standards Board applicable to natural gas pipelines, which are incorporated by reference into FERC regulations, include various posting requirements for regulated pipelines. These standards require the posting of information related to pipeline capacity, natural gas quality, operational notices, customer indices, tariff provisions, and other items. The U.S. Energy Information Administration also publishes detailed information on U.S. natural gas pipelines and underground storage.[26] FERC also requires that interstate pipelines and certain intrastate and Hinshaw[27] facilities file various forms and operational reports.[28] In addition to the forgoing, the various states also require LDCs to file certain information with the state commissions and/or publicly post certain information. The aforementioned information and data from the applicable generators should also be used to evaluate fuel risk.

Furthermore, as increasing penetration of wind and solar resources and battery energy storage occurs to meet state objectives and policies for emissions reductions, natural gas will become the swing fuel. Natural gas will be in high demand, not only during periods of extreme cold and hot weather, but also during periods of low solar and wind output or even when needed for battery energy storage when solar and wind energy is depressed. At other times, when solar and wind energy is in excess and battery energy storage is insufficient to absorb this excess, natural gas generators and thus natural gas usage will significantly decline to accommodate the solar and wind energy and avoid curtailments of clean energy.

Oil

~~The main risks associated with fuel oil are typically regional depot capacity and transportation (e.g., pipeline, barge, or truck) from the depot to the plant site. Since the fuel oil is stored in tanks, the capacity of the regional depot(s) limits the amount of fuel oil that can be purchased when a need arises. Even in cases where depot levels are adequate to meet the plant needs, the ability to move the fuel oil from the depot to the plant may be challenging due to inclement weather that affects the ability of trucks to move the fuel oil safely. There may also be emissions limitations or other environmental constraints that may limit the amounts or location for liquid fuel storage and/or prevent full utilization of fuel oil in certain areas during portions of the year. For example, oil-fired generation cannot run between May and September in ozone nonattainment locations unless the state governor declares an emergency.~~ The main risks associated with fuel oil are:

- Severe cold weather events of unusually long duration;
- Multiple, severe cold weather events that occur before sufficient replenishment has occurred; and
- Deeper and more-protracted reliance on oil due to the failure of other resource types.

These risks may be quantified through modelling of the following variables, initial conditions, and constraints:

- Initial inventories may be quantified through fuel surveys, historical tankage levels, and adjustments due to commodity prices, especially relative to the predominant marginal fuel;

- Burn rates may be determined from equipment technical specifications, field unit parameters, and survey responses from the generators;
- Emissions limitations may be determined from a review of each facility's Title V Operating Permit and recent operating profile;
- Replenishment rates may be more difficult to model; however, the maximum replenishment rate is limited by the offload capability at the facility. However, if severe weather persists, trucks and barges may not be able to replenish on-site inventories at these maximal rates and may need to be adjusted downward. These limitations could be due to physical transportation conditions or could be due to competition with heating oil deliveries.

Regardless, the main risks are needs outpacing replenishment plus on site storage over varying time horizons, and facilities reaching emissions limitations for the remainder of the heating season.

Coal

Risks associated with coal supply are primarily in the transportation of coal from the mine to the power plant. ~~The~~Approximately 70% of coal to US power plants is delivered by rail, and the rail network is comprised of an extensive grid of intersecting and interconnected tracks that offer multiple pathways for rerouting deliveries in the event of a physical disruption, but temporary slow-downs or disruptions to supply can occur in the rail system due to weather (e.g., floods or snow), derailments, or track repairs. Similar to other fuel types, longer-term disruptions can occur during a pandemic caused by labor shortages resulting in limited rail and trucking capacity. Barge transport can be temporarily impaired by icy, low-level, or flooded conditions on river systems. Generators rely on their on-site coal supply for operation until deliveries can be restored. However, conditions like frozen or wet coal could impact on--site coal supply. Coal commodity and rail transportation contracts may contain ratability language that states shipments must be taken consistently even though there may be some month-to-month flexibility. This ratability causes a natural rise and fall of the on-site stockpile based on periods of high and low demand. Any disruptions during the periods of high demand may exacerbate low inventories. Additionally, coal plants are typically optimized to run

---

[25] Such analyses are very similar to what many lenders offering non-recourse finance obtained from an Independent Fuel Consultant.

[26] Energy Information Administration, Natural Gas Storage Report, and Wholesale Electricity and Natural Gas Market Data: https://www.eia.gov/naturalgas/.

[27] Hinshaw Pipelines are local distribution pipelines or companies served by interstate pipelines that are not subject to FERC jurisdiction by reason of section 1(c) of the Natural Gas Act.

[28] *See* FERC Forms: https://www.ferc.gov/docs-filing/forms.asp.

using only one of the four types of coal, potentially limiting generation capability if that coal becomes unavailable due to long-term supply or transportation disruptions.

Nuclear

As described in **Chapter 2** nuclear facilities store fuel on-site in a highly controlled and secure environment. There are many layers of safety at nuclear sites to protect from physical and cyber risks.

Hydro

All hydroelectric projects are dependent on upstream sources for fuel supply water. Those sources can be snowpack, other hydro projects, free flowing rivers, lakes, streams, or a combination. Ultimately, the source is a function of precipitation. History has shown quite a diversity in the volume of water available for hydropower generation. The total volume can run between 50–150% of the expected average. In some areas, much of the precipitation falls in the form of snow and becomes useable water during the spring thaw. The rate of the melt or “run-off” is almost as important as the volume. Slow melts are best as fast melts can lead to spilling water past fully loaded turbines or loss of water as a fuel due to lack of storage. Deeply cold winters can also result in frozen rivers and streams, cutting off fuel to downstream projects during times of elevated power demand. Temperature and precipitation are critical factors in the availability of water for hydropower production.

Formatted: Left: 0.22", Right: 0.22"

Wind and Solar

Where many of the risks associated with fuels described in the prior sections can be empirically measured in definite terms, the risks associated with wind and solar are more probabilistic and often subject to non-human controllable variation. The primary risk is uncertainty in meteorological conditions, such as wind speed and cloud cover, and can vary widely by region and locality within a planning footprint. These risks also vary through time. For instance, a wind farm may be able to sustain operations through a cold weather event of short duration during which blade icing occurs but does not reach a threshold which requires turbine shutdown, while the same farm may reach the shutdown threshold during a longer duration event. The same occurs for solar generation at high temperatures where output decreases as a function of ambient temperature and enclosed panels are subjected to the same radiative heating effects as an automobile which raise the temperature seen by the panel. These uncertainty risks may be quantified through probabilistic modelling using historical weather data to determine a distribution of production levels. Since most distributed energy and behind the meter resources are wind or solar driven, planners should attempt to collect a reasonable amount of information on the location and type of these resources and include them in the probabilistic modelling. In order to bound the potential risk outcomes from the uncertainties impacting wind and solar resources, studies should examine scenarios that include a range of geographical and production variabilities, i.e., different weather scenarios overlaid on the region.

Chapter 4: Fuel-Related Reliability Risk Analysis Framework

The BES, for the most part, is similar enough from area to area that a specified baseline set of criteria can be defined and followed, resulting in similar and comparable results from transmission planning studies. TPL-001 defines and prescribes these planning studies very well; criteria have been developed over many years, resulting in multiple revisions to the standard. Even though TPL-001 references a fuel contingency analysis in Table 1 Steady State & Stability Performance Extreme Events as a possible study contingency, the (default) contingency results in the loss of only two generating stations and may not represent a significant pipeline segment, compressor station, storage facility, barge transport, or other fuel supply disruption for many systems. This chapter provides details regarding the scope of fuel-related generator outages beyond the minimum requirements for TPL-001 transmission system planning assessments.

Formatted: Left: 0.22", Right: 0.22"

The framework presented below does not identify a single methodology but rather outlines an approach to assist planners in determining what factors may be considered to conduct a meaningful fuel-related reliability risk analysis for the BPS. The actions described are intended to be flexible enough to account for all fuel types, broad enough to support the unique circumstances in each region, and performable out of order (or in some cases not at all). This framework does not provide specific solutions or next steps that could be taken after assessing the results of any particular study.

Appendix A outlines this framework in checklist format

Formatted: Left: 0.22", Right: 0.22"

The methodology described in this section may be applied narrowly or across a broad range of credible assumptions as determined by the planner performing the study. The selected assumptions should ensure that the study is both relevant and meaningful. It may be prudent to subject the BPS system under study to a range of high-probability, low-impact (HPLI) contingencies as well as some high-impact, low-probability (HILP) contingencies. Studying HPLI contingencies may shed light on operational needs during such instances and inform changes to processes and procedures to preserve reliability (e.g., improvements in the ability of generators to schedule or contract for natural gas). Even if they are not the primary motivation for the analysis, studying HILP contingencies that stress test the system will bookend the study set and may inform regulators or other interested parties of the reliability impact of such extreme conditions and may inform emergency preparedness efforts. Examples of HILP scenarios include severe reduction of non-firm natural gas supply, prolonged pipeline repair, extreme prolonged weather events that affect both supply of and demand for natural gas, or unanticipated low production from variable energy resources (VERs) such as solar and wind.

> The examples used throughout this chapter are intended to be illustrative and do not imply or prescribe mandatory actions

Based on the unique risks in different regions, the fuel-related reliability risk analysis outlined in this chapter (although not required) is recommended as a best-practice approach for supporting existing studies (e.g., TPL-001 extreme events analysis) or for conducting a stand-alone analysis. In either case, documentation of each step of the process is critical. Documenting the rationale behind the methodology and assumptions will better inform those reviewing the study both presently and in the future and may also inform subsequent studies.

Formatted: Left: 0.22", Right: 0.22"

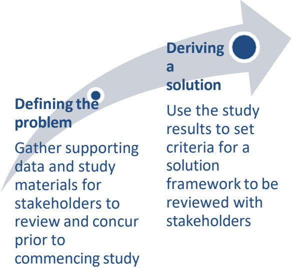
Step 1: Problem Statement and Study Prerequisites

To perform a valid fuel-related reliability risk analysis, there are numerous considerations that should be taken into account that will help shape the direction and results of the analysis. Prior to beginning any analysis, the planner must determine the purpose or goal of the study and, just as importantly, what the study will not do. It is at this point that the criteria, concerns, scenarios and required data will become more evident. Determining which elements of fuel supply risk are to be examined in a single study can be challenging as different combinations of risks can lead to an unmanageable number of model runs.

Formatted: Left: 0.22", Right: 0.22"

Consider the following to help define the study:

- Have a clearly defined goal for the study. Set the criteria of the study and define the criteria for system performance. A study that crosses the threshold of meeting certain criteria will do so when fuel is in short supply, generators are no longer able to run, or there is a supply/demand imbalance. The imbalance can be system-wide or, equally as important, a local area imbalance that results in the potential exceedance of a NERC Reliability Standard defined System Operating Limit (SOL) or Interconnection Reliability Operating Limit (IROL) of the BPS. This philosophy can help determine contingencies that may not be obviously catastrophic, but still highlight issues that may need mitigation.
- Communicate the goals of the study with stakeholders and gain agreement on principal concepts.



Gather supporting data and study materials for stakeholders to review and concur prior to commencing study

Use the study results to set criteria for a solution framework to be reviewed with stakeholders

Formatted: Left: 0.22", Right: 0.22"

- Decide the analysis timeline prior to commencing work. If the problem definition and the solution are going to be two separate phases of a study, set that expectation early in the process. Often, the deriving solution means following the directives of governing entities (NERC, FERC, governmental agencies, state public utility commissions, etc.). If this is the case, that is the goal of the study.

> For example: "The purpose of this study is to determine the minimum required resources to be retained in a capacity auction while accounting for system-wide fuel supply constraints."

- Clearly state the boundaries of the study. If there are certain aspects that will not be addressed by the study, make that distinction clear as early in the process as possible.

> For example: "The study will be limited only to the generators that are currently in the interconnection queue through 2030." Or "The analysis being performed will only consider credible single points of disruption in the gas and fuel oil supply chains."

Formatted: Left: 0.22", Right: 0.22"

Step 2: Data Gathering

Data is essential for a valid fuel-related reliability risk analysis. While the planners performing the study are very familiar with the transmission system and the inputs needed to perform traditional studies, there are many considerations outside the normal inputs that are needed for this analysis. Much of the data needed is likely not directly accessible to the planner and will therefore require the assistance of others in their company (e.g., operations personnel) or even fuel suppliers themselves. FERC has through its Order 787 authorized the sharing of confidential information between jurisdictional pipelines and system operators in order to ensure reliability. Planners should consider using that authority to obtain needed information from the pipelines on a cooperative basis. The following is a list of data sources and methods for acquiring data that can be used by planners to collect the information that they need to perform the study outlined in Step 1:

- Coordinate fuel assurance assumptions with generator owners/operators:
    - This may be achieved with surveys that may include, but are not limited to, primary fuel availability, details of fuel supply and transport agreements, usable on-site storage capability, historic inventory levels, resupply and back- up fuel availability and strategy, resource limitations on alternate fuels (MW output, switching time and process details, changes in heat rate), emissions concerns, and staffing concerns.
        - It may be helpful to discuss the formation of such a survey with generator owners/operators and other stakeholders to seek their guidance and expertise on the level of data they may be able and willing to provide.
    - Validate/benchmark that the data received is consistent with the recent operational experiences when possible

Formatted: Left: 0.22", Right: 0.22"

Appendix B contains a detailed list of potential survey questions

Formatted: Left: 0.22", Right: 0.22"

Suggestions to Establish and Maintain a Suitable Fuel Survey

Consider managing a survey of this type through an established stakeholder forum

- This will ensure that any changes to the survey are subject to stakeholder discussion and therefore more thoroughly vetted
- Ensure that the information is reaching the target audience as there can be a disconnect between generator owners/operators and the stakeholder representatives

Consider hosting additional engagements like a winter generator readiness seminar

- This offers the opportunity to discuss with a more targeted audience of generator owners/operators and not just their representatives

Consider conducting fuel-constrained scenarios as part of your regular training cycle

- This offers an opportunity to solicit concerns and gather potential impacts of limited fuel supply on system operations across a wide spectrum of electric and cross-sector stakeholders
- This exercise also has the potential to identify fuel disruption impacts that can be further addressed directly with fuel suppliers to seek actions to mitigate these impacts

- Gather appropriate fuel supply contingencies (to be further analyzed and filtered in Step 4):
  - Coordinate with fuel suppliers or fuel specialists within your company, member companies, and/or collaborate with the experts who own and operate the fuel supply chains, including (but not limited to) natural gas and fuel oil pipelines, fuel producers, fuel oil refineries, storage and trucking companies, rail carriers, and ocean or river bound tanker ships/barges. Their input will aid in the assessment of the potential for disruption or failure. It will also lend credence to the assumptions.
  - Take steps to fully understand what information is already posted on a gas pipeline's EBB and how that information can readily be used for greater situational awareness. Ask for educational sessions when necessary to understand how to interpret posted information in a way that provides the most value. .
  - Discuss the fuel supplier's response plans if fuel supply disruptions were to happen. Rather than rely solely on a hands-off type of study (which still has value), consider the possible mitigating actions of the fuel supplier after the disruptions occur in order to incorporate the impact to the BPS into your analysis. Also consider the time considerations between the disruption and when it will impact the power system. Not all failures have immediate impact.
    - Outreach may include a review of disruption scenarios with each of the fuel suppliers operating within the studied region to assess the viability of both the assumed disruption scenarios as well as the potential downstream impacts.

As an example, ask the pipeline companies what remaining capacity would be available if they lost a particular pipeline segment. Depending on the pipeline configuration, the capacity serving the area's generators may be reduced by 10%, 50%, or not impacted at all. Each case would produce different input assumptions for the study.

Consider review of internal operational policies and procedures with the pipelines to better understand the impact of those procedures during a fuel supply disruption scenario.

Formatted: Left: 0.22", Right: 0.22"

Step 3: Formulate Study Input Assumptions and Initial System Conditions

Assumptions and system conditions may be developed by using information obtained from data gathering efforts outlined in Step 2 as well as regional historical experience to establish relevant scenarios for incorporation into the analysis. These assumptions may be specific (e.g., specific generator outage rates determined from regional historical averages) or expressed in terms of a range (e.g., low, medium, and high ranges of projected generator retirements affecting future fuel mix). Steps to develop these assumptions and conditions for the analysis include (but are not limited to) the following:

~~One existing analysis modeled a 14-day cold weather duration based on historical weather analysis. The study focused on cold weather events because historical risks to procurement of adequate fuel were most prominent during the winter when the needs of commercial and residential heating were competing with natural gas-fired and dual-fuel generators. The study considered projected typical winter load conditions as well as extreme winter load.~~

- Determine which fuel(s) to study. When doing so, consider the interdependence of various fuel types and how a large disruption to one fuel source may impact another fuel source.
- Develop fuel assumptions using the best available information:
  - Document fuel supply assumptions for plants where data is not available or up to date to maintain visibility of areas where the study may have weaknesses.
  - Consider fuel supply alternatives, such as dual fuel use and service from alternate pipelines.
- Determine weather and load assumptions:
  - Weather input to the study can be historical normal and extreme weather applied to future scenarios or some version of a weather or climate forecast that describes the study time frame.
  - For a fuel risk analysis, the system under study is more than just the BPS. There are going to be shared resources between different sub-systems that are interdependent; for example, natural gas is used for both heating and power generation. Understanding the relationship between those two classes of natural gas demand is paramount when performing this study. Knowing what will happen when the natural gas system is full due to colder temperatures will define what direction the study goes and, in large-part, the results of the study. Fuel oil works in a similar fashion but with a different mode of transportation. Although pipelines can carry fuel oil, it is typically via truck or barge. But the fundamental concept is the same—when it gets cold and the demand for fuel is up, supply chains become full and resulting supply options and priorities may be unexpected.
- Determine interchange assumptions and interface capability:
  - This should include coordination with neighboring entities to ensure accuracy and agreement of their interchange contribution. Consider whether the conditions selected for the study will also impact an adjacent area's interchange contribution.
  - A study may assume interchange transaction quantities that reflect the economic interaction between the studied systems and neighboring systems consistent with real-time operations. Alternatively, a historical analysis may be performed to determine an upper and lower bound for capacity and energy imports and exports.

    Coordination with neighboring systems should also include potential impacts of a natural gas disruption in one area on gas-fired generation in adjacent areas—affecting the amount of electric interchange support available.

- Determine generator outage rates and reductions assumptions:

- Generator outage rates may be defined by using standard methods (e.g., EFORd) or using a simple analysis of historical performance. Depending on the approach or assumptions, this may deviate from the normally accepted methods.

> **EFORd** *– Equivalent Forced Outage Rate demand*
> the probability a generator will fail completely or in part when needed

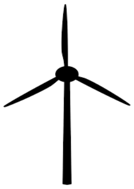
- Take care not to double count outages. Understand that if a generator is out of service due to normal outages, it cannot also be counted as a generator that is out of service due to fuel and vice-versa.

One analysis may assume generator forced outage rates across a 5-year historical period

Another may consider the impact of extreme cold weather on generator performance and calculate forced outage rates using a regression analysis

If fuel supply-related contingencies are explicitly modeled, then be sure to exclude them from the regression

- Determine assumptions related to VERs



  - These considerations will be critical in areas with high penetration of VERs where the output range can vary significantly.

As ofDuring 2022, wind generation output ranged from 0.55 GW to 16 24.3 GW in SPPMISO

- Consider the evolution of generation technology, changes in fuel mix, and the interdependency of future resource installation:
  - The current interconnection queue and integrated resource plans/resource adequacy plans may inform planners of resources to be selected in longer-term analyses.
  - Resource planning forecasts are performed on a regular basis. These studies evaluate the future needs and technologies to meet those needs:
    - These studies may reveal, for example, the likelihood of renewable ~~energyvariable~~energy variable energy resource additions and battery energy storage that result in early retirement of coal or fuel oil resources.
    - State emissions reduction objectives and policies could result in significant changes to the resource mix over a short period of time placing additional and changing demands on certain fuels such as natural gas.for additional dual-fuel resources, as another example, would likely introduce more gas/fuel oil generators into the interconnection queue.
  - It may be difficult to predict how the future resource mix will vary based on factors like governmental policy initiatives. Include a range of assumptions for items that have uncertainty.[29]

---

[29] https://www.iso-ne.com/static-assets/documents/2018/01/20180117_operational_fuel-security_analysis.pdf

ISO-NE OPERATIONAL FUEL SECURITY ANALYSIS[30]

ISO New England's Operational Fuel Security Analysis modeled a wide range of resource combinations that might be possible several years into the future. The study examined varying resource retirements, LNG availability, oil inventory, interchange, and renewable resources. In addition to a reference case which incorporated the likely levels of each variable, these input assumptions were varied individually to characterize the sensitivity between unfavorable to favorable boundary cases. Several combination scenarios, examining how multiple related changes would affect the outcome, were also examined which adjusted more than one of the key variables to represent future resource portfolios that could develop and their effects on fuel security.

- Determine performance criteria. For example:
    - If the study being performed contemplates a HILP contingency, perhaps the performance criteria would be that 90% of firm load is maintained for a short period of time. However, when HILP is studied, it should be done for emergency preparedness and not for measuring the reliability of specific system resources. Another consideration in this scenario would be acceptable system ratings and limits. If the study being performed contemplates a HPLI contingency, perhaps the performance criteria would be set to a base case, or up to unavailability of interruptible load.
- Determine the study frequency, outlook, and duration according to the risks identified through data gathering. Depending on the assumptions, electric system, or fuel supply chains that may have changed, the planner should use engineering judgement and historical information. See the three-column graphic on the next page for additional information.

---

[30] Id.

Frequency	Outlook	Duration
For choosing a study frequency (i.e., how often the study is performed), consider the following: • Operational time frame studies could be performed on a weekly, or monthly basis, or other near-term periodicity. For example, one existing analysis involves a winter weekly or non-winter biweekly energy study that is used on an ongoing basis for operations planning. • Seasonal studies could be performed periodically in the prewinter or presummer time frames in anticipation of the peak load seasons. • Longer-term studies could be performed annually, every few years, or on a longer-term periodicity as necessary. • Ad-hoc (one-time) studies could also be performed to assess a unique set of conditions and to achieve specific objectives, and may be more limited in scope.	For choosing a study outlook (i.e., when does the studied time horizon begin) consider the following: • Short-term operations planning study outlooks (e.g., one-week out, one-month out, six-months out, other-less than a year out) could be used. • Alternatively, near-term (1–5 years), long-term (6–10 years) transmission planning time horizons, or even greater study outlooks could be used if appropriate for the objectives of the study. For example, one existing analysis was based on a five-year look-ahead study to assess system resilience under future resource portfolios.	For choosing a study duration (i.e., what is length of the study window), consider the following: • The duration could be anywhere from a snapshot of the current system to a few days out or even to multiple years, depending on what is appropriate for the assumptions or objectives of the study. For example, one existing analysis involves a 14-day study window to model a plausible 14-day extreme cold weather scenario based on historical weather analysis. • Consider varying durations of fuel disruptions to determine how reliability conditions may change over time given a particular fuel disruption.

ISO-NE performs a 21-day look ahead energy assessment based on the lead time it takes to schedule an LNG and fuel oil truck delivery within the associated region.

- Include any special or additional scenarios or assumptions, such as the following:
  - Heavy seasonal directional power transfers
  - Changes in resource ~~mixgeneration~~mix/generation mix
  - Low variable energy resource production for a multi-day period
  - Drought or flooding conditions
  - Changes in fuel supply situation (e.g., closure of refineries or LNG storage facilities, new provisions that limit or prevent local gas and fuel oil transport)
  - System-wide blackout scenario (e.g., scenario studying fuel-related reliability risks to blackstart units and potential impact on system restoration following a blackout)
- Document the rationale behind study assumptions and initial system conditions

Formatted: Left: 0.22", Right: 0.22"

Step 4: Contingency Selection

The data gathered at this point will help to form the basis for contingencies to the fuel supply of the studied system. Some aspects will be known, and some will be assumed. It is possible that not all contingencies will be included in the final study once the probability and credibility of the various scenarios are better established. It may be prudent to establish a priority level for different contingencies based on the planner's experiences. There are many factors to consider in filtering and selecting the appropriate contingencies to study; this may include, but is not limited to, the following:

- The cause of the fuel disruption (which helps with developing proper mitigation)[31]
- The frequency with which the disruption has occurred in the past in this or other locations
- The probability or likelihood that the disruption will occur in the future
- The expected duration of the disruption based on historical data or reasonable assumptions that acknowledge system improvements over historical data:
    - Fuel disruption duration can be seasonally dependent. For example, a failed fuel delivery system during the high-demand winter months will likely be shorter in duration than a disruption during low-demand periods.
- The amount of fuel supply interrupted (This is a line to be drawn based on relevance to the scenario being studied.)

The loss of a single natural gas compressor engine at a station is more likely than the loss of an entire compressor station. Many fuel supply systems contain redundancies and safeguards, making a full outage of service less likely than a partial outage.

- The location of the disruption, even outside of your footprint as fuel delivery is a worldwide operation
    - Interdependence of global markets on local systems should not be overlooked (e.g., LNG imports in Japan surged following the 2011 Fukushima nuclear power shutdown.)
- The generating units that may be affected by the disruption (Be sure to account for remaining generating capability if any.)
    - Consider alternatives available to impacted generating units, such as dual fuel use and service from alternate pipelines[32]
- The extent or scope of the interruption as to whether it impacts other companies, industries, or other subsystems, such as the following:

---

[31] NERC Generator Availability Data System data collection was updated for 2020 reporting and going forward cause coding for "lack of fuel" reporting will be much improved.

[32] Eastern Interconnection Planning Collaborative (EIPC), 2015 Gas-Electric System Interface Study, Section 10 on Natural Gas and Electric System Contingency Analysis, https://eipconline.com/phase-ii-documents.

  - If flooding has washed out the railways in a particular area, rerouting coal delivery around that area will likely be more difficult due to all rail traffic trying to reroute to meet guaranteed delivery dates.
  - Consider the likelihood of mutual assistance between suppliers. It is within the realm of possibility that a pipeline or fuel oil transporter could suffer a loss of capability and receive assistance from an interconnected pipeline or associated supplier.
  - Consider whether electric load shedding to resolve BPS problems will impact fuel availability or subsequent plant operations.
  - Consider the impact of electric contingencies on the natural gas system or recovery from a natural gas disruption (e.g., loss of power to electric driven natural gas compressor stations or transmission contingencies that may restrict the redispatch of non-natural-gas-fired generators).
- The influence of governmental agencies may also factor into the studied response to contingencies:
  - Consider historical reactions by governing agencies.
  - Consider guidance from governmental agencies, such as the potential for cyber and/or man-made threats to fuel delivery systems.
  - Consider working with relevant governmental agencies to share the analysis, develop and gain any needed approval for mitigation measures.
- Nontraditional solutions may be available when directed by emergency management or similar agencies. Conversely, fuel supply could be made unavailable due to decisions made at the governmental level. For example, a port necessary for the delivery of LNG or fuel oil may be shut down following worldwide events that result in a state of heightened security. Another example may be the limited usage of fuel oil unless a special (environmental) waiver is granted by state or federal officials.

PJM FUEL SECURITY ANALYSIS

PJM introduced four different gas pipeline contingencies that represented disruption of supply in a segment for four different natural gas pipelines within the PJM region. Each contingency resulted in reduced capacity on the affected segment of the interstate pipeline, thereby impacting the ability to deliver natural gas to generating units downstream of the disruption. For each contingency, PJM simulated partial disruptions (medium impact event resulting in loss of a one out of multiple parallel lines in a pipeline segment) and full disruptions (high impact event resulting in loss of all parallel lines in a pipeline segment). Each of these contingencies modeled took into consideration the design of the affected pipeline segment to determine the reduced capacity of the pipeline and impact to downstream generator availability. The methodology for layering in the disruption scenarios and the assumptions for the duration of the disruptions were based on observed conditions during recent pipeline disruption events as well as consultations with the Natural Gas Council and major interstate pipeline companies serving the PJM region.

Following a pipeline disruption event impacting one of the looped lines in a pipeline segment, PHMSA has historically required a mandatory capacity reduction (typically about 20% firm capacity reduction) in the adjacent non-impacted lines within the same pipeline right-of-way until initial investigation of the incident is complete. PHMSA has also historically restricted access to an affected pipeline segment following an event for safety reasons, delaying immediate restoration efforts by pipeline operators. Both the capacity reduction and delayed restoration due to PHMSA's response should be considered when studying the natural gas pipeline contingency impact and duration.

- Document the rationale for each contingency selected.

Step 5: Selection of Tool(s) for Analysis

Because of individual system conditions and goals, no single type of transmission system analysis will meet the need of every planner. Therefore, each planner should consider the information gathered in the steps above and choose analysis tools that can provide information that will allow for a thorough assessment of their supply and transmission systems. This analysis may be power flow, stability or dynamic simulation, production cost modeling, market simulation, fuel oil and natural gas pipeline hydraulic flow modeling, deterministic versus probabilistic modeling, in-house tools, or any combination of these tools and others.

☐ Power flow
☐ Stability simulation
☐ Production cost modeling
☐ Market simulation
☐ Pipeline flow model
☐ Deterministic vs. probabilistic model
☐ In-house tools

Regardless of the tool(s) chosen, the rationale for the selection should be documented and reviewed periodically to ensure that the appropriate tools continue to be utilized and provide continuity from the end of the analysis to what was defined in the goals.

Step 6: Perform Analysis and Assess Results

Based on the information from Steps 1–5, system analysis will be performed and assessed. The assessment will evaluate system performance based on the criteria defined in Step 3 to determine if system deficiencies exist and, if so, what actions might be considered to improve the observed deficiencies. Every step of the process was defined, including the criteria for system performance. At this point of the analysis, the state of the system is known. If the assessment determines that the system does not meet the prescribed criteria for reliable operation of the power system, and corrective actions are needed, this step is where that would happen.

When delivering the results of the study, consider the audience. Consider their level of knowledge of the system being studied and speak to the audience at a level they will understand. Use commonly understood terminology, processes, and procedures so that the audience will more likely comprehend the results as intended.

Step 7: Develop Solution Framework

As noted in Step 3, fuel assurance studies should be completed on an ongoing basis. Regular analysis will help planners and other stakeholders better understand emerging risks as the power grid undergoes rapid transformation. Planners are encouraged to develop a solution framework to ensure fuel assurance in advance of any potential credible reliability issues. It is at this point that the planner should consider engaging governmental agencies that may be able to assist with developing a framework of potential solutions. One example might be contacting state environmental departments to discuss power plant air and water permits should a HILP contingency occur. At a larger regional level, planners are encouraged to consider developing a response and mitigation plan for grid, generator, and natural gas operators to guide their response to fuel assurance contingencies as identified in Step 4. Further, the development of a communications protocol for grid, generator, and natural gas operators could benefit the regional response to and mitigation of contingencies as identified in the risk analysis framework. These proactive actions will ensure preparedness and improved situational awareness to handle these potential risks in the future.

Formatted: Left: 0.22", Right: 0.22"

Formatted: Left: 0.22", Right: 0.22"

Formatted: Left: 0.22", Right: 0.22"

Formatted: Left: 0.22", Right: 0.22"

Appendix A: Risk Analysis Framework Checklist

This checklist outlines the actions recommended in **Chapter 4** into a list that entities may use as a reference when performing their own analysis. As mentioned at the beginning of **Chapter 4**, the listed steps are intended to be flexible enough to account for all fuel types, broad enough to support the unique circumstances in each region, and may be performed out of order (or in some cases not at all).

Step 1: Problem Statement and Study Prerequisites

- ☐ Define the study goal (i.e., problem statement)
- ☐ Set the criteria for system performance
- ☐ Communicate the goals of the study with all stakeholders (electric and fuel suppliers)
- ☐ Gain agreement on principal concepts
- ☐ Determine the timeline prior to commencing work
- ☐ Set the boundaries of the study
- ☐ Document agreed upon goals, time line, boundaries, etc.

Step 2: Data Gathering

- ☐ Coordinate fuel assurance assumptions with generator owners/operators
- ☐ Survey stakeholders (see **Appendix B**)
- ☐ Identify relevant fuel supply contingency events
- ☐ Maintain documentation for future use

Step 3: Formulate Study Input Assumptions and Initial System Conditions

- ☐ Determine fuel(s) to be studied
- ☐ Determine the interdependence of various fuel types
- ☐ Determine how a large disruption to one fuel source may impact another fuel
  - ☐ If needed, develop fuel assumptions in the absence of actual information
- ☐ Determine weather and load assumptions
- ☐ Determine interchange and interface capability
- ☐ Determine generator outage and reductions rate assumptions (e.g., EFORd)
- ☐ Determine assumptions related to variable energy resources
- ☐ Determine expected changes in regulatory policy, generation technology, and fuel mix, including the interdependency of resource installation
- ☐ Determine performance criteria using stakeholder input (e.g., is load loss acceptable? If so, for how long?)
- ☐ Determine study frequency, outlook, and duration
- ☐ Include any special or additional assumptions or system conditions, the following are examples:
  - ☐ Heavy seasonal energy transfers

    - ☐ Changes in generation mix
    - ☐ Droughts
    - ☐ Flooding
    - ☐ System-wide blackout scenario
- ☐ Document rationale for assumptions and system conditions selected

Step 4: Contingency Selection

Filter down identified contingencies. Consider CEII ramifications. Consider factors like the following:

- ☐ Cause of the fuel disruption
- ☐ Frequency with which the disruption has occurred in the past in this or other locations
- ☐ Probability or likelihood that the disruption will occur in the future
- ☐ Expected duration of the disruption based on historical data or reasonable assumptions
- ☐ Amount of the fuel supply interrupted
- ☐ Location of the disruption
- ☐ Generating units affected by the disruption and remaining generating capability (if any)
- ☐ Extent or scope of the interruption (does it impact other companies, industries, etc.)
- ☐ Influence of governmental agencies on the response to contingencies
- ☐ Document rationale for contingency selection

Step 5: Selection of Tool(s) for Analysis

Select analysis tools appropriate for the study, such as follows:

- ☐ Power flow
- ☐ Stability simulation
- ☐ Production cost modeling
- ☐ Market simulation
- ☐ Pipeline hydraulic flow modeling
- ☐ Deterministic vs. Probabilistic modeling
- ☐ In-house tools
- ☐ Document rationale for selection

Step 6: Perform Analysis and Assess Results

- ☐ Perform analysis
- ☐ Document and assess results
- ☐ Consider CEII ramifications

Step 7: Develop Solution Framework

☐ Identify potential risks

☐ Develop solution framework as needed and in concert with stakeholders, regulators, etc.

☐ Update existing plans and procedures

Formatted: Left: 0.22", Right: 0.22"

Appendix B: Items to Include in a Fuel/Energy Survey

This list is indicative but not all encompassing of the questions that planners may ask of its generator owners/operators depending on the regional study goals and the possibility of regional fuel type generation considerations.

When drafting a survey, consider whether certain questions should be made mandatory. Also consider how to format answer selections; should some be limited to multiple choice, is free form text more appropriate, etc. It will also be important to seek consistency in units of measurement. Make an effort to clarify what units are desired (MW, MWh, MMBtu/day, etc.) so that compiling and analyzing responses is straightforward.

General Information

- Resource information
    - Name
    - Contact
    - Unit identifier
    - Type
- Square footage of fence footprint and what percentage of that space is empty
- Is there a “bump-up” compressor on-site? How often is it used?
- Net max and min sustainable rating
- Design and/or current operational max/min ambient temperature
- Unit maximum Summer heat rate
- Unit maximum Winter heat rate
- Dual Fuel Unit heat rate on different fuels
- Primary fuel source
- Alternate fuel source
    - Fuel switching requirements, or other considerations
- Date of last MW disruption (or not received) on primary fuel (within the last 5 years)
- Amount of MWs disrupted (or not received)
    - Reason for disruption (or not received)
- Have any fuel supply procurement processes been compromised?
    - For example, limited trucking capability, navigation issues, lack of refinement capability from supplier
    - How often?
    - Any seasonal issues?
- Planned retirement date
- Is staffing required to start the unit?
- Is staffing required to switch fuels?

- Is unit black-start capable or on ISO/RTO system restoration Plan?
- Consumable item most limiting unit operations (e.g., limestone, chemicals, demineralized water trailers, air or water emission credits)
- Does the unit/station have existing on-site natural gas compression
- Availability of on-site boost compression
- Is there backup power on-site?
- Are there state restrictions on future use of this unit?
- What is the impact and duration of maintenance shutdowns?
- What is the risk of third-party damage to plant, inventory or transportation types to the plant?

Natural Gas Pipeline Information

- Companies providing physical natural gas pipeline connections
- Critical compressor facilities
  - Identify whether natural gas or electric compressors connected to or required by the unit (if known)
  - Identify if spare compression is available at each compressor site
- Required minimum pressure for full, half, and minimum output
- Required minimum pressure for unit operation (<full output)
- Peak burn rate
- Transportation contract
  - No-notice service, firm, enhanced Firm, secondary firm, interruptible, etc.
  - Transportation contract options available for natural-gas-fired generators
- Commodity
  - Type of service—firm or interruptible, Other?
    - Number of available suppliers
  - Number of pipelines
  - Storage access
  - Asset Management Arrangements (e.g., firm delivery expressed in MMBtu/day)
- Seasonal operations considerations
  - Identify any force majeure events called by the pipeline in the last 10 years
  - Identify any critical generators connected to the pipeline that could affect your deliveries
  - What is the nature of the balancing flexibility the pipeline offers you and provide a link to the tariff summary
- Seasonal maintenance considerations

Oil Information

- Limitations on oil burn, number of hours, emissions limitations, seasonality limits

- Number of hours of operation at max/min output on oil
- Maximum fuel storage capability
- Type(s) of oil (e.g., residual fuel oil, fuel oil #2, etc.)
    - Available usable fuel in storage (typical annual-average value)
- Plans to increase available usable fuel amount
- Assurance level for additional deliveries
- Can fuel be replenished faster than it is used?
- Alternate fuel contracts
- Number of alternate fuel suppliers
- Fuel primary and alternate transportation type (pipeline, barge, rail, truck, etc.)
- Fuel resupply limitations
    - Notice time and delivery time
    - Deliveries expected over given period of time (e.g., how many per day)
    - Proximity of supplier(s)
    - Available offloading facilities
- Does unit need natural gas to start?
    - If so, is the fuel stored on site?
- Do other units share oil inventory?
- If so, number of hours of operation at max output on shared oil

Coal Information

- Maximum storage capacity
    - Current inventory amount
- Inventory resupply plans
- Assurance level for additional deliveries
- Alternative suppliers
- Maximum output that can be sustained indefinitely
- Fuel primary transportation type (barge, rail, truck, etc.)
- Can fuel be replenished faster than it is used?
- Secondary transportation
- Fuel delivery time
- Is delivery on a schedule?
- Scheduled time between replenishments
- Maximum amount delivered in a single shipment

- Typical coal level for replenishment order
- Units that share coal inventory
- Max runtime for unit with shared fuel inventory
- Does unit need oil or natural gas to start?
  - If so, what fuel(s) is stored on site?
- What is the unit’s history of freezing coal inventory/piles and are any measures in place to mitigate freezing?

Alternate Fuel Information

- Alternate fuel source(s)
- Additional staffing requirements to start the unit on alternate fuel
- Number of hours of operation at max on alternate fuel
- Maximum fuel storage capability
- Available usable fuel in storage
- Plans to increase available usable alternate fuel amount
- Assurance level for additional deliveries
- Alternative suppliers
- Fuel primary transportation type (barge, rail, truck, etc.)
- Can fuel be replenished faster than it is used?
- Secondary transportation
- Alternate fuel resupply time
- Unit net MW max capability on alternate fuel
- Does the unit have to be taken off-line to switch to the alternate fuel?
  - If not, what is the MW output level needed to perform switching?
- Time to transition to alternate fuel
- Date alternate fuel capability was last tested
- Amount of net MW output achieved while on alternate fuel
- Does unit need natural gas to start?
  - If so, is the fuel stored on site?
- Max number of starts per day on alternate fuel
- Number of starts per week on alternate fuel
- Can generator operate on both fuels simultaneously?

Environmental/Emissions

- Unit environmental/emissions limitations
- Pollutant responsible for most limiting emissions limit

- Limit periodicity of pollutant responsible for most limiting emissions limit
- Pollutant responsible for most second most limiting emissions limit
- Limit periodicity of pollutant responsible for most second most limiting emissions limit
- Other environmental/emissions concerns

Guideline Information and Revision History

Commented [MS1]: Elsa or Bob, add the tables from the EG Operational Coordination RG

Metrics

Pursuant to the Commission's Order on January 19, 2021, North American Electric Reliability Corporation, 174 FERC ¶ 61,030 (2021), reliability guidelines shall now include metrics to support evaluation during triennial review consistent with the RSTC Charter8.

Baseline Metrics

All NERC reliability guidelines include the following baseline metrics:

- BPS performance prior to and after a reliability guideline as reflected in NERC's State of Reliability Report and Long Term Reliability Assessments (e.g., Long Term Reliability Assessment and seasonal assessments)
- Use and effectiveness of a reliability guideline as reported by industry via survey
- Industry assessment of the extent to which a reliability guideline is addressing risk as reported via survey

Specific Metrics

The RSTC or any of its subcommittees can modify and propose metrics specific to the guideline in order to measure and evaluate its effectiveness, listed as follows:

- RTOS will conduct periodic evaluations of the gas system supply constraints that have resulted in derates to generators. These will be categorized and tracked for trend analyses. This information is available to NERC in GADS7.

Effectiveness Survey

On January 19, 2021, FERC accepted the NERC proposed approach for evaluating reliability guidelines. This evaluation process takes place under the leadership of the RSTC and includes:

- industry survey on effectiveness of reliability guidelines;
- triennial review with a recommendation to NERC on the effectiveness of a reliability guideline and/or whether risks warrant additional measures; and
- NERC's determination whether additional action might be appropriate to address potential risks to reliability in light of the RSTC's recommendation and all other data within NERC's possession pertaining to the relevant issue.

NERC is asking entities who are users of reliability and security Guidelines to respond to the short survey provided in the link below.

Guideline Effectiveness Survey

Errata

Date: N/A

Contributors

Contributor	Company
Matthew Agen	American Gas Association
~~Randall Van Aartsen~~	~~Jacksonville Electric Authority~~
Nancy Bagot	Electric Power Supply Association
~~Jordan Bakke~~	~~MISO Energy~~
~~Eric Baran~~	~~Western Interstate Energy Board~~
~~Karie Barczak~~	~~DTE Energy~~
~~Scott Barfield-McGinnis~~	~~North American Electric Reliability Corporation~~
~~Marcus Beasley~~	~~SERC Reliability Corporation~~
~~Olivier Beaufils~~	~~Wood Mackenzie~~
~~Richard Becker~~	~~SERC Reliability Corporation~~
~~Matthew Beilfuss~~	~~WE Energies~~
~~Bashir Bhana~~	~~Independent Electricity System Operator~~
~~Katrina Blackley~~	~~North American Electric Reliability Corporation~~
~~Jeffery Bloczynski~~	~~Americas Power~~
Michelle Bloodworth	Americas Power
~~Jonathan Booe~~Sean Bodkin	~~North American~~Dominion Energy ~~Standards Board~~
~~Mike Boughner~~	~~Xcel Energy~~
~~Peter T. Brandien~~	~~Independent System Operator - New England~~
John Brewer	National Energy Technology Laboratory
~~Dick Brooks~~	~~Reliable Energy Analytics LLC.~~
David Brown	NextEra Energy Resources, LLC
Layne Brown	Western Electricity Coordinating Council
~~Keith Burrell~~	~~New York Independent System Operator~~
~~Masuncha Bussey~~Jim Davis	~~Duke~~Dominion Energy
~~Rob Cashell~~Joan Dreskin	~~Colorado Springs Utilities~~Interstate Natural Gas Association of America
~~Augustine Caven~~	~~PJM Interconnection~~
~~Thomas Coleman~~	~~North American Electric Reliability Corporation~~
~~Jeffery Dagle~~	~~Pacific Northwest National Laboratory~~
~~Enoch Davies~~	~~Western Electricity Coordinating Council~~
~~Lewis De La Rosa~~	~~Texas Reliability Entity~~
~~Leeth DePriest~~	~~Southern Company~~
~~Jay Dibble~~	~~Calpine~~
~~William Donahue~~	~~Puget Sound Energy~~
Katie Ege	Great River Energy
~~Omar Elabbady~~	~~Xcel Energy~~
~~Christine Ericson~~	~~Illinois State Government~~
~~Ed Ernst~~	~~North American Transmission Forum~~
~~Lynna Estep~~	~~North American Transmission Forum~~
~~Brian Evans-Mongeon~~	~~Utility Services, Inc.~~
~~Eric Eyberg~~	~~Wood Mackenzie~~
~~Patrick Farace~~	~~Federal Energy Regulatory Commission~~
~~Daniel~~Dan Farmer	Entergy
~~Philip Fedora~~Brian Fitzpatrick	~~Northeast Power Coordinating Council~~PJM Interconnection
~~Mike Ferguson~~Dale Hinson	~~Indeck~~Dominion Energy ~~Services, Inc.~~

Formatted ... [3]
Formatted ... [5]
Formatted ... [1]
Formatted ... [4]
Formatted Table ... [2]
Formatted ... [8]
Formatted ... [10]
Formatted ... [6]
Formatted ... [9]
Formatted Table ... [7]
Formatted ... [13]
Formatted ... [15]
Formatted ... [11]
Formatted ... [14]
Formatted Table ... [12]
Formatted ... [18]
Formatted ... [16]
Formatted ... [17]
Formatted ... [21]
Formatted ... [23]
Formatted ... [19]
Formatted ... [22]
Formatted Table ... [20]
Formatted ... [26]
Formatted ... [24]
Formatted Table ... [25]
Formatted ... [27]
Formatted ... [28]
Formatted ... [30]
Formatted ... [32]
Formatted ... [29]
Formatted ... [31]
Formatted ... [36]
Formatted ... [33]
Formatted ... [35]
Formatted Table ... [34]
Formatted ... [37]
Formatted ... [38]
Formatted ... [41]
Formatted ... [43]
Formatted ... [39]
Formatted ... [42]
Formatted Table ... [40]
Formatted ... [46]
Formatted ... [47]
Formatted ... [44]
Formatted ... [48]
Formatted Table ... [45]
Formatted ... [49]
Formatted ... [50]
Formatted ... [53]
Formatted ... [51]
Formatted ... [52]

~~Jennifer Flandermeyer~~Cindy Hotchkiss	Southern Company~~Evergy~~

Formatted: Not Expanded by / Condensed by

Formatted: Normal

Formatted: Normal, Indent: Left: 0"

~~Contributors~~

~~Contributor~~	~~Company~~
~~Stephen Folga~~	~~Argonne National Laboratory~~
~~Michael Fortini~~	~~DTE Energy~~
~~Tim Fryfogle~~	~~ReliabilityFirst~~
~~Dennis Gee~~	~~Pacific Gas and Electric Company~~
~~Bill Graham~~	~~North American Electric Reliability Corporation~~
~~Venona Greaff~~	~~Occidental Petroleum Corporation (OXY)~~
~~Wayne Guttormson~~	~~Sask Power~~
~~Maria Hanley~~	~~Federal Energy Regulatory Commission~~
~~Katherine Harsanyi~~	~~United States Department of Energy~~
~~Christina Hayes~~	~~Berkshire Hathaway Energy Company~~
~~Daniel Head~~	~~Consolidated Edison Company~~
~~Lynn Hecker~~	~~MISO Energy~~
~~Bradley Heisey~~	~~Tenaska, Inc.~~
~~Mark Henry~~	~~Texas Reliability Entity~~
~~Michael Herman~~	~~PJM Interconnection~~
~~Jo Hsiung~~	~~Federal Energy Regulatory Commission~~
~~Michael Isper~~	~~Interstate Natural Gas Association of America~~
Patricia Jagtiani	Natural Gas Supply Association
~~Marilyn Jayachandran~~Alan Kloster	Evergy~~PJM Interconnection~~
~~Leah Kaffine~~	~~ABB~~
~~Anuj Kapadia~~	~~Federal Energy Regulatory Commission~~
~~James Kavicky~~	~~Argonne National Laboratory~~
~~Tom~~Mike Knowland	Independent System Operator ~~-~~New England
Andrea Koch	Edison Electric Institute
~~William Lamanna~~	~~North American Electric Reliability Corporation~~
~~Russell Laursen~~	~~WEC Energy Group~~
~~Suzanne Lemieux~~	~~American Petroleum Institute~~
Michael Lombardi	Northeast Power Coordinating Council
Connie Lowe	Dominion Energy
~~Glen Lyons~~	~~Exxon Mobil~~
~~Eli Massey~~	~~MISO Energy~~
~~David McConkey~~	~~Canadian Gas Association~~
~~William Meyer~~	~~NextEra Energy Resources, LLC~~
~~Leah Michalopulos~~	~~Canadian Electricity Association~~
~~Sharon Midgley~~	~~Exelon~~
~~Reene Miranda~~	~~Xcel Energy~~
~~Roger Moraitis~~	~~NextEra Energy~~
~~Mehmet Aydemir Nehrozoglu~~	~~Consolidated Edison Company~~
~~Brent Oberlin~~Mike Mattox	Midwest Independent System Operator~~ – New England~~
~~Brian O'Boyle~~	~~Consolidated Edison Company~~
~~Mark Olson~~Al McMeekin	North American Electric Reliability Corporation
~~Raymond Orocco-John~~Michael Oberleitner	~~Federal~~Dominion Energy ~~Regulatory Commission~~
~~C. J. Osmano~~Maggie O'Connell	Interstate Natural Gas Association of America
~~Darrell Pace~~	~~Southern Company~~
~~Jason Pan~~	~~Wood Mackenzie~~
~~Martin Paszek~~	~~Consolidated Edison Company~~
~~Jaimin Patel~~	~~Sask Power~~

Formatted: Not Expanded by / Condensed by

Formatted ... [54]

Formatted: Normal

Formatted: Normal, Indent: Left: 0"

Formatted Table

Formatted: Not Expanded by / Condensed by

Formatted: Normal

Formatted: Normal, Indent: Left: 0"

Formatted: Not Expanded by / Condensed by

Formatted ... [55]

Formatted: Normal

Formatted: Normal, Indent: Left: 0"

Formatted Table

Formatted: Not Expanded by / Condensed by

Formatted ... [56]

Formatted: Normal

Formatted: Normal, Indent: Left: 0"

Formatted: Not Expanded by / Condensed by

Formatted ... [57]

Formatted Table

Formatted ... [58]

Formatted ... [59]

Formatted: Not Expanded by / Condensed by

Formatted: Not Expanded by / Condensed by

Formatted: Normal

Formatted: Normal, Indent: Left: 0"

Formatted ... [60]

Formatted: Normal

Formatted: Normal, Indent: Left: 0"

Formatted Table

Formatted ... [61]

Formatted: Normal

Formatted: Normal, Indent: Left: 0"

Formatted Table

Formatted: Not Expanded by / Condensed by

Formatted: Normal

Formatted: Normal, Indent: Left: 0"

Formatted ... [64]

Formatted ... [62]

Formatted ... [63]

Contributors

~~Contributor~~	~~Company~~
~~Margaret Pate~~	~~North American Electric Reliability Corporation~~
Levetra Pitts	North American Electric Reliability Corporation
Thomas Popik	Foundation for Resilient Societies
~~Michael Powell~~	~~Canadian Electricity Association~~
~~Donna Pratt~~Elsa Prince	North American Electric Reliability Corporation
~~Theresa Pugh~~Joseph Ricasio	~~Theresa Pugh Consulting~~Independent Electricity System Operator
~~Ryan Ramcharan~~	~~Consolidated Edison Company~~
~~Raborn Reader~~	~~Enterprise Products Partners, LP~~
~~Laura Ritter~~	~~Duke Energy~~
Sammy Roberts	Duke Energy
~~Cathy Rourke~~	~~Tellurian, Inc.~~
~~Stephen Rourke~~	~~Independent System Operator - New England~~
~~John Rudiak~~	~~Avangrid~~
~~Allen Schriver~~Brent Sessions	~~Florida~~Western Area Power ~~and Light~~Administrator
Phillip Shafeei	Colorado Springs Utilities
~~Jared Shaw~~Tim Sherwood	Southern Company~~Entergy~~
~~Wayne Sipperly~~	~~North American Generator Forum~~
~~Aiden~~Chris Smith	~~Oneok, Inc.~~Interstate Natural Gas Association of America
~~Todd Snitchler (Vice Chair)~~Mark Spencer	~~Electric~~LS Power ~~Supply Association~~Development
~~Stephen Stafford~~	~~Georgia Transmission Corporation~~
~~Bob Staton~~	~~Xcel Energy~~
John Stevenson	New York Independent System Operator
~~David Swiech~~Katherine Street	~~DTE~~Duke Energy
~~Albert Taylor~~	~~Wabash Valley Power Alliance~~
~~Michelle Thiry (Chair)~~	~~Entergy~~
~~Chad Thompson~~Robert Tallman	North American Electric Reliability ~~Council of Texas~~Corporation
~~Justin Thompson~~	~~Arizona Public Service~~
~~Devon Tremont~~	~~Taunton Municipal Lighting Plant~~
~~Kyle VanderHelm~~	~~Tenaska, Inc.~~
~~Juan Villarreal~~	~~Villarreal Energy, LLC~~
~~Nick Voris~~	~~Kansas City Power and Light~~
~~Yajun Wang~~	~~Dominion Energy~~
~~Douglas Webb~~	~~Evergy~~
~~Steve Wenke~~	~~Avista Corporation~~
~~Matt Whitenett~~	~~Fortress Information Security~~
~~Patrick Wilkey~~	~~Argonne National Laboratory~~
~~Noman Williams~~	~~Grid Alliance~~
~~Wes Williams~~	~~Bryan Texas Utilities~~
~~Cyndy Wilson~~	~~United States Department of Energy~~
~~Scott Winner~~	~~Bonneville Power Administration~~
~~Brad Woods~~	~~Texas Reliability Entity~~
~~Craig Wrisley~~	~~Xcel Energy~~
~~Ping Yan~~	~~Electric Reliability Council of Texas~~
Charles Yeung	Southwest Power Pool, Inc.
~~Joel Yu~~	~~Consolidated Edison Company~~

Formatted ... [66]
Formatted ... [65]
Formatted ... [69]
Formatted ... [72]
Formatted ... [74]
Formatted ... [70]
Formatted ... [73]
Formatted Table ... [71]
Formatted ... [76]
Formatted ... [78]
Formatted ... [75]
Formatted ... [77]
Formatted ... [82]
Formatted ... [79]
Formatted ... [81]
Formatted Table ... [80]
Formatted ... [83]
Formatted ... [84]
Formatted ... [87]
Formatted ... [89]
Formatted ... [85]
Formatted ... [88]
Formatted Table ... [86]
Formatted ... [90]
Formatted ... [92]
Formatted Table ... [91]
Formatted ... [93]
Formatted ... [94]
Formatted ... [95]
Formatted ... [97]
Formatted ... [96]
Formatted ... [100]
Formatted ... [98]
Formatted ... [99]
Formatted ... [103]
Formatted ... [101]
Formatted ... [104]
Formatted Table ... [102]
Formatted ... [107]
Formatted ... [105]
Formatted ... [106]
Formatted ... [110]
Formatted ... [112]
Formatted ... [108]
Formatted ... [111]
Formatted Table ... [109]
Formatted ... [115]
Formatted ... [113]
Formatted ... [114]
Formatted ... [119]
Formatted ... [116]
Formatted ... [118]
Formatted Table ... [117]
Formatted ... [122]
Formatted ... [124]

Page 38: [1] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 38: [2] Formatted Table Mark Spencer 6/30/2023 3:00:00 PM

Formatted Table

Page 38: [3] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [4] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 38: [5] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [5] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [6] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 38: [7] Formatted Table Mark Spencer 6/30/2023 3:00:00 PM

Formatted Table

Page 38: [8] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [9] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 38: [10] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [10] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [10] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [11] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 38: [12] Formatted Table Mark Spencer 6/30/2023 3:00:00 PM

Formatted Table

Page 38: [13] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [14] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 38: [15] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [16] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 38: [17] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 38: [18] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [19] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 38: [20] Formatted Table Mark Spencer 6/30/2023 3:00:00 PM

Formatted Table

Page 38: [21] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [22] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 38: [23] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [23] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [23] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [24] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 38: [25] Formatted Table Mark Spencer 6/30/2023 3:00:00 PM

Formatted Table

Page 38: [26] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [27] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 38: [28] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [28] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [28] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [29] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 38: [30] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [31] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 38: [32] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [32] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [32] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [33] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 38: [34] Formatted Table Mark Spencer 6/30/2023 3:00:00 PM

Formatted Table

Page 38: [35] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 38: [36] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [37] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 38: [38] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 38: [39] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 38: [40] Formatted Table Mark Spencer 6/30/2023 3:00:00 PM

Formatted Table

Page 38: [41] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [42] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 38: [43] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [43] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [44] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 38: [45] Formatted Table Mark Spencer 6/30/2023 3:00:00 PM

Formatted Table

Page 38: [46] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [47] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 38: [48] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 38: [49] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Space Before: 0 pt, Line spacing: single

Page 38: [50] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0", Space Before: 0 pt, Line spacing: single

Page 38: [51] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 38: [52] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 38: [53] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 40: [54] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 40: [54] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 40: [54] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 40: [55] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 40: [55] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 40: [55] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 40: [55] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 40: [56] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 40: [56] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 40: [57] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Space Before: 0 pt, Line spacing: single

Page 40: [58] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0", Space Before: 0 pt, Line spacing: single

Page 40: [59] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 40: [59] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 40: [59] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 40: [60] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 40: [60] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 40: [61] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 40: [61] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 40: [61] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 40: [61] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 40: [62] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Space Before: 0 pt, Line spacing: single

Page 40: [63] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0", Space Before: 0 pt, Line spacing: single

Page 40: [64] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 40: [64] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 40: [64] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 40: [64] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 40: [64] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [65] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Body Text, Line spacing: Multiple 0.06 li

Page 41: [66] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Font: 10 pt

Page 41: [67] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Body Text, Line spacing: Multiple 0.06 li

Page 41: [68] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Font: 10 pt

Page 41: [69] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Left: 0.22", Right: 0.22"

Page 41: [70] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 41: [71] Formatted Table Mark Spencer 6/30/2023 3:00:00 PM

Formatted Table

Page 41: [72] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [73] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 41: [74] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [74] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [74] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [74] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [75] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 41: [76] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [77] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 41: [78] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [79] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 41: [80] Formatted Table Mark Spencer 6/30/2023 3:00:00 PM

Formatted Table

Page 41: [81] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 41: [82] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [82] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [82] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [82] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [83] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 41: [84] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 41: [85] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 41: [86] Formatted Table Mark Spencer 6/30/2023 3:00:00 PM

Formatted Table

Page 41: [87] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [88] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 41: [89] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [90] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 41: [91] Formatted Table Mark Spencer 6/30/2023 3:00:00 PM

Formatted Table

Page 41: [92] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 41: [93] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [93] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [94] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 41: [95] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [96] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 41: [97] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [97] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [98] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 41: [99] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 41: [100] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [101] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 41: [102] Formatted Table Mark Spencer 6/30/2023 3:00:00 PM

Formatted Table

Page 41: [103] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [104] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 41: [105] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 41: [106] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 41: [107] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [107] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [108] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 41: [109] Formatted Table Mark Spencer 6/30/2023 3:00:00 PM

Formatted Table

Page 41: [110] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [111] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 41: [112] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [112] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [112] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [112] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [113] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 41: [114] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 41: [115] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [116] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 41: [117] Formatted Table Mark Spencer 6/30/2023 3:00:00 PM

Formatted Table

Page 41: [118] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 41: [119] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [119] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [120] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal

Page 41: [121] Formatted Table Mark Spencer 6/30/2023 3:00:00 PM

Formatted Table

Page 41: [122] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [123] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Normal, Indent: Left: 0"

Page 41: [124] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [124] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [124] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Not Expanded by / Condensed by

Page 41: [125] Formatted Mark Spencer 6/30/2023 3:00:00 PM

Body Text, Space Before: 0.5 pt

Draft Reliability Guideline

Fuel Assurance and Fuel-Related Reliability Risk Analysis for the Bulk Power System

September 2023

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

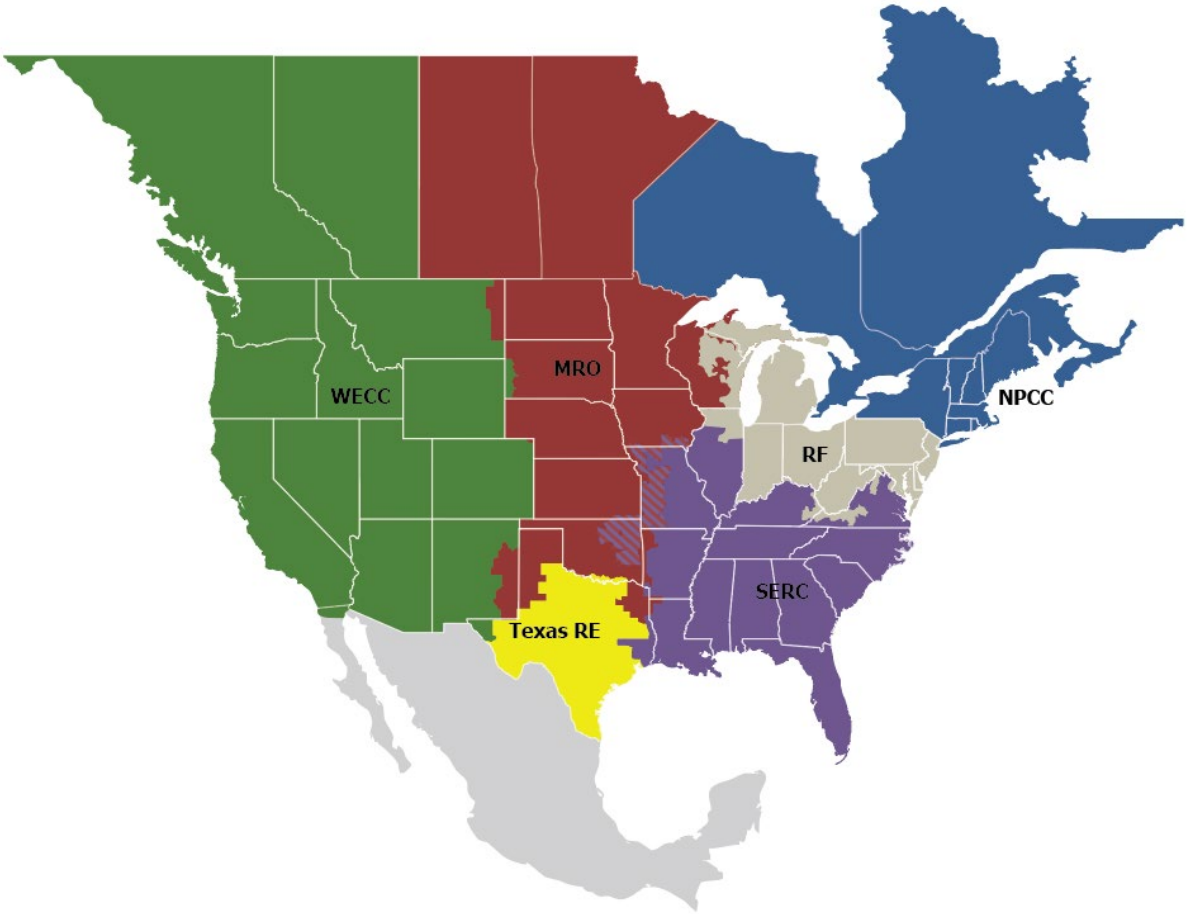
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the NERC and the six Regional Entities, is a highly reliable, resilient, and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six Regional Entities as shown on the map and in the corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Preamble

The NERC Reliability and Security Technical Committee (RSTC), through its subcommittees and working groups, develops and triennially reviews reliability guidelines in accordance with the procedures set forth in the RSTC Charter. Reliability guidelines include the collective experience, expertise, and judgment of the industry on matters that impact BPS operations, planning, and security. Reliability guidelines provide key practices, guidance, and information on specific issues critical to promote and maintain a highly reliable and secure BPS.

Each entity registered in the NERC compliance registry is responsible and accountable for maintaining reliability and compliance with applicable mandatory Reliability Standards. Reliability guidelines are not binding norms or parameters nor are they Reliability Standards; however, NERC encourages entities to review, validate, adjust, and/or develop a program with the practices set forth in this guideline. Entities should review this guideline in detail and in conjunction with evaluations of their internal processes and procedures; these reviews could highlight that appropriate changes are needed, and these changes should be done with consideration of system design, configuration, and business practices.

Executive Summary

NERC, as the Federal Energy Regulatory Commission (FERC) certified ERO,[2] is responsible for the reliability of the BES and has a suite of tools to accomplish this responsibility, including but not limited to the following:

- Lessons Learned
- Reliability and security guidelines
- Assessments and reports
- The Event Analysis Program
- The Compliance Monitoring and Enforcement program
- Mandatory Reliability Standards

It is in the public interest for NERC to develop reliability guidelines that are useful for maintaining and enhancing the reliability of the Bulk Electric System (BES). Reliability guidelines establish a voluntary code of practice on a particular topic for consideration and use by BES users, owners, and operators. The NERC Reliability and Security Technical Committee (RSTC), through its subcommittees and working groups, develops and triennially reviews and, as necessary, updates reliability guidelines in accordance with the procedures set forth in the RSTC Charter.[1]

Each entity registered in the NERC compliance registry is responsible and accountable for maintaining reliability and compliance with applicable mandatory Reliability Standards. Reliability guidelines include the collective experience, expertise, and judgment of the industry on matters that impact BPS operations, planning, and security. Reliability guidelines provide key practices, guidance, and information on specific issues critical to promote and maintain a highly reliable and secure BES. Reliability guidelines are not to be used to provide binding norms or create parameters by which compliance to NERC Reliability Standards are monitored or enforced. Entities are encouraged to review these guidelines in detail and in conjunction with evaluations of their internal processes and procedures. While the incorporation of guideline practices is strictly voluntary, reviewing, revising, or developing a program using these practices is highly encouraged to promote and maintain BES reliability.

---

[1] https://www.nerc.com/comm/RSTC/RelatedFiles/RSTC_Charter_Board_Approved_Nov_4_2021.pdf

Introduction

Purpose

The purpose of this reliability guideline is to ensure registered entities have relevant information to (i) plan for the procurement of sufficient fuel to serve load and have modeled contingencies for both short-term operational horizons to long-term planning timeframes, (ii) fully understand fuel supply chain risks, and (iii) offer additional conditions and constraints, especially during extreme events, to consider when performing studies. This reliability guideline may inform potential scenario analyses - e.g., loss of fuel, compressor outages, etc., but it is not intended to provide the environmental conditions contemplated under those studies.

Background

The rapid advancement of renewable generation, retirement of coal- and oil-fired generation, and increased use of natural gas have necessitated the need to re-evaluate the methods that the industry has historically utilized to analyze and maintain BPS reliability. Specifically, the increased reliance on just-in-time dispatchable generation, in particular, natural gas, to back up variable generation. This reliance requires an examination of the potential for compounded fuel/energy supply challenges and exemplifies the increased importance of thoroughly characterizing cross-sector interdependencies.

In November 2017, NERC published the Special Reliability Assessment: Potential Bulk Power System Impacts Due to Severe Disruptions on the Natural Gas System (2017 NERC Special Assessment).[5] In that report, NERC made numerous recommendations for assessing disruptions to natural gas infrastructure and related impacts to the reliable operation of the BPS in planning studies, several of which were assigned to the NERC Planning Committee (PC), a predecessor to the Reliability and Security Technical Committee (RSTC). In July 2018, the PC convened a workshop to highlight ongoing "fuel assurance" discussions and studies and to convene experts from across industries to develop a plan for action. In November 2018, the NERC Board approved a set of recommendations developed by the PC to address issues raised as a result of concerns from the 2017 NERC Special Assessment. One such recommendation was the development of this reliability guideline, which was assigned by the PC to the newly formed Electric Gas Working Group. The initial guideline was approved by the RSTC in March 2020. This document is the first revision to the March 2020 guideline and will provide entities guidance on how to evaluate such risk factors, ascertain potential impacts on the BPS, and potentially mitigate the risks.

This guideline offers a definition of "fuel assurance" in **Chapter 1** and takes a cursory look at all major fuel sources used to supply electric generation in **Chapter 2**. As each fuel type possesses a variety of physical and commercial characteristics that affect its delivery through its entire supply chain, **Chapter 3** describes specifically what those characteristics may be and provides guidance to assist planners and system operators in the development of fuel security analyses. Appendix A includes a design basis that was approved by the RSTC in October 2022 for a potential future electric-gas study.

here have been a number of relevant studies performed—especially by regional transmission organizations, independent system operators (RTO/ISO), and other organizations[2] to analyze and assess generator fuel-related considerations. This guideline combines the experience gained from these studies and post-event analyses to outlines a framework in **Chapter 4** that may be applied across all NERC Regions for effectively evaluating potential reliability risks to the BPS through the lens of fuel assurance. Applying this framework for a given area will provide indications of where credible risks to reliability exist and will highlight areas for further analysis and consideration.

---

[2] E.g., *The Eastern Interconnection Planning Collaborative Gas-Electric Interface Study* performed under the DOE grant and completed in June 2015

Though this guideline discusses planning, commonalities in the assessment techniques, processes, and procedures discussed are applicable to all time frames and may be adopted by more than just Transmission Planners and Planning Coordinators. Terms like “planner,” “generator owner/operator,” and “fuel supplier” are not capitalized intentionally so that the concepts presented may be considered and applied in the broadest sense as they pertain to the BES.

In accordance with Section 8 of the RSTC charter, approved Reliability Guidelines or Technical Reference Document shall be reviewed for continued applicability by the RSTC at a minimum of every third year since the last revision. The contents of this guideline encompass updates developed by the Electric Gas Working Group during its 2023 triennial review[3] that include insights and recommendations taken from the *FERC-NERC-Regional Entity Staff Report: The February 2021 Cold Weather Outages in Texas and the South Central United States*.[4] The EGWG will continue to work with NERC to gauge the effectiveness of this reliability guideline and support efforts for continued improvement and opportunities for education and information sharing.

---

[3] INSERT RSTC APPROVAL & DATE

[4] https://www.nerc.com/pa/rrm/ea/Documents/February_2021_Cold_Weather_Report.pdf

Chapter 1: Fuel Assurance

For the purposes of this guideline, "fuel assurance" will be defined as follows:

- **Fuel Assurance:** Proactively taking steps to identify fuel arrangements or other alternatives that would provide confidence such that fuel interruptions are minimized to maintain reliable BPS performance during both normal operations and credible disruptive events.

Fuel Assurance is critical across all planning time horizons and continuing on to real-time operations.[5] The criteria to establish the level of confidence referenced in the definition is unique to respective planning areas and is established by planners, system operators, and/or generator owners/operators based on internal assessments, situational awareness, contractual supply arrangements, and understanding of asset characteristics. The regional planner's focus is to assess the vulnerabilities of the entire region to withstand fuel disruptions that could impact multiple generators and impact reliable BPS performance. The role of the system operator demands significant situational awareness and system operators would benefit from utilizing all relevant public and non-speculative non-public information available in order to facilitate reliable delivery of fuel in the operational horizon. Generator Owners/Operators should communicate in a timely manner to the system operators how the terms of their fuel and transportation contracts may impact their unit specific performance parameters and operations and whether they reasonably foresee fuel availability issues. As the fuel mix of generation and wholesale electricity market structures can vary greatly across reliability areas, this guideline does not and cannot prescribe a single approach to the process.

NERC encourages planners to proactively model, evaluate and consider specific BPS impacts based on credible events that could compromise the provision of reliable service to all or part of the region within the regional planner's area of responsibility and to develop strategies to mitigate credible risks. Regional planners may consider modeling extreme fuel disruptions to better understand the impact of catastrophic events so that they may prepare for such emergencies. Recognizing that there is no way to anticipate or measure all potential threats and catastrophic scenarios, stakeholders and system operators should focus on effective measures that will maintain reliable and fuel-secure BPS operations during credible events. While the individual unit owners are ultimately responsible for effectively managing the fuel needs of particular units, the system operators, in advance of an actual contingency, should understand the risk and consequences of losing critical generators. They should consider the steps necessary to limit the reliability impact of such losses, such as maintaining adequate reserves and potentially select other sources of supply in advance if the risk is unacceptable.

Fuel Assurance Principles

While each reliability area is unique, there are common principles for fuel assurance that may be applied more broadly to assist planners and system operators in their assessments of fuel supply reliability. Below are some examples of actions that various entities may perform to advance fuel assurance initiatives.

Transmission Planners/Planning Coordinators

Planners should consider using steps outlined in **Chapter 4.** of this guideline to develop credible fuel-related contingencies that may be used in planning studies, including (but not limited to) Reliability Standard TPL-001 (Transmission System Planning Performance Requirements).[6] Any identified fuel-related contingencies should be evaluated for reliability risks, and planners should determine what (if any) mitigation should be put in place. Planners might consider conducting generator fuel-related surveys to determine potential risks to the fuel supply of the generators. Using the survey data, planners may perform fuel-related reliability risk analyses as described in **Chapter**

---

[5] Time_Horizons.pdf (nerc.com)

[6] See NERC Standard TPL-001-4 – Transmission Planning Performance Requirements, Table 1 –Steady State & Stability Performance Extreme Events, 3.a.i.

4. Planners should also seek and use experts familiar with regional markets and practices to help interpret and analyze the survey data.

System Operators

System gas requirements and availability are influenced by locational electrical demands and constraints and when unit commitment are made. This suggests the need for a centrally situated party to maintain a high-level of situational awareness. System operators should consider how to work voluntarily with as many stakeholders as possible through non-disclosure agreements or other mechanisms to receive non-public information that would assist their detailed understanding of grid demands and challenges and to maintain this utmost situational awareness. FERC Order 787, for example, allows interstate gas pipelines and electric transmission operators to share, on a voluntary basis, non-public operational information with each other to promote grid reliability and operational planning. System operators should consider how they can maximize the use of public and non-public information, how to best coordinate with all parties while preserving the confidentiality of the non-public information, and make decisions that facilitate the proper utilization of gas infrastructure, leverage the value of precedent transportation arrangements, and respect the pipeline operational constraints.

Generator Owners/Operators[7]

Generator owners/operators should seek reliable delivery solutions from a transportation, commodity, and commodity procurement perspective. BES reliability risks associated with emissions limits, fuel availability, transportation or delivery options should be monitored and evaluated. For example, with regard to use of natural gas, consider the “firmness” of the transportation agreement to include policies, processes or tariff provisions which could restrict gas flow (e.g., NAESB pipeline scheduling timeline), flow rule and constraint realities; and the commodity availability at the relevant trading hub.

Generator owners/operators should consider credible fuel-related contingencies that may impact their facilities and provide fuel-related facility outage concerns as necessary to the relevant reliability authority. Planning for credible fuel-related contingencies strengthens a generator’s ability to ensure it can run when called upon during critical events. Lastly, where fuel delivery constraints are routinely evident, generator owners/operators should consider whether new options for fuel deliveries to a specific facility or their fleet are available.

---

[7] https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_LTRA_2022.pdf (Page 14)

Chapter 2: Electric Generation Fuel Supply Primer

This section describes the supply chain of each major generator fuel supply type at a high level. It describes illustrative challenges that may be encountered between production and consumption as well as other viable considerations specific to each fuel type. These considerations will assist planners in forming realistic assumptions when developing their own fuel assurance and reliability risk analysis.

Natural Gas

Over the last 18 years domestic production of natural gas has doubled[8], mostly due to new well development techniques that have lowered production costs and allowed extraction in previously uneconomic or technologically inaccessible fields. The relative economics of natural gas, coupled with tightening environmental regulations on other fuel types, led to the increased development of new gas-fired generation in some regions. Additionally, gas-fired combustion turbines and reciprocating engines have relatively fast-start times and ramping capabilities that complement the variable nature of wind and solar resources that are being developed in many parts of the United States at accelerating rates. Consequently, the bulk electric system increasingly relies on the gas industry to deliver more natural gas with greater flexibility.

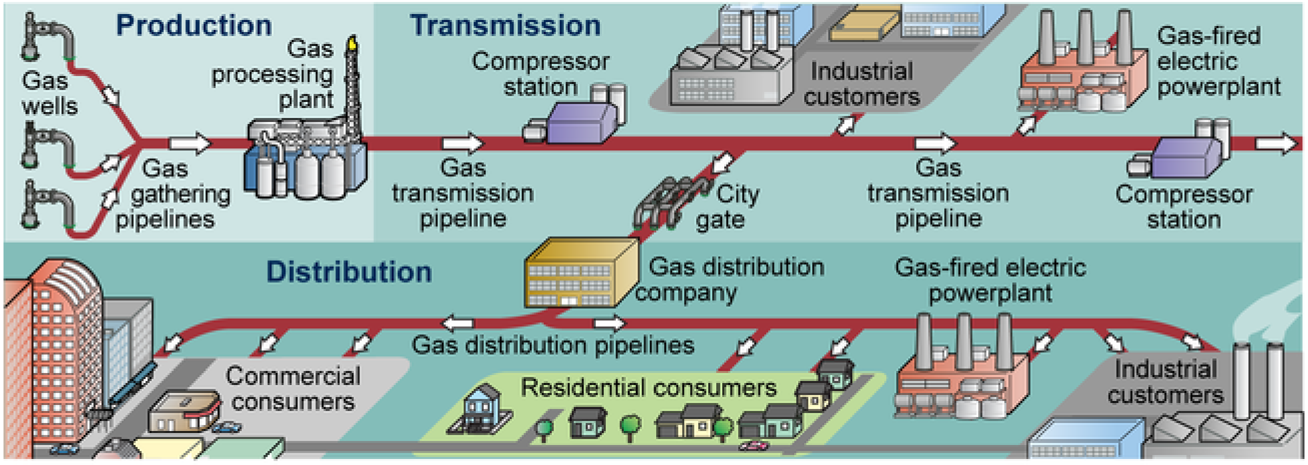
These increased new demands on the natural gas industry are highlighting issues that planners and system operators may not have had to grapple with previously but which are becoming more important to ensuring electric reliability. The physical differences between systems that convey compressed pipeline quality gas and electricity drive operational and administrative differences, which manifest through fundamental differences in scheduling and operational flexibility. Clearly, the throughput capacity of the natural gas system is of paramount importance; however, the timing that shippers nominate fuel and how that fuel must be taken is of equal importance and might, in many circumstances, impact their ability to run when called upon. Pipeline operators’ nomination and scheduling systems, and ultimately flow, are timed to ensure gas system reliability. Unlike the electric grid, pipeline operators require time to configure their systems in advance, and constrained conditions may limit system operators’ ability to call on gas-fired generators if fuel has not been nominated in accordance with pipeline tariff nomination deadlines and flow rules. Additionally when pipelines are flowing at near or maximum capacity, pipeline operational flexibility that is typically provided on a best efforts basis and supports non-spinning Operating Reserves may not be available. Both conditions require planners and system operators to examine the scheduling constraint timelines and the physical realities of the gas systems when performing studies and constructing day ahead operating plans, especially during stressed conditions. However, the limitations and constrained conditions may not exist universally and requires a careful, regional analysis of the natural gas supply chain. This section breaks the natural gas supply chain into segments, describes their function at a high level, and identifies areas of potential risk.

The natural gas supply and delivery chain includes three major segments, listed below:

- Production and Processing
- Transmission and Storage
- Distribution

---

[8] https://www.eia.gov/dnav/ng/hist/n9070us2A.htm



Source: GAO analysis of Energy Information Administration and Natural Gas Council documents. | GAO-20-658

Figure 2.1: Natural Gas Supply Chain

The rest of the section describes the characteristics of each segment and considerations relevant to the electric industry.

Production and Processing

Natural gas is primarily found in reservoir pools and shale rock formations in the earth and brought to the surface through production wells. Unprocessed natural gas withdrawn from natural gas or crude oil wells is usually “wet” natural gas because, along with methane, it contains natural gas liquids (NGL)—ethane, propane, butane, and pentane—and water vapor. Since methane, the primary constituent of pipeline-quality gas, remains in its gas phase down to -260 deg F, wellheads are more susceptible to “freeze-offs” when the wells have relatively high fractions of water vapor, which freezes in the wellhead or gathering system blocking the flow of gas. While the most effective method of preventing wellheads from freezing is to remove the water, this is not always cost-effective or possible. Another common method is to inject methanol into the gas stream for later removal. Producers may also be able to increase production in other areas or rely on using supplies they have natural gas in storage.[9] Some wellhead natural gas is sufficiently dry, and less prone to “freeze-offs.” Additionally, electrically-driven equipment, including compressors and processing facilities, used in the natural gas supply chain should be reviewed to ensure that it is on a critical circuit and would not be cut during manual load shedding, or that coordination occurs with operators of these facilities with sufficient time to facilitate switching to co-located non-electrically driven equipment or on-site backup power generation. It is imperative that both planners and system operators understand the diversity of production sources, what risks fuel producers face, and how those producers may mitigate those risks.

From the wellhead, natural gas is sent to processing plants where water vapor and nonhydrocarbon compounds are removed and NGLs are separated from the wet gas and sold separately. Like any other type of operations in the gas and power sector, processing plant operations can be impacted during critical events, and natural gas must be processed in order to meet interstate gas pipeline quality specifications. The processed natural gas is called dry, consumer-grade, or pipeline-quality natural gas. If the natural gas is not processed, and a pipeline cannot blend the gas, in most instances it will not be accepted into the interstate gas pipeline system. The processed natural gas is then transported via gathering systems into either intra- or interstate gas pipelines.

Transmission and Storage

Large-diameter interstate and intrastate pipeline transmission systems transport processed natural gas to large-volume customers (e.g., local distribution companies (LDCs), natural gas-fired power generation, industrial users, gas

---

[9] *Id.*

marketers). Processed natural gas is also transported to various storage facilities for future consumption. Compressor stations are located along the pipelines and storage network to maintain pressure at serviceable levels. In most cases, compressor units are powered by the natural gas in the pipelines. However, some compressor stations may have both natural gas and electric or even diesel-driven compressor units, and; others may rely solely on electric power. As mentioned above, it's important that pipeline operators identify their electric compressors and communicate those sites to the ISO/RTO so that, should an event warrant load shedding, those units are prioritized and curtailed last and restored first.

While the natural gas transmission system may continue to operate even with the failure of as many as half of the compressors, the pressure may not remain high enough to meet the specific pressure requirements of each power generator interconnected to the pipeline, which can range from around 100 psi up to more than 1,000 psi for some turbine models.[10] To add redundancy, many gas-fired generators have on-site boost compression that increases the pressure of the pipeline-delivered natural gas to the combustion inlet pressure required by the unit. Generation facilities that do not have boost compression may be more susceptible to outage under certain pipeline operating conditions.

Typically, limited supply and transportation disruptions can be managed through substitution, transportation rerouting, on site peaking supply, third-party delivered supply contracts, and storage services (though such infrastructure redundancy is much more limited in certain portions of North America, such as the Northeast). However, unlike electricity through a transmission line, gas flows much more slowly through a pipeline, which also necessitates more advanced planning by shippers and end users. Pipeline operators carefully manage the flows into and out of their pipelines, especially when demand on the pipeline is expected to be high, through scheduling procedures, alerts, notices, operational flow orders (OFOs)[11], and ultimately imposing over-run penalties restricting withdrawals if the shipper disregards the OFO A fundamental understanding of pipeline operations and market constructs is necessary to understand how gas scheduling may impact electric reliability.

Distribution

Intrastate transportation, balancing, storage, and distribution of natural gas by LDCs is subject to provincial regulation. LDCs are regulated by most states as local natural gas utilities that have an obligation to serve the customers for which the system is built to serve reliably (e.g., residential, and commercial heating customers). State statutes and public utility regulations may allow intrastate pipelines and LDCs to curtail services to some industrial or non-core customers, possibly including power generators, during emergencies to maintain the operational integrity of the system and/or maintain natural gas service to designated high-priority customers. Historically, these state regulatory requirements give the highest priority to residential (essential human need) and small commercial customers without short-term alternatives.

Pipeline Tariffs and Contracting Arrangements

The interstate pipeline industry is contract-based, and understanding the supply and transportation fuel arrangements requires having a basic knowledge of these contract terms and conditions. Shippers that are interconnected directly to interstate facilities contract with the pipeline and storage operators in accordance with the terms of FERC-approved agreements and tariffs. Gas-fired generators purchase bundled commodity supply and transportation services from a third-party marketer or an exchange, or enter into commodity and transportation contracts separately. Marketers either hold the transportation service outright or offer capacity released by other shippers with firm entitlement rights under an asset management agreement. The entitlement holder may not need all of its capacity at all times and allow marketers to re-sell released capacity to offset the entitlement holder's fixed reservation cost. However, it is important to note that the volume and liquidity of this secondary market moves inversely to the demands of firm shippers. That is, when gas demand is highest, shippers that have not made prior

---

[10] https://gasturbineworld.com/shop/performance-specs/2022-performance-specs-38th-edition/

[11] An Operational Flow Order is a mechanism to protect the operational integrity of the pipeline. It requires shippers to balance their gas supply with their usage on a hourly and/or daily basis, within a specified balance, per the tariff's requirements. It is not a curtailment.

arrangements may not be able to obtain the bundled fuel and transportation in the secondary market. Shippers that are interconnected to intrastate pipelines or to LDCs will have contracting arrangements unique to the jurisdiction and the contracting parties; users are advised to consult the facility-specific contracts for additional details.
Interstate shippers may select transportation and storage services based on the level of certainty and reliability desired. Some gas-fired generators contract for firm transportation ("FT"), which is a reservation of capacity on the pipeline from the origin ("receipt point specified") to the designated delivery point. The delivery point is usually a city gate (if the generator is connected to the LDC), an interconnecting pipeline, or the gas meter at the generator's facility. The receipt points may vary and a few examples include generators holding FT:

1. only on a short lateral that interconnects to an interstate pipeline;
2. on segments of an interstate pipeline that are known to be constrained; or
3. to a liquid trading hub or a dedicated storage facility;

Other generators that are interconnected to a main pipeline within a liquid trading hub may not enter into a transportation contracts. On the other hand, some generators may contract for FT and storage, which may be classified as "enhanced" transportation services. This contracted service allows shippers to call on gas "non-ratably" and generally shortens the flow lag from normal FT or IT service. Enhanced service should not be mistaken for "no-notice" or on-demand service, which is a premium service in which the pipeline commits to serve the shipper when called upon, yet typically is ratable service. Consequently, current FT recourse pipeline services may not be well-suited to serve non-spinning Operating Reserves, which require electricity to be generated with little or no advance notice and gas at large rates to be delivered non-uniformly. The intent is not to enumerate every possible contracting combination but to illustrate that the contracting arrangements are extremely varied and may not be the primary determinant of gas availability.

Contracting firm transportation capacity alone does not guarantee delivery of natural gas supplies at a specific location and time. Firm delivery must also consider a purchase of fuel (sufficiently in advance of when needed), pipeline nomination cycles, flow rules, and then-effective pipeline constraints. The North American Energy Standards Board ("NAESB") has developed uniform nomination windows for shippers to "nominate" gas prior to and during the gas day, which currently runs from 9:00am – 9:00am Central Clock Time ("CCT"). While shippers may nominate during any nomination cycle, during high demand periods most gas deliveries are nominated and scheduled at the Timely Nomination Cycle. Therefore, it is important for a shipper to nominate at the earliest cycle to ensure that it has secured its delivery point. There typically is less capacity available later in the nomination cycles. This is especially true if the receipt point is relatively illiquid or the transportation path follows segments that are known to often be constrained. Moreover, firm shippers may "bump" scheduled interruptible shippers up to the Intraday 3 cycle (7:00pm CCT intraday) per FERC policy.

Another important consideration is that pipeline operators are not obligated to flow the gas until the flow time specified in the NAESB nomination timeline approved by FERC. In some cases, this delay from the end of the nomination cycle until gas is allowed to flow to the shipper is up to 4 hours. However, many pipelines have tariff authority and often use best efforts to allow a generator gas to flow sooner than the flow time specified in the NAESB timeline. It is important to note that when gas demand is high, this operational flexibility should not be assumed. In fact, planners should make allowances for these constraints in their modelling efforts and system operators and generators should communicate frequently with the pipeline operators, and review pipeline critical notices, to understand how much flexibility, if any, may be afforded under stressed conditions.

An additional complexity is that pipeline operators may also issue OFOs which to require shippers to stay within certain daily and/or hourly imbalance tolerances per the pipeline tariff. These OFOs may be necessary to maintain the pipeline's, and their shippers', operational reliability and integrity, particularly during extremely (high or low) demand periods. For example during a ratable OFO, this means that shippers must flow their daily scheduled quantity of gas in 1/24th hourly increments, with some small percentage of hourly imbalances, but returning back within balance by the end of the gas day. Should a shipper disregard the OFO, significant penalties may accrue for non-compliance. If an OFO is issued, affected generators may need to modify their minimum or maximum run times; and reduce their ability to follow load. Synchronized generators, operating under a ratable OFO, may need to reduce their regulation ranges and operating reserve capabilities. Pipeline operators are required to post all critical and non-critical notices on their respective Electronic Bulletin Boards ("EBB"), including the specifics, duration, and geographic location of any OFO. Finally, it is important to know whether shippers have contractual entitlement to have gas delivered to a "primary delivery point." If a pipeline calls a primary delivery point restriction it is important to understand whether the generator has delivery at that primary delivery point. under constrained conditions, when firm transportation shippers are using their full contractual entitlements and there is not excess capacity, a pipeline operator may the pipeline operators restrict delivery to "primary delivery points." U ", unless the shipper's location is a "primary delivery point" it would not be able to schedule gas to the facility and thus be unavailable.

While we cannot understate the complexity of understating how a large number of shippers and pipeline operators may interact under certain scenarios, most of the information necessary to develop reasonable judgments is publicly available. FERC requires pipeline and storage operators to post a significant amount of data on their EBBs, including information about pipeline design, operating and operationally available capacity by receipt and delivery point, critical and non-critical notices, identification of firm pipeline shippers, and capacity release information. Additionally, interstate pipelines and storage operators may communicate non-public information, on a voluntary basis, to grid operators and vice versa to facilitate the reliable operation of their respective grids, per FERC Order 787. Intrastate pipelines are typically under the jurisdiction of state regulatory authorities, and the amount of publicly available information varies widely from state-to-state. While FERC Order 787 only covers pipeline and storage operators and grid operators, it does not prevent grid operators from requesting and receiving non-public data from intrastate pipeline operators and LDCs under non-disclosure agreements.

In addition to transportation services, customers also purchase the physical commodity directly from a gas producer or from a gas marketer to receive natural gas at contracted points into the applicable transportation system agreements and/or at other points of delivery at their respective interconnection points or market center. Larger volume customers (e.g., LDCs and electric generation facilities) may also purchase natural gas upstream at or near the point of production and contract for pipeline service to transport the commodity to the point of delivery. In addition, based on market conditions, these entities and other market participants may purchase natural gas at a market center and contract for transportation from that point to a delivery point(s). While commodity arrangements may be as varied as transportation arrangements, the generators that are typically used for grid balancing – i.e., gas peakers, typically do not have enough operational certainty to enter into forward contracts for the commodity. If these particular generators do not receive unit commitments with sufficient advanced notice, they may not be able to source the commodity during the operating day under constrained conditions, and especially at more thinly traded hubs. A reasonable proxy for liquidity may be the volume of transaction for a particular point on Intercontinental Exchange, Inc. ("ICE").

In summary, gas-fired generators' contractual arrangements offer insight into how gas may be transported to facilities; however, other factors influence generators ability to effectuate gas deliveries. These conditions may be crudely grouped as "transportation constraints." Another important consideration, especially for gas peakers, is the relative natural gas supply liquidity during periods of high demand of the shipper's trading hub. If the supply/trading hub is relatively illiquid and the generator does not usually receive unit commitments day ahead, the risk that these generators may not be able to source the commodity during peak demand days increases. Obviously, both transportation and commodity are required to ensure fuel can be delivered. Some generators may be uniquely positioned or have sufficiently mitigated performance risk through transportation and commodity contracts to be at low risk if of non-performance. Conversely, other generators may be poorly positioned and have high transportation and commodity risk. While still others may have either heightened transportation or commodity risk, but not both. It may be necessary planners examine historical pipeline critical notices and trading hub history in addition to historical generator performance to determine fuel availability risk.

Oil

Fuel oil is obtained from the petroleum distillation process as either a distillate or a residual and is then distributed to regional bulk terminals for distribution to end users. Transportation to generation sites is typically by pipeline, barge, truck, or a combination of the three methods where it is off-loaded into on-site fuel tanks. Each power plant with storage tanks will have unloading facilities that frequently limit the ability to replenish the on-site storage tanks. Each generator with oil as either the primary or back-up fuel must decide the amount of fuel oil that will be kept in inventory or reserved for other uses such as maintenance or black start service obligations. Aside from any emissions limitations, facilities typically do not have sufficient replenishment capability to run continuously at maximum output for long durations. Replenishment rates are dependent on availability of transport tankers (maritime or over-the-road) and pipelines, and expected transportation constraints - e.g., competition with resupply of home heating oil, dearth of licensed drivers, roads impassable due to weather conditions, rivers impassable due to ice conditions, etc. There are multiple types of fuel oil and generators are typically designed to operate on or switch to a specific type. A majority of oil combustion capable units in the NERC footprint fire distillate ultra low-sulfur fuel oil #1 – e.g., ultra-low-sulfur diesel, jet fuel, kerosene, etc. or #2, also known as home heating oil. Others primarily combust distillate fuel oil one of the three residual “bunker” fuels #4, #5, and #6.

Coal

Four major types of coal are used to produce electric power, each of which varies in heat content and chemical composition:

- **Bituminous:** Bituminous coal is a middle rank coal between subbituminous and anthracite containing 45%–86% carbon. Bituminous usually has a high heating (Btu) value (11,000 – 15,000 Btu/lb). and is the most common type of coal used in electricity generation in the United States. In 2021, bituminous accounted for about 45% of coal mined in the U.S., with a majority originating from mines in five states. Since 2020, all coal produced in Canada was sourced from bituminous seams.
- **Subbituminous:** Subbituminous coal is black and dull (not shiny) containing 35%–45% carbon and has a higher heating value (8,500 – 13,000 Btu/lb) than lignite. In 2021, subbituminous accounted for about 46% of coal mined in the U.S. with more than 85% coming from the Powder River Basin in Wyoming.
- **Lignite:** Lignite coal, aka brown coal, is the lowest grade coal with the least concentration of carbon (25%–35%) and the lowest heat content (4,000 – 8,000 Btu/lb). In 2021, lignite accounted for about 8% of coal mined in the U.S. with most going to electricity generators a short distance from the mine. Most lignite is produced and consumed in North Dakota and Texas.
- **Waste coal:** Usable material that is a byproduct of previous coal processing operations. Waste coal is usually composed of mixed coal, soil, and rock (mine waste), often called gob or culm. Most waste coal is burned as-is in unconventional fluidized-bed combustors with the fuel source co-located with or near to the generator. The heat and carbon content of waste coal is highly variable and is often blended with higher grade coals to ensure a minimum combustor heat input. Most waste coal combusting facilities are located near former mine sites and were purpose built for reclamation.

Coal is extracted from surface and underground mines in various regions around the United States. The United States has over 250 years of remaining coal reserves. It is then crushed and washed in preparation for transport to power plants. Transportation is typically by rail, barge, truck, or conveyor belts; the latter used at what are called mine-mouth power plants. Coal may be delivered directly to a power plant or to a nearby unloading terminal from which it proceeds to the power plant by truck or a conveyance system. At the plant, coal is stored on-site in piles to be used as needed for generation, typically in an amount sufficient for several weeks to several months of operation. Long-term supply contracts are used to ensure high levels of reliable coal deliveries. Equally as important, coal plants require certain reagents to scrub the flue gas – e.g., any of a number of forms of lime, aqueous or anhydrous ammonia, activated carbon, etc. and chemicals to support ongoing operations – e.g., water treatment chemicals.

These reagents and chemicals are typically transported via truck and most facilities have storage sufficient for a few weeks operations.

Nuclear

Nuclear plants are refueled every 18–24 months. Required outages cannot normally be delayed due to costs and scheduling of specially trained labor. Nuclear plants need to maintain certain reactivity levels in nuclear fuel. At times, this reactivity requirement has led to units derating in shoulder months in order to conserve fuel and be available to operate 100% during peak months.

Four major processing steps must occur to make usable nuclear fuel: mining and milling, conversion, enrichment, and fuel fabrication. The uranium used in power plants comes from Kazakhstan, Canada, Australia, and several western states in the United States. Major commercial fuel enrichment facilities are in the United States, France, Germany, the Netherlands, the United Kingdom, and Russia.[12]

Both fresh and spent fuel are typically stored on site at nuclear plants in specialized facilities, when not in the reactor, that are built to withstand significant physical events, including weather, seismic, and other types of natural disaster. Licensees must abide by robust security measures (e.g., armed security officers), physical barriers, and intrusion detection and surveillance systems.[13]

The Nuclear Regulatory Commission regulates nuclear facilities in the United States and the Nuclear Safety Commission regulates facilities in Canada. Nuclear power plants must show that they can defend against a set of adversary characteristics called the Design Basis Threat (DBT). DBT imposes security requirements on nuclear power plants based on analyses of various factors, such as the potential for a terrorist threat. The Nuclear Regulatory Commission regularly evaluates the DBT for updates and alignment with the threat environment.

Nuclear facilities use digital and analog systems to monitor, operate, control, and protect their plants. Digital assets critical to plant systems for performing safety and security functions are isolated from the external networks, including the internet. This separation provides protection from many cyber threats.

Hydro

An integrated hydro-electric system, like those found in the Pacific Northwest, is more frequently energy limited than capacity limited from its mix of storage and run-of-river projects. The storage projects fill and draft annually and tend to have a steady discharge. Fluctuations in discharge (generation) are usually driven by snow melt water content, flood control, maintenance of navigation channels, seasonal icing, and downstream water temperature objectives. The run-of-river projects more closely follow demand as the projects fill and draft daily. However, run of river projects have limited storage to meet demand because the water needs to be in the right place(s) at the right time(s). Hydro-electric generation also has many non-power objectives that can limit hydro- electric power production (e.g., lake/river level management, recreational use, stream flow speeds, etc.) Information sharing, communication, and coordination is critical across different hydro projects, utilities, states, and countries.

Variable Energy Resources, Energy Storage, and Developing Technologies

Technologies like weather dependent BPS-connected solar photovoltaic and wind generation are being integrated at an accelerating pace, and the "fuel" for wind and solar generation are effectively limitless but are only available as weather conditions permits. For storage devices, including batteries, the energy they provide is dependent on some other electric energy producing resource. Therefore, storage devices are not electric generators but rather may time shift the consumption of electricity generated in a less constrained period to a more constrained period.

---

[12] https://www.nei.org/fundamentals/nuclear-fuel

[13] https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/security-enhancements.html and https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/cyber-security-bg.html

Operators and planners should ensure sufficient energy is available given the non-dispatch-limited controllable nature of solar and wind resources and the regulatory imposition of "must-take" requirements in many areas. In particular, peak demand hours will present new challenges for planning and procuring fuels for flexible, swing generation, such as natural gas generation, as the penetration of nature-controlled resources increase. Two primary concerns are emerging as penetrations increase. Many regions are using probabilistic analysis and capacity-based metrics, such as Effective Load Carrying Capability, to model the resource adequacy contribution of variable generation during extreme conditions, yet the actual generation during these conditions could vary widely in either direction across a planning footprint. Therefore, it is important to examine the distribution of possible variable generation outputs from the modelling efforts and select appropriately low tail probability generation scenarios to ensure there are sufficient back-up resources in the event these low probability generation conditions occur. The second concern is to ensure that back-up resources may be both deliverable and able to respond in the operational horizon to changes in variable generation. There exists an inherent error between the forecasted variable generation and what is actual produced in the operating day. While the error may be small, there may be unique conditions that make this error much larger – e.g., icing of wind turbine blades, fog, smoke, temperature extremes, etc., and it is imperative to ensure there are sufficient back-up resources that are capable of responding during these outlier events. Moreover, these issues may be compounded by the inherent increase of forecast risk across a weekend and holiday periods when gas typically trades for multiple days ahead of the Day Ahead electric market. These conditions highlight the importance of modelling low probability, or extreme scenarios, with respect to resource adequacy contribution and potential for generation forecast error, quantifying the potential need, and confirming that there is sufficient dispatchable generation is available and any temporal constraints that dispatchable generation may have due to fuel arrangements.

Other technologies (e.g., energy storage) are still in early stages of development, and deployment of these technologies will require further evaluation and consideration as they mature. For instance, system operators and planners need to understand how co-located facilities with variable energy production and storage systems charge and discharge onto the grid. The charging and discharging behavior of energy storage devices may be responsive to regulatory demands and incentives, or ancillary service market price signals, and are not always conducive to assisting operators manage real time energy demand. For storage devices, including batteries, the energy they provide is dependent on some other electric energy producing resource. Therefore, storage devices are not electric generators but rather a mechanism for time shifting the production of electricity for later deployment, and offer fuel assurance only to the extent that they can shift energy generation from a less constrained period to a more constrained period. Additionally, many of today's energy storage technologies are subject to operational temperature limitations that may limit their ability to charge and discharge[14].

Hydrogen and ammonia are other emergent technologies developing technology that will require close attention and coordination as they potentially grow as fuels for power generation. If hydrogen utilizes the same transportation infrastructure as natural gas, it has 1/3rd the heating value on a volumetric basis, which will require significant build out to deliver the same energy. Today, most hydrogen is produced using natural gas reforming technologies and is primarily used in petroleum refining and chemical production. As hydrogen technologies advance and hydrogen use as a power generation fuel expands, it will be necessary for planners to consider many of the same concerns that exist today with the supply and procurement of natural gas in addition to coordinating with hydrogen producers relying on electrically intensive processes such as electrolyzers and hydrogen fueled generators to ensure that sufficient stocks and production are maintained to ensure the availability of generation during extreme conditions.

---

[14] https://batteryuniversity.com/article/bu-410-charging-at-high-and-low-temperatures

Chapter 3: Fuel Supply Risk Analysis Consideration

As described in **Chapter 1**, fuel assurance is critical across all planning time horizons and continuing on to real-time operations. Some fuel assurance risks may not be completely mitigated and must be accepted, and some risks may increase the fuel assurance risk of other resource types in the same time horizon. Fuel assurance risk is not static over time, and there may be interdependencies between different resource types, especially in the real time. Therefore, it is imperative that a thorough risk analysis investigate how fuel may be limited over various time horizons, how risks between fuel type may be interrelated, and if the generator's parameters allow timely conversion of fuel into electricity to match system demands. This chapter describes the supply chain considerations of each generator fuel supply type that will help planners and system operators form realistic assumptions when developing their own fuel-related reliability risk analyses.

Natural Gas

Chapter 2 touched on the myriad ways transportation and commodity procurement are combined to deliver gas to generators. There are four main considerations when qualifying fuel risk for gas-fired generators, but no one factor may be able to adequately capture fuel risk or be dispositive of risk. Moreover, some risks may not be additive and it may be difficult, if not impossible, to quantify these risks. However, a structured framework may allow planners and operators to assign generators to risk categories or rank generators by their relative risk. Planners and operators may then use these results to influence decisions regarding the quantity and type of Planning and Operating Reserves required.

The four factors are:

- The timing of when the generator typically receives a unit commitment relative to the NAESB gas pipeline nomination cycles;
- The gas fired generator's contractual arrangements—i.e., the "firmness" of the transportation path from the customer's receipt point to the generation facility's meter (delivery point);
- The "firmness" of the generator's supply arrangements as well as the accessibility of readily available supply alternatives in the spot market to supplement or backup day-ahead purchases (such as having trading hubs, pools or pipeline interconnects in close proximity);
- Historic constraint points along the generator's transportation path.

While a generator's contractual arrangements are not the only determinant of fuel assurance risk, planners and operators may easily ascertain whether a generator has purchased firm transportation or storage from a pipeline, which pipeline rate schedule establishes the terms of the generator's service, and the generator's receipt and delivery points. Each pipeline posts an Index of Customers—a list of their firm transportation and storage shippers—on their public websites and updates the Index quarterly. The Index is not dispositive of a generator's contractual arrangements; a generator may contract with an asset manager rather than with the pipeline for its natural gas transportation and supply needs. Nor is the possession of rights to firm transportation dispositive of fuel assurance risk. In some circumstances, such as when the pipeline is fully subscribed, the generator may be unable to purchase firm transportation absent an expansion of pipeline capacity.

After identifying the generator's contractual arrangements, planners and operators should inquire further into the generator's circumstances:

- **Is the primary delivery point coincident with the generator's gas meter?** If it is not, this might indicate a pipeline capacity constraint at the generator's location. In this circumstance, planners and operators should consider how often and under what conditions the pipeline restricted deliveries to primary delivery points or to primary point shippers. When such restrictions occur, a generator on a secondary delivery point would be unable to transport gas to its facility. There are sufficient occurrences where deliveries to secondary firm locations can occur and may otherwise lessen some of this type of fuel delivery risk.

- **If the generator obtains pipeline capacity through capacity release or through a marketer/asset manager, under what conditions can the releasing shipper or manager "recall" the capacity?** Capacity release and market/asset manager arrangements might permit the release shipper or manager to recall (i.e., take back) pipeline capacity obtained by a generator. Planners and operators should identify the circumstances under which recall might occur and consider the pipeline capacity unavailable under those conditions.
- **How frequently is the natural gas commodity traded at points accessible to the capacity path? What volume of natural gas commodity trades at those points?** Pipeline transportation contracts specify the receipt point where the shipper will deliver natural gas commodity into the pipeline system. While not dispositive, pipeline paths that include "liquid" points—points that have high volumes of trades throughout a given gas day or interconnect with other interstate pipelines with liquid trading points—tend to provide more certainty that the natural gas commodity will be available to the generator. If the generator's transportation path does not include liquid points, then planners and operators should further investigate the "firmness" of supply.
- **How does the minimum pressure the pipeline must provide at the generator's delivery point compare to the minimum required pressure to operate the generator's facility?** If the contractual delivery pressure is less than the generator's minimum operating pressure, how often has the facility been de-rated or unavailable due to pressure limitations? How often has the pipeline restricted the shipper to its tariff pressure limitations? If no minimum pressure is specified in the generator shipper's pipeline transportation contract, has the generator been derated or unavailable due to low supply pressure?

As the section above indicates there are many factors that impact the real time delivery of natural gas supply to a power generator. No single factor should be deemed dispositive as to whether a natural gas fuel arrangement is reliable or unreliable, as pipelines and pipeline conditions vary across the United States. Notwithstanding, **Appendix A** outlines some factors Planners may consider when determining the reliability of supply arrangements (specifically, fuel supply delivery).

The timing of the generator's unit commitment might affect its ability to obtain fuel. As a general rule, natural gas fuel procurement and associated scheduled pipeline deliveries are best ensured with a timely dispatch signal/unit commitment. Regardless of how "firm" a generator's pipeline capacity contract may be, if committed after the day ahead Timely Cycle, natural gas supply availability, in the commodity market, should also be considered.

Furthermore, fuel delivery flexibility and constraints can vary by pipeline, season, planned or unplanned maintenance events, delivery location and peak demand events. The points, listed below, provide some guidance when considering the importance of the timing for a generator unit commitment, as it relates to scheduling deliveries on the pipeline. Except for a force majeure situation or previously notified maintenance event, once scheduled by the pipeline, a generator using a firm primary path (primary receipt and delivery points) should not be subject to interruption throughout the five pipeline nomination cycles. Consequently, the following points apply to generators using secondary firm, non-traditional or interruptible transportation rights:

- If a generator, without primary firm rights through or to a constrained delivery point is dispatched too late in the gas day and scheduled volumes are at or near capacity (at the constrained point), the pipeline may not have sufficient excess capacity to meet all or part of the generator's nominated volumes.
- A generator, using firm transportation rights, may "bump" any interruptible shipper's scheduled volumes, until the intra-day 3 ("ID3") nomination cycle.
- If a generator's interruptible scheduled volume survives through the ID3 nomination cycle, it cannot be interrupted or otherwise lessened by a firm shipper's ID3 nomination.

The timing of the generator's unit commitment might affect its ability to obtain fuel. As a general rule, natural gas fuel procurement and associated scheduled, pipeline deliveries are best ensured with a timely dispatch signal/unit commitment. Regardless of how "firm" a generator's pipeline capacity contract may be, if committed after the day ahead Timely Cycle, natural gas supply availability, in the commodity market, should also be considered.

Furthermore, fuel delivery flexibility and constraints can vary by pipeline, season, planned or unplanned maintenance events, delivery location and peak demand events. The points, listed below, provide some guidance when considering the importance of the timing for a generator unit commitment, as it relates to scheduling deliveries on the pipeline. Except for a force majeure situation or previously notified maintenance event, once scheduled by the pipeline, a generator using a firm primary path (primary receipt and delivery points) should not be subject to interruption throughout the five pipeline nomination cycles. Consequently, the following points apply to generators using secondary firm, non-traditional or interruptible transportation rights.

- If a generator, without primary firm rights through or to a constrained delivery point is dispatched too late in the gas day and scheduled volumes are at or near capacity (at the constrained point), the pipeline may not have sufficient excess capacity to meet all or part of the generator's nominated volumes.
- A generator, using firm transportation rights, may "bump" any interruptible shipper's scheduled volumes, until the intra-day 3 ("ID3") nomination cycle.
- If a generator's interruptible scheduled volume survives through the ID3 nomination cycle, it cannot be interrupted or otherwise lessened by a firm shipper's ID3 nomination.

The natural gas industry does not have a history of susceptibility to failure or to wide-spread failure from a single point of disruption due to multiple factors including (i) the dispersion of production and storage,[22] (ii) access to multiple pipeline paths for most pipeline customers, and. That said, a temporary outage of (i) a single facility, single pipeline or a delivery point, (ii) loss of a percentage of gas supply due external factors – e.g., wellhead freeze offs, hurricanes, cyber security risk, etc. and (iii) loss of a large gas processing facility are credible scenarios to examine. When considering such a natural gas supply disruption within a given area, the examination would not just be limited to the loss of the natural gas supply but also the associated loss of electric generation and any ancillary needs, such as the loss of electric natural gas compression.

Planners should fully examine the credible reliability risks associated with the natural gas supplied to generators within the reliability footprint of the planner. Further, planners should view the system through an "all-hazards" lens and evaluate additional considerations, including weather, regional policies, and cyber-related risks. The following paragraphs outline the information that planners should seek to understand as a precursor to a more rigorous fuel assurance and reliability risk analysis.

To begin, planners should seek to understand the strategies employed regarding natural gas supply to each generator within their reliability footprint and any applicable regulatory requirements. This could include regular and emergency transportation/service agreements, call options, or other marketing arrangements being employed by the generator owners/operators to meet its resources capacity obligations. This examination could also include reviewing access to on-site fuel storage (e.g., fuel oil, propane, LNG, compressed natural gas), access to off-site storage,[23] access and availability of an alternate pipeline connection, and the availability of non-firm natural gas services and supply. Planners may also consider the alternative fuel capability of the generator, how any such alternatives are contracted and managed, and any environmental and regulatory requirements that may limit the use of the alternative fuel.

The PJM study "Fuel Security Analysis:[15] A PJM Resilience Initiative" investigated the two following natural gas "disruption" scenarios with different recovery expectations:

"Line Hit," such as an excavating crew accident	"Other," such as corrosion
This type of disruption is easily identified, isolated to a smaller area requiring repairs, and would only cause about a five-day disruption.	This could take longer as investigations are needed over a larger area and will likely be a more "sustained" type of outage.

Figure 3.1: Fuel Security Analysis

Planners should examine each generator and its potential physical access to supply (including access to pipeline, distribution, and storage facilities), the amount of capacity subscribed and available at each supply facility, and the ability of the facility to meet daily and seasonal demand swings. In addition, planners should review potential curtailments to key supply points on their respective transportation agreements (e.g., LDCs needing to redirect supply to "essential human needs" if a severe supply disruption occurs). These details are important in order to formulate.

supply alternatives to consider when examining a possible supply shortage or failure. While physically severing an interstate pipeline is very uncommon, it can occur in situations like third-party damage. Furthermore, a facility may need to be taken out of service for maintenance. Other considerations include specific pipeline resilience, geography, and potential state or federal restrictions on pipeline expansion, competition for supply with heating and industrial demands, and upstream demand that may impact the region.[25] Environmental permits, such as those that allow streambed alteration, may be required and will vary by repair required and specific location. Quick agreement on any environmental mitigation measures will speed obtaining those permits. As noted previously, the planner's role is to have specific knowledge of the fuel assurance of individual generators in order to be able to assess, over the planning area, whether any fuel assurance problems at a particular unit can impact the maintenance of reliability to the area as opposed to just impacting the deliverability of that particular unit. Planners need to recognize this distinction so as to avoid taking on management responsibilities that more appropriately lie with the individual unit owner.

In order to assess the forgoing, data can be obtained from certain public sources. FERC regulations and the business practice standards of the Wholesale Gas Quadrant of the North American Energy Standards Board applicable to natural gas pipelines, which are incorporated by reference into FERC regulations, include various posting requirements for regulated pipelines. These standards require the posting of information related to pipeline capacity, natural gas quality, operational notices, customer indices, tariff provisions, and other items. The U.S. Energy Information Administration also publishes detailed information on U.S. natural gas pipelines and underground storage.[26] FERC also requires that interstate pipelines and certain intrastate and Hinshaw[27] facilities file various forms and operational reports.[28] In addition to the forgoing, the various states also require LDCs to file certain information with the state commissions and/or publicly post certain information. The aforementioned information and data from the applicable generators should also be used to evaluate fuel risk.

Furthermore, as increasing penetration of wind and solar resources and battery energy storage occurs to meet state objectives and policies for emissions reductions, natural gas will become the swing fuel. Natural gas will be in high demand, not only during periods of extreme cold and hot weather, but also during periods of low solar and wind output or even when needed for battery energy storage when solar and wind energy is depressed. At other times, when solar and wind energy is in excess and battery energy storage is insufficient to absorb this excess, natural gas generators and thus natural gas usage will significantly decline to accommodate the solar and wind energy and avoid curtailments of clean energy.

---

[15] https://www.pjm.com/-/media/library/reports-notices/fuel-security/2018-fuel-security-analysis.ashx?la=en

Oil

The main risks associated with fuel oil are:

- Severe cold weather events of unusually long duration;
- Multiple, severe cold weather events that occur before sufficient replenishment has occurred; and
- Deeper and more-protracted reliance on oil due to the failure of other resource types.
- Air permitting for hours of utilization of fuel oil can be restrictive
- Some combustion turbines require demineralized water injection for NOx emissions control and replenishment rates for demineralized water can create a restriction on generator availability

These risks may be quantified through modelling of the following variables, initial conditions, and constraints:

- Initial inventories may be quantified through fuel surveys, historical tankage levels, and adjustments due to commodity prices, especially relative to the predominant marginal fuel;
- Burn rates may be determined from equipment technical specifications, field unit parameters, and survey responses from the generators;
- Emissions limitations may be determined from a review of each facility’s Title V Operating Permit and recent operating profile;
- Replenishment rates may be more difficult to model; however, the maximum replenishment rate is limited by the offload capability at the facility. However, if severe weather persists, trucks and barges may not be able to replenish on-site inventories at these maximal rates and may need to be adjusted downward. These limitations could be due to physical transportation conditions or could be due to competition with heating oil deliveries.

Regardless, the main risks are needs outpacing replenishment plus on site storage over varying time horizons, and facilities reaching emissions limitations for the remainder of the heating season.

Coal

Coal supply risks are associated with supply limitations and the transportation of coal from the mine to the power plant. Future coal generation and, therefore, coal supply risks will be influenced by environmental rules, market rules, NERC guidelines, and the deployment of carbon capture technology. With respect to coal transportation, approximately 70% of coal to US power plants is delivered by rail, and the rail network is comprised of an extensive grid of intersecting and interconnected tracks that offer multiple pathways for rerouting deliveries in the event of a physical disruption, but temporary slow-downs or disruptions to supply can occur in the rail system due to weather (e.g., floods or snow), derailments, or track repairs. Similar to other fuel types, longer-term disruptions can occur during unanticipated long-term events such as the pandemic, that cause labor shortages resulting in limited rail and trucking capacity. Barge transport can be temporarily impaired by icy, low-level, or flooded conditions on river systems. Generators rely on their on-site coal supply for operation until deliveries can be restored. However, conditions like frozen or wet coal could impact on-site coal supply. Coal commodity and rail transportation contracts may contain ratability language that states shipments must be taken consistently. This ratability causes a natural rise and fall of the on-site stockpile based on periods of high and low demand. Any supply disruptions during the periods of high demand may exacerbate low inventories. Additionally, coal plants are typically optimized to run using only one of the four types of coal, potentially limiting generation capability if that coal becomes unavailable due to long-term supply or transportation disruptions.

Nuclear

As described in Chapter 2 nuclear facilities store fuel on-site in a highly controlled and secure environment. There are many layers of safety at nuclear sites to protect from physical and cyber risks.

Hydro

All hydroelectric projects are dependent on upstream sources for fuel supply water. Those sources can be snowpack, other hydro projects, free flowing rivers, lakes, streams, or a combination. Ultimately, the source is a function of precipitation. History has shown quite a diversity in the volume of water available for hydropower generation. The total volume can run between 50–150% of the expected average. In some areas, much of the precipitation falls in the form of snow and becomes useable water during the spring thaw. The rate of the melt or “run-off” is almost as important as the volume. Slow melts are best as fast melts can lead to spilling water past fully loaded turbines or loss of water as a fuel due to lack of storage. Deeply cold winters can also result in frozen rivers and streams, cutting off fuel to downstream projects during times of elevated power demand. Temperature and precipitation are critical factors in the availability of water for hydropower production.

Variable Energy Resources, Energy Storage, and Developing Technologies

Where many of the risks associated with fuels described in the prior sections can be empirically measured in definite terms, the risks associated with wind and solar are more probabilistic and often subject to non-human controllable variation. The primary risk is uncertainty in meteorological conditions, such as wind speed and cloud cover, and can vary widely by region and locality within a planning footprint. These risks also vary through time. For instance, a wind farm may be able to sustain operations through a cold weather event of short duration during which blade icing occurs but does not reach a threshold which requires turbine shutdown, while the same farm may reach the shutdown threshold during a longer duration event. Awareness of turbine limitations for wind speed should also be included. Output is decreased not only for low wind conditions, but turbines have cut-out protection that immediately cease output during high wind conditions to protect the turbines from damage. The same occurs for solar generation at high temperatures where output decreases as a function of ambient temperature and enclosed panels are subject to the same radiative heating effects as an automobile which raise the temperature seen by the panel. Since sunlight irradiance can be limited by conditions other than natural weather, the operator should also be aware of other airborne events such as fire, smoke, dust and atmospheric conditions limiting solar radiation. Another aspect to consider for solar resources is the effect of cosmic events such as solar eclipse. Solar panels are also designed with specific solar emissivity settings set in the PV module. Although these settings are technology related and have little variance, planners and operators should be aware of how sunlight irradiance may have different effects on different solar resources as well as how solar panel cleaning intervals may impact output. Weather related uncertainty risks may be quantified through probabilistic modelling using historical weather data to determine a distribution of production levels. Since most distributed energy and behind the meter resources are wind or solar driven, planners should attempt to collect a reasonable amount of information on the location and type of these resources and include them in the probabilistic modelling. In order to bound the potential risk outcomes from the uncertainties impacting wind and solar resources, studies should examine scenarios that include a range of geographical and production variabilities, i.e., different weather scenarios overlaid on the region. There are software and services that provide wind and sunlight irradiance forecasts that can aid planners in assessing risk. It is also worth mentioning that probabilistic planning outcomes can be improved with greater amounts of actual performance data. As more performance data is collected over time for wind and solar resources, models should be updated to improve the accuracy of studies.

Chapter 4: Fuel-Related Reliability Risk Analysis Framework

The BES, for the most part, is similar enough from area to area that a specified baseline set of criteria can be defined and followed, resulting in similar and comparable results from transmission planning studies. TPL-001 defines and prescribes these planning studies very well; criteria have been developed over many years, resulting in multiple revisions to the standard. Even though TPL-001 references a fuel contingency analysis in Table 1 Steady State & Stability Performance Extreme Events as a possible study contingency, the (default) contingency results in the loss of only two generating stations and may not represent a significant pipeline segment, compressor station, storage facility, barge transport, or other fuel supply disruption for many systems. This chapter provides details regarding the scope of fuel-related generator outages beyond the minimum requirements for TPL-001 transmission system planning assessments.

The framework presented below does not identify a single methodology but rather outlines an approach to assist planners in determining what factors may be considered to conduct a meaningful fuel-related reliability risk analysis for the BPS. The actions described are intended to be flexible enough to account for all fuel types, broad enough to support the unique circumstances in each region, and executable out of order (or in some cases not at all). This framework does not provide specific solutions or next steps that could be taken after assessing the results of any particular study.

The methodology described in this section may be applied narrowly or across a broad range of credible assumptions as determined by the planner performing the study. The selected assumptions should ensure that the study is both relevant and meaningful. It may be prudent to subject the BPS system under study to a range of high-probability, low-impact (HPLI) contingencies as well as some high-impact, low-probability (HILP) contingencies. Studying HPLI contingencies may shed light on operational needs during such instances and inform changes to processes and procedures to preserve reliability (e.g., improvements in the ability of generators to schedule or contract for natural gas). Even if they are not the primary motivation for the analysis, studying HILP contingencies that stress test the system will bookend the study set and may inform regulators or other interested parties of the reliability impact of such extreme conditions and may inform emergency preparedness efforts. Examples of HILP scenarios include severe reduction of non-firm natural gas supply, prolonged pipeline repair, extreme prolonged weather events that affect both supply of and demand for natural gas, or unanticipated low production from variable energy resources (VERs) such as solar and wind.

Based on the unique risks in different regions, the fuel-related reliability risk analysis outlined in this chapter (although not required) is recommended as a best-practice approach for supporting existing studies (e.g., TPL-001 extreme events analysis) or for conducting a stand-alone analysis. In either case, documentation of each step of the process is critical. Documenting the rationale behind the methodology and assumptions will better inform those reviewing the study both presently and in the future and may also inform subsequent studies.

Step 1: Problem Statement and Study Prerequisites

To perform a valid fuel-related reliability risk analysis, there are numerous considerations that should be taken into account that will help shape the direction and results of the analysis. Prior to beginning any analysis, the planner must determine the purpose or goal of the study and, just as importantly, what the study will not do. It is at this point that the criteria, concerns, scenarios and required data will become more evident. Determining which elements of fuel supply risk are to be examined in a single study can be challenging as different combinations of risks can lead to an unmanageable number of model runs.

Consider the following to help define the study:

- Have a clearly defined goal for the study. Set the criteria of the study and define the criteria for system performance. A study that crosses the threshold of meeting certain criteria will do so when fuel is in short supply, generators are no longer able to run, or there is a supply/demand imbalance. The imbalance can be system-wide or, equally as important, a local area imbalance that results in the potential exceedance of a NERC Reliability Standard defined System Operating Limit (SOL) or Interconnection Reliability Operating Limit (IROL) of the BPS. This philosophy can help determine contingencies that may not be obviously catastrophic, but still highlight issues that may need mitigation.

- Communicate the goals of the study with stakeholders and gain agreement on principal concepts.
- Decide the analysis timeline prior to commencing work. If the problem definition and the solution are going to be two separate phases of a study, set that expectation early in the process. Often, the deriving solution means following the directives of governing entities (NERC, FERC, governmental agencies, state public utility commissions, etc.). If this is the case, that is the goal of the study.
- Clearly state the boundaries of the study. If there are certain aspects that will not be addressed by the study, make that distinction clear as early in the process as possible.

Step 2: Data Gathering

Data is essential for a valid fuel-related reliability risk analysis. While the planners performing the study are very familiar with the transmission system and the inputs needed to perform traditional studies, there are many considerations outside the normal inputs that are needed for this analysis. Much of the data needed is likely not directly accessible to the planner and will therefore require the assistance of others in their company (e.g., operations personnel) or even fuel suppliers themselves. FERC has through its Order 787 authorized the sharing of confidential information between jurisdictional pipelines and system operators in order to ensure reliability. Planners should consider using that authority to obtain needed information from the pipelines on a cooperative basis. The following is a list of data sources and methods for acquiring data that can be used by planners to collect the information that they need to perform the study outlined in **Step 1**:

- Coordinate fuel assurance assumptions with generator owners/operators:
    - This may be achieved with surveys that may include, but are not limited to, primary fuel availability, details of fuel supply and transport agreements, usable on-site storage capability, historic inventory levels, resupply and back- up fuel availability and strategy, resource limitations on alternate fuels (MW output, switching time and process details, changes in heat rate), emissions concerns, and staffing concerns.
        - It may be helpful to discuss the formation of such a survey with generator owners/operators and other stakeholders to seek their guidance and expertise on the level of data they may be able and willing to provide.
    - Validate/benchmark that the data received is consistent with the recent operational experiences when possible

Table 4.1: Suggestions to Establish and Maintain a Suitable Fuel Survey

Consider managing a survey of this type through an established stakeholder forum
• This will ensure that any changes to the survey are subject to stakeholder discussion and therefore more thoroughly vetted • Ensure that the information is reaching the target audience as there can be a disconnect between generator owners/operators and the stakeholder representatives
Consider hosting additional engagements like a winter generator readiness seminar
• This offers the opportunity to discuss with a more targeted audience of generator owners/operators and not just their representatives
Consider conducting fuel-constrained scenarios as part of your regular training cycle
• This offers an opportunity to solicit concerns and gather potential impacts of limited fuel supply on system operations across a wide spectrum of electric and cross-sector stakeholders • This exercise also has the potential to identify fuel disruption impacts that can be further addressed directly with fuel suppliers to seek actions to mitigate these impacts

- Gather appropriate fuel supply contingencies (to be further analyzed and filtered in Step 4):
  - Coordinate with fuel suppliers or fuel specialists within your company, member companies, and/or collaborate with the experts who own and operate the fuel supply chains, including (but not limited to) natural gas and fuel oil pipelines, fuel producers, fuel oil refineries, storage and trucking companies, rail carriers, and ocean or river bound tanker ships/barges. Their input will aid in the assessment of the potential for disruption or failure. It will also lend credence to the assumptions.
  - Take steps to fully understand what information is already posted on a gas pipeline's EBB and how that information can readily be used for greater situational awareness. Ask for educational sessions when necessary to understand how to interpret posted information in a way that provides the most value. .
  - Discuss the fuel supplier's response plans if fuel supply disruptions were to happen. Rather than rely solely on a hands-off type of study (which still has value), consider the possible mitigating actions of the fuel supplier after the disruptions occur in order to incorporate the impact to the BPS into your analysis. Also consider the time considerations between the disruption and when it will impact the power system. Not all failures have immediate impact.
    - Outreach may include a review of disruption scenarios with each of the fuel suppliers operating within the studied region to assess the viability of both the assumed disruption scenarios as well as the potential downstream impacts.[16]

Step 3: Formulate Study Input Assumptions and Initial System Conditions

Assumptions and system conditions may be developed by using information obtained from data gathering efforts outlined in Step 2 as well as regional historical experience to establish relevant scenarios for incorporation into the analysis. These assumptions may be specific (e.g., specific generator outage rates determined from regional historical averages) or expressed in terms of a range (e.g., low, medium, and high ranges of projected generator retirements

---

[16] As an example, ask the pipeline companies what remaining capacity would be available if they lost a particular pipeline segment. Depending on the pipeline configuration, the capacity serving the area's generators may be reduced by 10%, 50%, or not impacted at all. Each case would produce different input assumptions for the study.
Consider review of internal operational policies and procedures with the pipelines to better understand the impact of those procedures during a fuel supply disruption scenario.

affecting future fuel mix). Steps to develop these assumptions and conditions for the analysis include (but are not limited to) the following:

- Determine which fuel(s) to study. When doing so, consider the interdependence of various fuel types and how a large disruption to one fuel source may impact another fuel source.
- Develop fuel assumptions using the best available information:
  - Document fuel supply assumptions for plants where data is not available or up to date to maintain visibility of areas where the study may have weaknesses.
  - Consider fuel supply alternatives, such as dual fuel use and service from alternate pipelines.
- Determine weather and load assumptions:
  - Weather input to the study can be historical normal and extreme weather applied to future scenarios or some version of a weather or climate forecast that describes the study time frame.
  - For a fuel risk analysis, the system under study is more
  - than just the BPS. There are going to be shared resources between different sub-systems that are interdependent; for example, natural gas is used for both heating and power generation. Understanding the relationship between those two classes of natural gas demand is paramount when performing this study. Knowing what will happen when the natural gas system is full due to colder temperatures will define what direction the study goes and, in large-part, the results of the study. Fuel oil works in a similar fashion but with a different
  - mode of transportation. Although pipelines can carry fuel oil, it is typically via truck or barge. But the fundamental concept is the same—when it gets cold and the demand for fuel is up, supply chains become full and resulting supply options and priorities may be unexpected.
- Determine interchange assumptions and interface capability:
  - This should include coordination with neighboring entities to ensure accuracy and agreement of their interchange contribution. Consider whether the conditions selected for the study will also impact an adjacent area's interchange contribution.
  - A study may assume interchange transaction quantities that reflect the economic
  - interaction between the studied systems and neighboring systems consistent with real-time operations. Alternatively, a historical analysis may be performed to determine an upper and lower bound for capacity and energy imports and exports.
  - Coordination with neighboring systems should also include potential impacts of a natural gas disruption in one area on gas-fired generation in adjacent areas—affecting the amount of electric interchange support available.
- Determine generator outage rates and reductions assumptions:
  - Generator outage rates may be defined by using standard methods (e.g., EFORd) or using a simple analysis of historical performance. Depending on the approach or assumptions, this may deviate from the normally accepted methods.
- Take care not to double count outages. Understand that if a generator is out of service due to normal outages, it cannot also be counted as a generator that is out of service due to fuel and vice-versa.[17]
- Determine assumptions related to VERs:

---

[17] During 2022, wind generation output ranged from 0.55 GW to 24.3 GW in MISO

    - These considerations will be critical in areas with high penetration of VERs where the output range can vary significantly.[18]
- Consider the evolution of generation technology, changes in fuel mix, and the interdependency of future resource installation:
    - The current interconnection queue and integrated resource plans/resource adequacy plans may inform planners of resources to be selected in longer-term analyses.
    - Resource planning forecasts are performed on a regular basis. These studies evaluate the future needs and technologies to meet those needs:
        - These studies may reveal, for example, the likelihood of renewable energy variable energy resource additions and battery energy storage that result in early retirement of coal or fuel oil resources.
        - State emissions reduction objectives and policies could result in significant changes to the resource mix over a short period of time placing additional and changing demands on certain fuels such as natural gas for additional dual-fuel resources, as another example, would likely introduce more gas/fuel oil generators into the interconnection queue.
    - It may be difficult to predict how the future resource mix will vary based on factors like governmental policy initiatives. Include a range of assumptions for items that have uncertainty.[19]

ISO-NE OPERATIONAL FUEL SECURITY ANALYSIS[20]

ISO New England's Operational Fuel Security Analysis modeled a wide range of resource combinations that might be possible several years into the future. The study examined varying resource retirements, LNG availability, oil inventory, interchange, and renewable resources. In addition to a reference case which incorporated the likely levels of each variable, these input assumptions were varied individually to characterize the sensitivity between unfavorable to favorable boundary cases. Several combination scenarios, examining how multiple related changes would affect the outcome, were also examined which adjusted more than one of the key variables to represent future resource portfolios that could develop and their effects on fuel security.

Figure 4.1: ISO-NE Operational Fuel Security Analysis

- Determine performance criteria. for example:
    - If the study being performed contemplates a HILP contingency, perhaps the performance criteria would be that 90% of firm load is maintained for a short period of time. However, when HILP is studied, it should be done for emergency preparedness and not for measuring the reliability of specific system resources. Another consideration in this scenario would be acceptable system ratings and limits. If the study being performed contemplates a HPLI contingency, perhaps the performance criteria would be set to a base case, or up to unavailability of interruptible load.
- Determine the study frequency, outlook, and duration according to the risks identified through data gathering. Depending on the assumptions, electric system, or fuel supply chains that may have changed, the planner should use engineering judgement and historical information. See the three-column graphic on the next page for additional information.
- Determine performance criteria. For example:
    - If the study being performed contemplates a HILP contingency, perhaps the performance criteria would be that 90% of firm load is maintained for a short period of time. However, when HILP is studied, it should

---

[18] *During 2022, wind generation output ranged from 0.55 GW to 24.3 GW in MISO*

[19] https://www.iso-ne.com/static-assets/documents/2018/01/20180117_operational_fuel-security_analysis.pdf

[20] Id.

be done for emergency preparedness and not for measuring the reliability of specific system resources. Another consideration in this scenario would be acceptable system ratings and limits. If the study being performed contemplates a HPLI contingency, perhaps the performance criteria would be set to a base case, or up to unavailability of interruptible load.

- Determine the study frequency, outlook, and duration according to the risks identified through data gathering. Depending on the assumptions, electric system, or fuel supply chains that may have changed, the planner should use engineering judgement and historical information. See the three-column graphic on the next page for additional information.

Table 4.2:Choosing a Study

Frequency	Outlook	Duration
For choosing a study frequency (i.e., how often the study is performed), consider the following: • Operational time frame studies could be performed on a weekly, or monthly basis, or other near- term periodicity. For example, one existing analysis involves a winter weekly or non-winter biweekly energy study that is used on an ongoing basis for operations planning. • Seasonal studies could be performed periodically in the prewinter or presummer time frames in anticipation of the peak load seasons. • Longer-term studies could be performed annually, every few years, or on a longer-term periodicity as necessary. • Ad-hoc (one-time) studies could also be performed to assess a unique set of conditions and to achieve specific objectives, and may be more limited in scope.	For choosing a study outlook (i.e., when does the studied time horizon begin) consider the following: • Short-term operations planning study outlooks (e.g., one-week out, one-month out, six-months out, other- less than a year out) could be used. • Alternatively, near-term (1–5 years), long-term (6–10 years) transmission planning time horizons, or even greater study outlooks could be used if appropriate for the objectives of the study. For example, one existing analysis was based on a five-year look-ahead study to assess system resilience under future resource portfolios.	For choosing a study duration (i.e., what is length of the study window), consider the following: • The duration could be anywhere from a snapshot of the current system to a few days out or even to multiple years, depending on what is appropriate for the assumptions or objectives of the study. For example, one existing analysis involves a 14-day study window to model a plausible 14- day extreme cold weather scenario based on historical weather analysis. • Consider varying durations of fuel disruptions to determine how reliability conditions may change over time given a particular fuel disruption.[21]

---

[21] ISO-NE performs a 21-day look ahead energy assessment based on the lead time it takes to schedule an LNG and fuel oil truck delivery within the associated region.

- Include any special or additional scenarios or assumptions, such as the following:
    - Heavy seasonal directional power transfers
    - Changes in resource mix/generation mix
    - Low variable energy resource production for a multi-day period
    - Drought or flooding conditions
    - Changes in fuel supply situation (e.g., closure of refineries or LNG storage facilities, new provisions that limit or prevent local gas and fuel oil transport)
    - System-wide blackout scenario (e.g., scenario studying fuel-related reliability risks to blackstart units and potential impact on system restoration following a blackout)
- Document the rationale behind study assumptions and initial system conditions

Step 4: Contingency Selection

The data gathered at this point will help to form the basis for contingencies to the fuel supply of the studied system. Some aspects will be known, and some will be assumed. It is possible that not all contingencies will be included in the final study once the probability and credibility of the various scenarios are better established. It may be prudent to establish a priority level for different contingencies based on the planner's experiences. There are many factors to consider in filtering and selecting the appropriate contingencies to study; this may include, but is not limited to, the following:

- The cause of the fuel disruption (which helps with developing proper mitigation)[22]
- The frequency with which the disruption has occurred in the past in this or other locations
- The probability or likelihood that the disruption will occur in the future
- The expected duration of the disruption based on historical data or reasonable assumptions that acknowledge system improvements over historical data:
    - Fuel disruption duration can be seasonally dependent. For example, a failed fuel delivery system during the high-demand winter months will likely be shorter in duration than a disruption during low-demand periods.
- The amount of fuel supply interrupted (This is a line to be drawn based on relevance to the scenario being studied.)[23]
- The amount of fuel supply interrupted (This is a line to be drawn based on relevance to the scenario being studied.)[24]
- The location of the disruption, even outside of your footprint as fuel delivery is a worldwide operation
    - Interdependence of global markets on local systems should not be overlooked (e.g., LNG imports to Europe surged following the Russian invasion of Ukraine in 2022 .))
- The generating units that may be affected by the disruption (Be sure to account for remaining generating capability if any.)

---

[22] NERC Generator Availability Data System data collection was updated for 2020 reporting and going forward cause coding for "lack of fuel" reporting will be much improved.

[23] The loss of a single natural gas compressor engine at a station is more likely than the loss of an entire compressor station. Many fuel supply systems contain redundancies and safeguards, making a full outage of service less likely than a partial outage.

[24] The loss of a single natural gas compressor engine at a station is more likely than the loss of an entire compressor station. Many fuel supply systems contain redundancies and safeguards, making a full outage of service less likely than a partial outage.

    - Consider alternatives available to impacted generating units, such as dual fuel use and service from alternate pipelines[25]
- The extent or scope of the interruption as to whether it impacts other companies, industries, or other subsystems, such as the following:
    - If flooding has washed out the railways in a particular area, rerouting coal delivery around that area will likely be more difficult due to all rail traffic trying to reroute to meet guaranteed delivery dates.
    - Consider the likelihood of mutual assistance between suppliers. It is within the realm of possibility that a pipeline or fuel oil transporter could suffer a loss of capability and receive assistance from an interconnected pipeline or associated supplier.
    - Consider whether electric load shedding to resolve BPS problems will impact fuel availability or subsequent plant operations.
    - Consider the impact of electric contingencies on the natural gas system or recovery from a natural gas disruption (e.g., loss of power to electric driven natural gas compressor stations or transmission contingencies that may restrict the redispatch of non-natural-gas-fired generators).
- The influence of governmental agencies may also factor into the studied response to contingencies:
    - Consider historical reactions by governing agencies.
    - Consider guidance from governmental agencies, such as the potential for cyber and/or man-made threats to fuel delivery systems.

PJM FUEL SECURITY ANALYSIS

- Consider working with relevant governmental agencies to share the analysis, develop and gain any needed approval for mitigation measures.
    - Nontraditional solutions may be available when directed by emergency management or similar agencies. Conversely, fuel supply could be made unavailable due to decisions made at the governmental level. For example, a port necessary for the delivery of LNG or fuel oil may be shut down following worldwide events that result in a state of heightened security. Another example may be the limited usage of fuel oil unless a special (environmental) waiver is granted by state or federal officials.[26]
- Document the rationale for each contingency selected.

Step 5: Selection of Tool(s) for Analysis

Because of individual system conditions and goals, no single type of transmission system analysis will meet the need of every planner. Therefore, each planner should consider the information gathered in the steps above and choose analysis tools that can provide information that will allow for a thorough assessment of their supply and transmission systems. This analysis may be power flow, stability or dynamic simulation, production cost modeling, market simulation, fuel oil and natural gas pipeline hydraulic flow modeling, deterministic versus probabilistic modeling, in-house tools, or any combination of these tools and others.

---

[25] Eastern Interconnection Planning Collaborative (EIPC), 2015 Gas-Electric System Interface Study, Section 10 on Natural Gas and Electric System Contingency Analysis, https://eipconline.com/phase-ii-documents.

[26] Following a pipeline disruption event impacting one of the looped lines in a pipeline segment, PHMSA has historically required a mandatory capacity reduction (typically about 20% firm capacity reduction) in the adjacent non-impacted lines within the same pipeline right-of-way until initial investigation of the incident is complete. PHMSA has also historically restricted access to an affected pipeline segment following an event for safety reasons, delaying immediate restoration efforts by pipeline operators. Both the capacity reduction and delayed restoration due to PHMSA's response should be considered when studying the natural gas pipeline contingency impact and duration.

Regardless of the tool(s) chosen, the rationale for the selection should be documented and reviewed periodically to ensure that the appropriate tools continue to be utilized and provide continuity from the end of the analysis to what was defined in the goals.

Step 6: Perform Analysis and Assess Results

Based on the information from Steps 1–5, system analysis will be performed and assessed. The assessment will evaluate system performance based on the criteria defined in Step 3 to determine if system deficiencies exist and, if so, what actions might be considered to improve the observed deficiencies. Every step of the process was defined, including the criteria for system performance. At this point of the analysis, the state of the system is known. If the assessment determines that the system does not meet the prescribed criteria for reliable operation of the power system, and corrective actions are needed, this step is where that would happen.

When delivering the results of the study, consider the audience. Consider their level of knowledge of the system being studied and speak to the audience at a level they will understand. Use commonly understood terminology, processes, and procedures so that the audience will more likely comprehend the results as intended.

Step 7: Develop Solution Framework

As noted in Step 3, fuel assurance studies should be completed on an ongoing basis. Regular analysis will help planners and other stakeholders better understand emerging risks as the power grid undergoes rapid transformation. Planners are encouraged to develop a solution framework to ensure fuel assurance in advance of any potential credible reliability issues. It is at this point that the planner should consider engaging governmental agencies that may be able to assist with developing a framework of potential solutions. One example might be contacting state environmental departments to discuss power plant air and water permits should a HILP contingency occur. At a larger regional level, planners are encouraged to consider developing a response and mitigation plan for grid, generator, and natural gas operators to guide their response to fuel assurance contingencies as identified in Step 4. Further, the development of a communications protocol for grid, generator, and natural gas operators could benefit the regional response to and mitigation of contingencies as identified in the risk analysis framework. These proactive actions will ensure preparedness and improved situational awareness to handle these potential risks in the future.

Appendix A: Factors to Consider

Does the transportation contract provide firm no notice service supported by natural gas storage, which mitigates nomination and scheduling concerns as well as commodity supply risk due to storage-based supply. With no notice service, the pipeline commits it will have capacity to serve the no notice shipper throughout the Gas Day. An arrangement including these attributes generally would be more reliable than one without these capabilities, particularly during peak demand periods and/or when the generator is dispatched intra-day.

Does the delivery of the natural gas supply include some form of firm park-and-loan service allowing the generator to have an imbalance between the amount of gas received into its transportation contract and the amount of natural gas consumed at the generator without risk of service interruption or severe imbalance or overrun penalties. Such service could mitigate the gas supply risk by allowing the generator to take firm delivery of a volume of gas not solely tied to the amount of natural gas scheduled during the normal pipeline nomination cycles.

Does the pipeline transportation agreement include the firm right to take delivery of the natural gas supply on an hourly basis consistent with the expected burn profile of the generator? In some cases, pipeline delivery contracts and/or tariffs limit hourly deliveries to 1/24th, 1/20th, or 1/16th of the daily delivery volume. Generally, firm hourly delivery entitlement that meet the generator’s needed hourly burn profile will be more reliable than those which need to operate at hourly take levels beyond the firm hourly entitlement.

Does the pipeline offer additional nomination cycles beyond those established by the NAESB standardized timeline, and if so, have those nomination cycles been effective resolving or limiting imbalance positions on the pipeline?
Does the generator have transportation rights to support its full generation output? If the generator has firm entitlement rights only for a portion of its output [either hourly or daily], this may indicate that incremental capacity is unavailable and gas deliveries may be limited under certain conditions.

Appendix B: Design Basis for a Natural Gas Study Whitepaper

Introduction

The purpose of this document is to guide the performance studies of the interface between the electric and natural gas systems. The recommendations below are not intended to require any analyses to be performed, nor are they intended to provide market solutions, but rather to improve upon the methods and approach in performing that analysis. A realistic set or range of initial conditions should be reviewed/considered when performing this reliability analysis.

What is a Design-Basis Gas Event?

A design-basis gas event is an event used to establish acceptable performance requirements of the reliable operation of the Bulk Power System (BPS) processes, structures, systems, and components, following a disruption of the natural gas fuel delivery system (i.e. pipeline or distribution network).

Examining an Event

When considering such a natural gas disruption within a given area, the examination is not just limited to the loss of the natural gas transportation. Rather, it includes any loss of electric generation with associated energy and essential reliability services, and any ancillary natural gas delivery system needs, such as the loss of electric compression on the natural gas system, the loss of processing plants, and the unavailability of production. The examination should also take into account the level of flexibility available on natural gas pipelines, according to the individual pipeline tariffs, and the impact that wholesale electric markets may have on the procurement of sufficient natural gas supply.

Assessment

Evaluation[27] should include the credible reliability risks (including durations) associated with the natural gas supplied to generators within the reliability footprint of the Registered Entity (RE) performing the evaluation, and its neighbors, which could have an impact on the reliable operation of the BPS of the RE. Further, the system should be viewed through an "all-hazards" lens, to include additional considerations, such as weather impacts, supply chain logistics, regional policies, wholesale electric market design, and security risks (cyber and physical). Evaluation should also include examination of each generator/plant as well as groups of generators/plants that are on the same gas transportation system. Assessments should include dependence on electric supply, potential physical access to natural gas supply (including access to pipeline, distribution, and storage facilities), the amount of capacity subscribed and available at each natural gas supply[28] facility, the amount of flexibility from daily nominations allowed, impacts of extreme weather events, and the ability of the natural gas facilities to meet daily and seasonal demand swings. As part of this assessment, considerations should be made for potential service restrictions and curtailments to key supply points based on the applicable transportation agreements and regulations (e.g., what level of service priority does a generation facility have pursuant to its transportation agreements, scheduling protocols, federal and state tariffs, and applicable regulations, particularly when severe weather or supply disruptions occur). The evaluation of the impact of curtailments of fuel supply should include the ability of dual fuel generators/plants to continue operation, and the associated limitations (e.g. switching time and limited maximum output), on alternate fuel from stored fuel or from multiple natural gas pipeline connections.

---

[27] Evaluation could be in any timeframe, Long Term Planning, Operations Planning, or Operations

[28] Supply facilities at any point in the natural gas supply chain

These key areas of evaluation would result in a confidence level of fuel assurance for all generators in a given planning area and

would highlight any potential system reliability risks given a gas supply disruption that impacts a significant amount of critical generation resources.

Additional information is available in the NERC Reliability Guideline: Gas and Electrical Operational Coordination Considerations[29]

---

[29] https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Gas_Electric_Guideline.pdf

Appendix C: Risk Analysis Framework Checklist

This checklist outlines the actions recommended in **Chapter 4** into a list that entities may use as a reference when performing their own analysis. As mentioned at the beginning of **Chapter 4**, the listed steps are intended to be flexible enough to account for all fuel types, broad enough to support the unique circumstances in each region, and may be performed out of order (or in some cases not at all).

Step 1: Problem Statement and Study Prerequisites

- Define the study goal (i.e., problem statement)
- Set the criteria for system performance
- Communicate the goals of the study with all stakeholders (electric and fuel suppliers)
- Gain agreement on principal concepts
- Determine the timeline prior to commencing work
- Set the boundaries of the study
- Document agreed upon goals, time line, boundaries, etc.

Step 2: Data Gathering

- Coordinate fuel assurance assumptions with generator owners/operators
- Survey stakeholders (see **Appendix B**)
- Identify relevant fuel supply contingency events
- Maintain documentation for future use

Step 3: Formulate Study Input Assumptions and Initial System Conditions

- Determine fuel(s) to be studied
- Determine the interdependence of various fuel types
- Determine how a large disruption to one fuel source may impact another fuel
- If needed, develop fuel assumptions in the absence of actual information
- Determine weather and load assumptions
- Determine interchange and interface capability
- Determine generator outage and reductions rate assumptions (e.g., EFORd)
- Determine assumptions related to variable energy resources
- Determine expected changes in regulatory policy, generation technology, and fuel mix, including the interdependency of resource installation
- Determine performance criteria using stakeholder input (e.g., is load loss acceptable? If so, for how long?)
- Determine study frequency, outlook, and duration
- Include any special or additional assumptions or system conditions, the following are examples:
  - Heavy seasonal energy transfers

    - Changes in generation mix
    - Droughts
    - Flooding
    - System-wide blackout scenario
- Document rationale for assumptions and system conditions selected

Step 4: Contingency Selection

Filter down identified contingencies. Consider CEII ramifications. Consider factors like the following:

- Cause of the fuel disruption
- Frequency with which the disruption has occurred in the past in this or other locations
- Probability or likelihood that the disruption will occur in the future
- Expected duration of the disruption based on historical data or reasonable assumptions
- Amount of the fuel supply interrupted
- Location of the disruption
- Generating units affected by the disruption and remaining generating capability (if any)
- Extent or scope of the interruption (does it impact other companies, industries, etc.)
- Influence of governmental agencies on the response to contingencies
- Document rationale for contingency selection

Step 5: Selection of Tool(s) for Analysis

Select analysis tools appropriate for the study, such as follows:

- Power flow
- Stability simulation
- Production cost modeling
- Market simulation
- Pipeline hydraulic flow modeling
- Deterministic vs. Probabilistic modeling
- In-house tools
- Document rationale for selection

Step 6: Perform Analysis and Assess Results

- Perform analysis
- Document and assess results
- Consider CEII ramifications

Step 7: Develop Solution Framework

- Identify potential risks
- Develop solution framework as needed and in concert with stakeholders, regulators, etc.
- Update existing plans and procedures

Appendix D: Items to Include in a Fuel/Energy Survey

This list is indicative but not all encompassing of the questions that planners may ask of its generator owners/operators depending on the regional study goals and the possibility of regional fuel type generation considerations.

When drafting a survey, consider whether certain questions should be made mandatory. Also consider how to format answer selections; should some be limited to multiple choice, is free form text more appropriate, etc. It will also be important to seek consistency in units of measurement. Make an effort to clarify what units are desired (MW, MWh, MMBtu/day, etc.) so that compiling and analyzing responses is straightforward.

General Information

- Resource information
    - Name
    - Contact
    - Unit identifier
    - Type
- Square footage of fence footprint and what percentage of that space is empty
- Is there a “bump-up” compressor on-site? How often is it used?
- Net max and min sustainable rating
- Design and/or current operational max/min ambient temperature
- Unit maximum Summer heat rate
- Unit maximum Winter heat rate
- Dual Fuel Unit heat rate on different fuels
- Primary fuel source
- Alternate fuel source
    - Fuel switching requirements, or other considerations
- Date of last MW disruption (or not received) on primary fuel (within the last 5 years)
- Amount of MWs disrupted (or not received)
    - Reason for disruption (or not received)
- Have any fuel supply procurement processes been compromised?
    - For example, limited trucking capability, navigation issues, lack of refinement capability from supplier
    - How often?
    - Any seasonal issues?
- Planned retirement date
- Is staffing required to start the unit?
- Is staffing required to switch fuels?

- Is unit black-start capable or on ISO/RTO system restoration Plan?
- Consumable item most limiting unit operations (e.g., limestone, chemicals, demineralized water trailers, air or water emission credits)
- Does the unit/station have existing on-site natural gas compression
- Availability of on-site boost compression
- Is there backup power on-site?
- Are there state restrictions on future use of this unit?
- What is the impact and duration of maintenance shutdowns?
- What is the risk of third-party damage to plant, inventory or transportation types to the plant?

Natural Gas Pipeline Information

- Companies providing physical natural gas pipeline connections
- Critical compressor facilities
    - Identify whether natural gas or electric compressors connected to or required by the unit (if known)
    - Identify if spare compression is available at each compressor site
- Required minimum pressure for full, half, and minimum output
- Required minimum pressure for unit operation (<full output)
- Peak burn rate
- Transportation contract
    - No-notice service, firm, enhanced Firm, secondary firm, interruptible, etc.
    - Transportation contract options available for natural-gas-fired generators
- Commodity
    - Type of service—firm or interruptible, Other?
        - Number of available suppliers
    - Number of pipelines
    - Storage access
    - Asset Management Arrangements (e.g., firm delivery expressed in MMBtu/day)
- Seasonal operations considerations
    - Identify any force majeure events called by the pipeline in the last 10 years
    - Identify any critical generators connected to the pipeline that could affect your deliveries
    - What is the nature of the balancing flexibility the pipeline offers you and provide a link to the tariff summary
- Seasonal maintenance considerations

Oil Information

- Limitations on oil burn, number of hours, emissions limitations, seasonality limits

- Number of hours of operation at max/min output on oil
- Maximum fuel storage capability
- Type(s) of oil (e.g., residual fuel oil, fuel oil #2, etc.)
    - Available usable fuel in storage (typical annual-average value)
- Plans to increase available usable fuel amount
- Assurance level for additional deliveries
- Can fuel be replenished faster than it is used?
- Alternate fuel contracts
- Number of alternate fuel suppliers
- Fuel primary and alternate transportation type (pipeline, barge, rail, truck, etc.)
- Fuel resupply limitations
    - Notice time and delivery time
    - Deliveries expected over given period of time (e.g., how many per day)
    - Proximity of supplier(s)
    - Available offloading facilities
- Does unit need natural gas to start?
    - If so, is the fuel stored on site?
- Do other units share oil inventory?
    - If so, number of hours of operation at max output on shared oil

Coal Information

- Maximum storage capacity
    - Current inventory amount
- Inventory resupply plans
- Assurance level for additional deliveries
- Alternative suppliers
- Maximum output that can be sustained indefinitely
- Fuel primary transportation type (barge, rail, truck, etc.)
- Can fuel be replenished faster than it is used?
- Secondary transportation
- Fuel delivery time
- Is delivery on a schedule?
- Scheduled time between replenishments
- Maximum amount delivered in a single shipment

- Typical coal level for replenishment order
- Units that share coal inventory
- Max runtime for unit with shared fuel inventory
- Does unit need oil or natural gas to start?
    - If so, what fuel(s) is stored on site?
- What is the unit's history of freezing coal inventory/piles and are any measures in place to mitigate freezing?

Alternate Fuel Information

- Alternate fuel source(s)
- Additional staffing requirements to start the unit on alternate fuel
- Number of hours of operation at max on alternate fuel
- Maximum fuel storage capability
- Available usable fuel in storage
- Plans to increase available usable alternate fuel amount
- Assurance level for additional deliveries
- Alternative suppliers
- Fuel primary transportation type (barge, rail, truck, etc.)
- Can fuel be replenished faster than it is used?
- Secondary transportation
- Alternate fuel resupply time
- Unit net MW max capability on alternate fuel
- Does the unit have to be taken off-line to switch to the alternate fuel?
    - If not, what is the MW output level needed to perform switching?
- Time to transition to alternate fuel
- Date alternate fuel capability was last tested
- Amount of net MW output achieved while on alternate fuel
- Does unit need natural gas to start?
    - If so, is the fuel stored on site?
- Max number of starts per day on alternate fuel
- Number of starts per week on alternate fuel
- Can generator operate on both fuels simultaneously?

Environmental/Emissions

- Unit environmental/emissions limitations
- Pollutant responsible for most limiting emissions limit

- Limit periodicity of pollutant responsible for most limiting emissions limit
- Pollutant responsible for most second most limiting emissions limit
- Limit periodicity of pollutant responsible for most second most limiting emissions limit
- Other environmental/emissions concerns

Contributors

NERC gratefully acknowledges the contributions and assistance of the following industry experts in the preparation of this guideline.

Name	Entity
Matthew Agen	American Gas Association
Nancy Bagot	Electric Power Supply Association
Michelle Bloodworth	Americas Power
Sean Bodkin	Dominion Energy
John Brewer	National Energy Technology Laboratory
David Brown	NextEra Energy Resources, LLC
Layne Brown	Western Electricity Coordinating Council
Jim Davis	Dominion Energy
Joan Dreskin	Interstate Natural Gas Association of America
Katie Ege	Great River Energy
Dan Farmer	Entergy
Brian Fitzpatrick	PJM Interconnection
Dale Hinson	Dominion Energy
Cindy Hotchkiss	Southern Company
Patricia Jagtiani	Natural Gas Supply Association
Alan Kloster	Evergy
Mike Knowland	Independent System Operator New England
Andrea Koch	Edison Electric Institute
Michael Lombardi	Northeast Power Coordinating Council
Connie Lowe	Dominion Energy
Mike Mattox	Midwest Independent System Operator
Al McMeekin	North American Electric Reliability Corporation
Michael Oberleitner	Dominion Energy
Maggie O'Connell	Interstate Natural Gas Association of America
Levetra Pitts	North American Electric Reliability Corporation
Thomas Popik	Foundation for Resilient Societies
Elsa Prince	North American Electric Reliability Corporation
Joseph Ricasio	Independent Electricity System Operator
Sammy Roberts	Duke Energy
Scott Barfield	North American Electric Reliability Corporation
Phillip Shafeei	Colorado Springs Utilities
Tim Sherwood	Southern Company
Chris Smith	Interstate Natural Gas Association of America
Mark Spencer	LS Power Development
John Stevenson	New York Independent System Operator
Robert Tallman	North American Electric Reliability Corporation
Charles Yeung	Southwest Power Pool, Inc.

Guideline Information and Revision History

Guideline Information	
Category/Topic: Fuel Assurance	**Reliability Guideline/Security Guideline/Hybrid:** Reliability Guideline
Identification Number: RG-FAS-0923-2	**Subgroup:** EGWG

Revision History		
Version	**Comments**	**Approval Date**
1	Approved by the RSTC	March 2020

Metrics

Pursuant to the Commission's Order on January 19, 2021, *North American Electric Reliability Corporation*, 174 FERC ¶ 61,030 (2021), reliability guidelines shall now include metrics to support evaluation during triennial review consistent with the RSTC Charter.

Baseline Metrics

All NERC reliability guidelines include the following baseline metrics:

- BPS performance prior to and after a reliability guideline as reflected in NERC's State of Reliability Report and Long Term Reliability Assessments (e.g., Long Term Reliability Assessment and seasonal assessments)
- Use and effectiveness of a reliability guideline as reported by industry via survey
- Industry assessment of the extent to which a reliability guideline is addressing risk as reported via survey

Specific Metrics

The RSTC or any of its subcommittees can modify and propose metrics specific to the guideline in order to measure and evaluate its effectiveness, listed as follows:

- RTOS will conduct periodic evaluations of the gas system supply constraints that have resulted in derates to generators. These will be categorized and tracked for trend analyses. This information is available to NERC in GADS7.

Effectiveness Survey

On January 19, 2021, FERC accepted the NERC proposed approach for evaluating Reliability Guidelines. This evaluation process takes place under the leadership of the RSTC and includes:

- industry survey on effectiveness of Reliability Guidelines;
- triennial review with a recommendation to NERC on the effectiveness of a Reliability Guideline and/or whether risks warrant additional measures; and
- NERC's determination whether additional action might be appropriate to address potential risks to reliability in light of the RSTC's recommendation and all other data within NERC's possession pertaining to the relevant issue.

NERC is asking entities who are users of Reliability and Security Guidelines to respond to the short survey provided in the link below.

Guideline Effectiveness Survey

Errata

Date: Example text here. Example text here. Example text here. Example text here. Example text here.

Agenda Item 16
RSTC Meeting
September 20, 2023

Product Security Sourcing Guide & Reference Guide

Supply Chain Working Group Security Guideline

Action

Accept to post for 45-day comment period

Background

The Supply Chain Working Group (SCWG) presents to the RSTC the following Security Guideline and Reference Guide for acceptance to post for 45-day comment period.

- Draft Security Guideline Product Security Sourcing Guide
- Draft Product Security Reference Guide (spreadsheet)

The Product Security Sourcing Guide presented here serves as an industry-standard guide for identifying key security and risk considerations to support procurement of grid technologies and products. Asset owners must maintain situational awareness of the risks associated with grid operations in an often-uncertain geo-political environment. This is often hindered by unverified trust and supplier controls and the presence of unknown product vulnerabilities. Therefore, asset owners can use this guide to define and enforce supplier controls that ensure minimum cybersecurity requirements have been implemented within grid products.

Summary

The cybersecurity controls documented in this Product Security Sourcing Guide and the accompanying Product Security Reference Guide can be leveraged by asset owners to coordinate purchase activities between cybersecurity professionals and their procurement organizations, while working in step with NERC to confirm these steps have been successfully executed. These controls also provide consistent guidance to the supplier community.

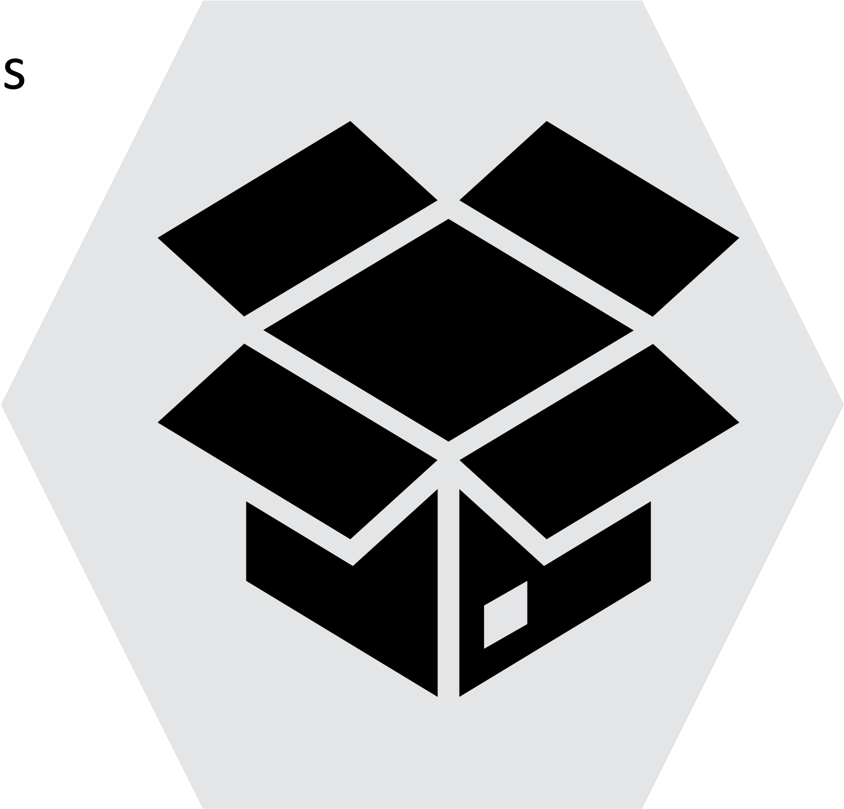
Product Security Sourcing & Reference Guide

Tobias Whitney, VP of Strategy and Policy, Fortress Information Security
Reliability and Security Technical Committee Meeting
September 20, 2023

RELIABILITY | RESILIENCE | SECURITY

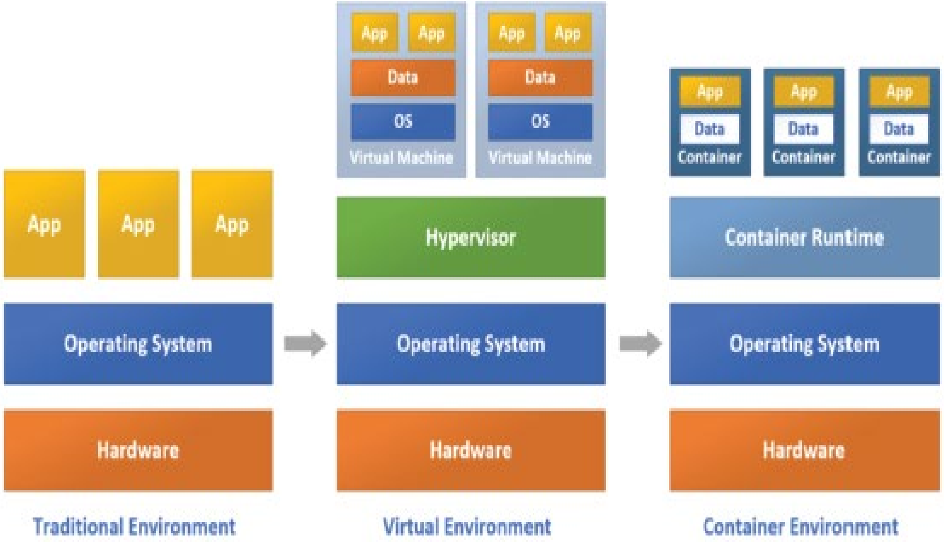
Outline

- Vendor-Level Controls, Artifacts and Attestations
- Grid Technologies and Applicable Control Environments
- Geo-political Risk Considerations
- Product Scarcity Risk Considerations
- Cloud Connectivity Product Risks
- Product Security Reference Guide

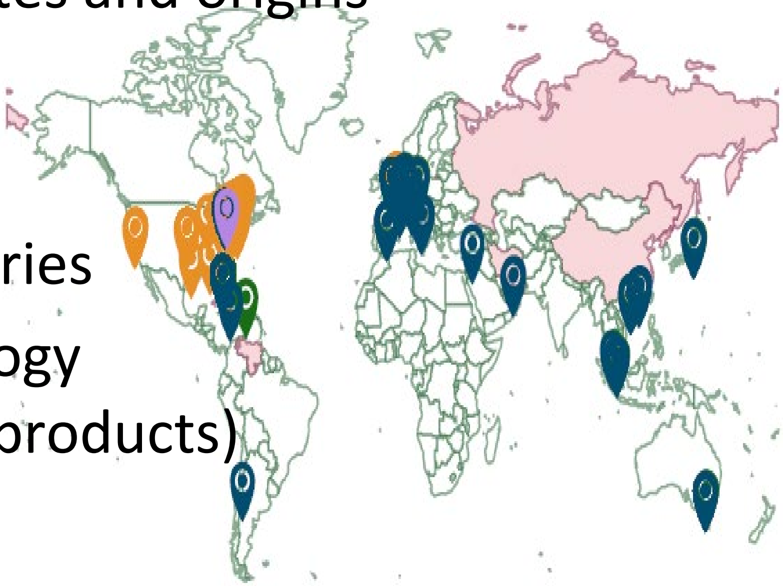


Key Sourcing Considerations

- Managing 3rd Party Risk Assessments & Contracts
  - Industry guidelines
  - Managing Critical Risks
  - Vendor Management Government
- Vendor Vulnerability Disclosure
  - Push / Pull Process
- Cloud / SAAS Risks
  - Virtual and Container



Key Sourcing Considerations



- Geo-political mapping
- Understanding “banned-entities”
- Identify national affiliations attributes and origins
- Manufacturing/assembly locations
- Cyber footprint
- Financial relationships and subsidiaries
- Application of Technology (technology considerations of the purchaser of products)
- BES related considerations
- Distribution, DER and Microgrids
- Defense Critical Infrastructure

Key Sourcing Considerations

- Availability of “Long Lead-Time” Technologies
- Incentivizing domestic sourcing
- US Buy/Build America
- Alternative Sourcing Options
- Lead Time Transparency
- Vendor Attestations

Product Security Reference Guide

- Mapped 12+ relevant OT and Grid related standards and guidelines:
  - NREL Cybersecurity Certification Recommendations
  - NIST Cyber Security Framework
  - NIST.IR 7628 Smart Grid Cybersecurity
  - NATF Supply Chain Criteria v3.0
  - DER Cybersecurity Framework
  - IEC 62443 Security for Industrial Automation
  - IEEE P1547.3
  - Others

Security Controls	Description
Vendor- Level Supply Chain Security	Perform independent penetration tests of all integrated COTS components and validate that vendors have established processes for managing device identity. Perform due diligence of all hardware, software, firmware and service suppliers, and require Software Bill of Materials (SBOMs) and Hardware Bill of Materials (HBOMs) for relevant products.
Geo-political Risk Considerations	Some organizations have requirements or mandates that dictate which companies and suppliers they may source from for certain grid technologies. Obtaining information about their geo-political footprint can help inform the purchasing organization of foreign ownership, control or influence risk.
Secure Development Processes and Practices	Validate that suppliers d have established cybersecurity training programs for product developers and that each product undergoes a threat modeling and operational impact assessment. Validate the use of secure coding practices and that suppliers have in place vulnerability discovery response plans and published methods for submission of independent vulnerability disclosures. This may include SBOMs to aid in the analysis of software risk management.
Device & Product Security Management, Tamper Protections and Physical Security Controls	Validate that products require change of default passwords upon first use, establish product lockouts based on failed login attempts, validate digital signatures on all updates, and allow disablement of ports and services. This may include the evaluation of component risk that can be identified through the review of HBOMs. Validate that products implement secure storage for cryptographic primitives and keys, restrict access to audit logs, and support disablement of specific ports and services.
Authentication, Authorization and Access Controls	Validate that products require multi-factor authentication (MFA) for all administrative access, implement role-based access controls to support separation of duties, require minimum password complexity, and implement session timeouts.
Monitoring and Logging	Validate that products log user actions including login events, privilege escalation, account creation, unauthorized file access, and remote access attempts.
System Segmentation	Ensure that systems segment systems based on trust, risk profiles or other security-relevant attributes; segment all data acquisition interfaces from management functions, and segment all enterprise networks from the Internet.
Information Protection	Validate that products encrypt all interfaces, use standards-compliant cryptographic modules/libraries, authenticate all messages, protect integrity of all messages, and secure all wireless interfaces.
Vulnerability Management & Disclosure	Validate that manufacturers have processes and procedures in place to accept vulnerability disclosure reports from customers and independent security researchers and can track those reports to closure.

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

DRAFT
Security Guideline
Product Security Sourcing Guide

XX 2023

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

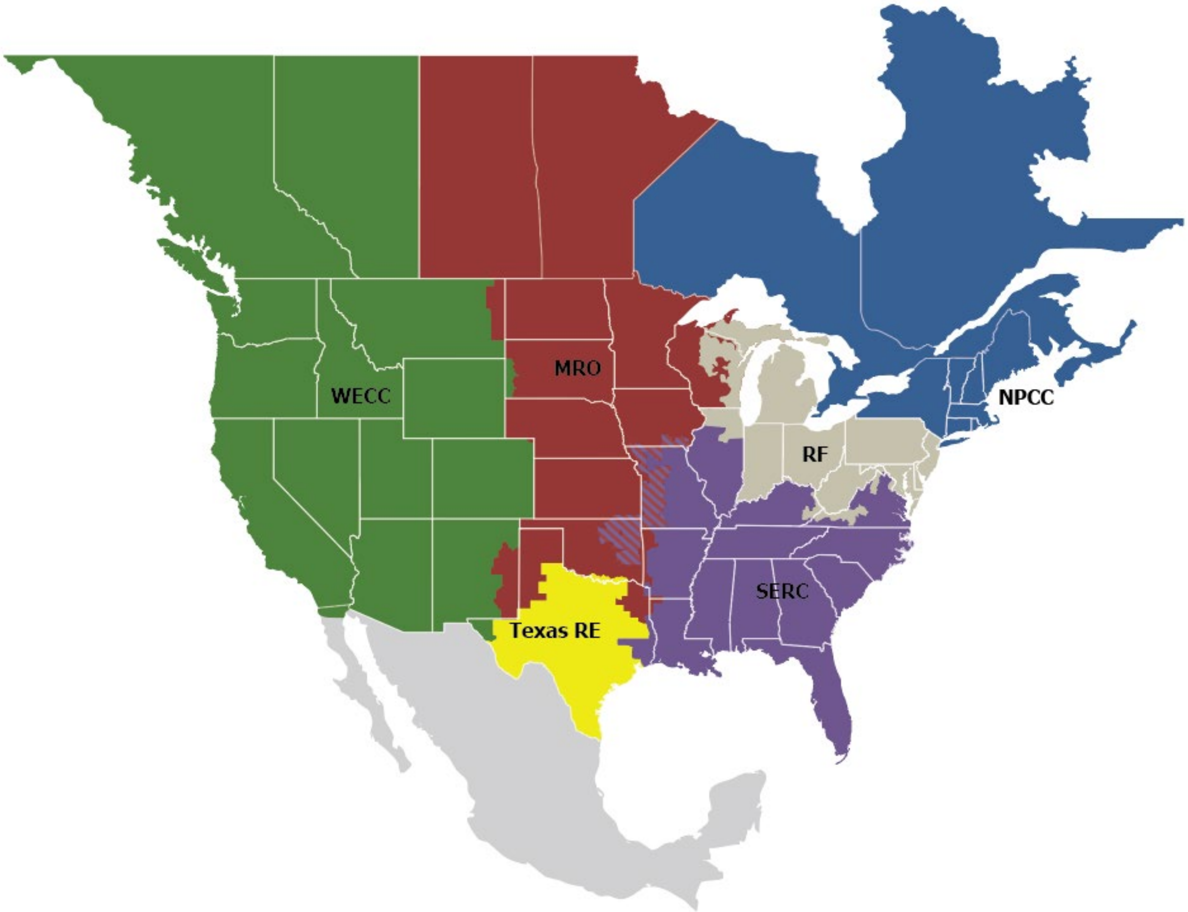
Table of Contents

Preface

Electricity is a critical component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which comprises NERC and the six Regional Entities, is that of a highly reliable, resilient, and secure North American bulk power system (BPS). Our mission is to ensure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is composed of six Regional Entity boundaries as shown in the map and corresponding table below. The multicolored areas denote overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners /Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Preamble

Through its subcommittees and working groups, the NERC Reliability and Security Technical Committee (RSTC) develops and triennially reviews reliability and security guidelines in accordance with the procedures set forth in the RSTC Charter. Reliability and security guidelines reflect the collective experience, expertise, and judgment of the industry on matters that impact BPS operations, planning, and security. Reliability and security guidelines provide key practices, guidance, and information on specific issues critical to promoting and maintaining an exceptionally reliable and secure BPS.

Each entity registered in the NERC compliance registry is responsible and accountable for maintaining reliability and compliance with applicable mandatory reliability standards. Reliability guidelines are not binding norms or parameters nor are they reliability standards; however, NERC encourages entities to review, validate, adjust, and/or develop a program with the practices set forth in this guideline. Entities should review this guideline in detail and in conjunction with evaluations of their own internal processes and procedures. These reviews could highlight that appropriate changes are needed; if called for, such changes should be made with consideration of system design, configuration, and business practices.

Introduction

Continuously evolving power grid designs, including distributed energy resources, integrated renewables, and cloud-based operations, have created new attack vectors for attackers to exploit, particularly in the controllers that manage energy systems. As the networking of embedded systems within energy grids continues to expand, the attack surfaces will only grow larger. Asset owners must understand the unique risks associated with grid operations and enforce stringent requirements on product developers to mitigate potential security vulnerabilities.

The energy grid is a critical part of US infrastructure and highly vulnerable to cyber-attacks. Some examples of cyber threats to the energy grid include:

- Malware: Malware can be used to infiltrate energy grid systems, steal data, or cause system failures.
- Phishing: Phishing attacks are commonly used to gain access to energy grid systems. Attackers use phishing emails to trick users into revealing login credentials or downloading malware.
- Ransomware attacks: Ransomware attacks are a growing concern for energy grid operators. Attackers use ransomware to encrypt data and demand payment for its release.
- Insider threats: Insider threats are also a significant concern for the energy grid. Disgruntled employees or contractors with access to sensitive systems can cause grave damage.
- Overreliance on oversees manufacturing of critical infrastructure could be disrupted in times of international conflict or other emergency conditions.

While the NERC Supply Chain Risk Management Standards focus primarily on the security controls of the supplier, the Product Security Sourcing Guide presented here serves as an industry-standard guide for identifying key security and risk considerations to support procurement of grid technologies and products. Asset owners must maintain situational awareness of the risks associated with grid operations in an often-uncertain geo-political environment. This is often hindered by unverified trust and supplier controls and the presence of unknown product vulnerabilities. Therefore, asset owners can use this guide to define and enforce supplier controls that ensure minimum cybersecurity requirements have been implemented within grid products.

The cybersecurity controls documented in this Product Security Sourcing Guide and the accompanying Product Security Reference Guide can be used by asset owners to coordinate purchase activities between cybersecurity professionals and their procurement organizations, while working in step with NERC to confirm these steps have been successfully executed. These controls also provide consistent guidance to the supplier community.

Vendor-Level Controls, Artifacts and Attestations

Once an asset owner has set out to determine whether a new grid technology is needed, the first step is to begin vetting the vendor through various internal and third-party risk assessment procedures. The industry has developed a number of tools, initiated by the NERC CIP Supply Chain Risk Management Standards, that, over time, have been expanded in terms of guidelines and plans.

NATF guidelines

- Supply Chain Security Assessment Model[1]
- NATF CIP-013 Implementation Guidance-Independent Assessments of Vendors (ERO Endorsed)[2]
- NATF CIP-013 Implementation Guidance-Supply Chain Risk Management Plans (ERO Endorsed)[3]

EEI Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk[4]
NERC SCWG guidelines

- Security Guideline: Vendor Risk Management Lifecycle[5]
- Security Guideline: Supply Chain Provenance[6]

While the NERC CIP Supply Chain Risk Management Standards focus primarily on the procurement of grid technologies and products, entities should consider similar practices for a broader range of technology acquisitions as a best practice.

Managing critical vendors

Effective vendor management enables organizations to proactively mitigate risks throughout the vendor engagement lifecycle. It is essential to establish governance and processes for continuous risk monitoring of your most critical vendors. Cyber risk is constantly changing and evolving at an increasingly rapid rate. Point-in-time security assessment questionnaires, although effective in establishing a baseline security assessment, should be augmented with routine assessments throughout a vendor's engagement. The frequency of subsequent assessments should be based on the initial assessment and the dependence and criticality of the vendor and adjusted as necessary when novel or notorious threats emerge. For instance, if a supplier is impacted by a popular open-source software vulnerability, such as Log4j, it would be reasonable to request from the vendor updated assessment impacts and any changes to the supplier's control environment.

Vendor management governance

It's advisable to establish vendor management processes that are the best fit your organization. In order to ensure the right contract, metrics, and frequency of assessments are in force, segment or categorize vendors based on your initial assessment results and cyber risks. Use this approach to determine which vendors are most critical or strategic to your operations. Identify accountable resources or vendor relationship managers and establish proactive methods,

---

[1] https://www.natf.net/docs/natf/documents/resources/supply-chain/supply-chain-security-assessment-model.pdf
[2] https://www.natf.net/docs/natf/documents/resources/supply-chain/natf-cip-013-implementation-guidance-independent-assessments.pdf
[3] https://www.natf.net/docs/natf/documents/resources/supply-chain/natf-cip-013-implementation-guidance-supply-chain-risk-management-plans.pdf
[4] https://www.eei.org/-/media/Project/EEI/Documents/Issues-and-Policy/Model--Procurement-Contract.pdf
[5] https://urldefense.com/v3/__https:/www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Vendor_Risk_Management_Lifecycle.pdf__;!!DR3VkBMYqM1H!bCwBYFYdKM5cOQlWOCKFQvPm4yIN0UY3LHFSk-SPtsRbmWhjtBdzFmRNBwBdHJnMu5R4HaJNhZnbJdqc4AuJyK7T4yqcaA$
[6] https://urldefense.com/v3/__https:/www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Supply*20Chain*20Provenance.pdf__;JSU!!DR3VkBMYqM1H!bCwBYFYdKM5cOQlWOCKFQvPm4yIN0UY3LHFSk-SPtsRbmWhjtBdzFmRNBwBdHJnMu5R4HaJNhZnbJdqc4AuJyK44O5IPag$

such as scorecards, to proactively assess the performance of your most critical vendors. This will require cross-functional collaboration between Procurement, Information Technology, Cyber Security, and Compliance, among others.

Vendor management risk mitigation practices

Establish and maintain a list of your most critical vendors that includes supplier points of contact as well as escalation contacts for issue resolution. Procurement and cybersecurity teams should be collaborating closely by ensuring that their Cyber Security Supply Chain Risk Management plans identify continuous monitoring scenarios during the supplier lifecycle that may trigger a security reassessment. These should including but not be limited to:

- Material changes in supplier scope-of-engagement. (E.g., original purchase or hardware followed by a subsequent software purchase later in the engagement.)
- Mergers, acquisitions, or changes in ownership.
- A security incident or vulnerability notification.
- A change in the type of physical and logical access required by a supplier or their resources.
- An uncharacteristic change in supplier performance.

Determine comprehensive stakeholder responsibilities for the following roles:

- Cybersecurity
- Engineering
- Procurement
- Information Technology
- Operations

Additionally, the following metrics and conditions must be implemented:

- Risk assessment frequency for critical vendors, ranked by
  - High risk
  - Medium risk
  - Low risk
- Raise supplier accountability
  - Highlight performance or non-compliance
  - Increase strategic alignment
- Risk mitigation upon contract renewal or amendment
  - Demonstrate how risk is mitigated with compliance and enforcement
  - Update contract templates and standards accordingly

Grid Technologies and Applicable Control Environments

After the initial vendor vetting has been completed, the next step is to understand what types of grid technology are being purchased by the asset owner and what considerations should be addressed given the regulatory, standards, and compliance considerations of the given environment within which the system will be implemented. Product developers should implement the product, supply chain, and development environment security controls for their technologies and products in a manner consistent with the controls required for the operating environment. Energy companies have complex operating environments that will dictate which regulations and standards are met for a given operating environment. In practice, there are three core operating environments:

1. **Bulk Electric System** (BES) – the official definition of the BES can be found here[7]. The BES can be considered as those systems associated with anything at or above 100KV or 50MVA, and applicable to low, medium or high BCS categorizations of the NERC CIP standard.
2. **Non-BPS (Distribution, DER, and Renewables)** – systems not considered to be under the jurisdiction of FERC or NERC, which are, instead, generally under the jurisdiction of state public utility commissioners. This category of systems is not mandated to be compliant with NERC CIP standards and therefore does not have a uniform set of cybersecurity requirements.
3. **Defense-Critical Electric Infrastructure** – "any electric infrastructure that serves" a Critical Defense Facility, "but is not owned or operated by the owner or operator of such facility."[8]

Table 1 provides a high-level view of the minimum essential controls for grid products based on the operating environments described above. Detailed control descriptions, including measures of compliance, can be found in the Product Security Reference Guide.

Table 1: Minimum Essential Controls

Security Controls	Description
Vendor- Level Supply Chain Security	Perform independent penetration tests of all integrated COTS components, establish an identity/access management program. Perform due diligence on all hardware, software, firmware, and service suppliers, and generate Software Bill of Materials (SBOMs) and Hardware Bill of Materials (HBOMs) for relevant products.
Geo-political Risk Considerations	Some organizations have requirements or mandates that dictate which companies and suppliers they may source for certain grid technologies. Obtaining information about their geo-political footprint can help inform the purchasing organization of foreign ownership, control or influence risk.
Secure Development Processes and Practices	Establish cybersecurity training programs for all developers and perform threat modeling and operational impact assessments for each product. Use secure coding practices, document vulnerability discovery response plans, and publish methods for submission of independent vulnerability disclosure. This may include SBOMs to aid in the analysis of software risk management.
Device & Product Security Management, Tamper Protections and	Require change of default passwords upon first use, establish product lockouts based on failed login attempts, validate digital signatures on all updates, and allow disablement of ports and services. They may include the evaluation component risk that can be identified through the review of HBOMs. Implement secure storage for

---

[7] https://www.nerc.com/pa/Stand/2018%20Bulk%20Electric%20System%20Definition%20Reference/BES_Reference_Doc_08_08_2018_Clean_for_Posting.pdf

[8] https://www.energy.gov/oe/articles/oe-dcei-strategy-eac-101420

Table 1: Minimum Essential Controls	
Security Controls	**Description**
Physical Security Controls	cryptographic primitives and keys, restrict access to audit logs, and support disablement of specific ports and services.
Authentication, Authorization and Access Controls	Require multi-factor authentication (MFA) for all administrative access, implement role-based access controls to support separation of duties, require minimum password complexity, and implement session timeouts.
Monitoring and Logging	Log user actions, including login events, privilege escalation, account creation, unauthorized file access, and remote access attempts.
System Segmentation	Segment systems based on trust, risk profiles or other security-relevant attributes; segment all data acquisition interfaces from management functions and segment all enterprise networks from the Internet.
Information Protection	Encrypt all product interfaces, use standards-compliant, cryptographic modules and/or libraries, authenticate all messages, protect integrity of all messages, and secure all wireless interfaces.
Vulnerability Management & Disclosure	Implement controls that ensure manufacturer has processes and procedures in place to accept vulnerability disclosure reports from customers and independent security researchers and can track those reports to closure.

Product Vulnerability Disclosure

Vulnerability disclosure can be managed in two ways: (1) communications from a *customer to the supplier* (known as Pull) and (2) communications from the *supplier to a customer* (Push). The Pull case is less frequently needed, but a mature supplier organization will be prepared for it and should be willing to share those preparations with their clients and customers.

Disclosure to the supplier

Make sure the asset owner understands how to report vulnerabilities. Until the asset owner has a vulnerability in hand it will not need more than a contact channel and broad outlines of how the process works. Detailed procedural information is normally provided by the supplier upon initiating an actual disclosure. That process should include these steps:

- Contact the channel for initial contact.
- Expect information about how the process will be handled – confirmation, trajectory, and timeline.
- The process should describe a secure method for confidential transfer of information relating to vulnerability.

Disclosure from the supplier

Disclosure from the supplier can be either current or historical. Current disclosures relate to new vulnerability findings and information as they are identified. Historical disclosures are records for past products and/or versions and are useful when dealing with non-current products.

Current disclosure by the supplier: "Push" or "Pull" Process

When procuring from a supplier, that relationship becomes part of your accepted risk picture. When security vulnerabilities occur in the products get from them, those risks add to the system's risk posture. Security vulnerability disclosures are how an asset owner learns of vulnerabilities and gains the information necessary to react to them to keep risk at an acceptable level.

As part of vulnerability risk management, vendors should be able to provide a SBOM to assist in managing the risk of security vulnerabilities in products. At the least, these will allow you to determine whether the security of the asset owner's systems might be affected at the time that a serious vulnerability in a software component is announced, and likely before a supplier using that component has provided an update.

Information about vulnerabilities can take the form of notifications from the supplier (Push), such as email or a communications channel that provides product release notes and security notices. Push notifications from a supplier or vendor are more likely to be sent in "real time" – i.e., close to the time that the vulnerability is confirmed. Given the possibility that the asset owner may not always immediately pick up these types of Push notifications in a timely way, it's advisable to establish a system of "pulling" updates on vulnerability information. Doing so provides a high degree of assurance (though not 100 percent) that you have all the information currently available.

However, once an asset owner acquires the system, it will need timely and sufficient information to make an informed decision, usually whether to install an offered update, apply mitigating security controls, or do nothing. Asset owners will need to ask suppliers:

- How will you learn of vulnerabilities?
- Is there more than one legitimate channel?
- Is the channel trustworthy (e.g., https, using TLS protocol as maintained by IETF)? How do you ensure that the information is authentic?

- Are there specific disclosure times, or can disclosures occur at any time?
- Does the supplier have a way to inform customers of a zero-day (product vulnerability not yet patched)?
- Does the supplier treat unsupported/out-of-date components as a security vulnerability?

Vulnerability disclosures must serve your needs. Vulnerability disclosures must:

- Name the affected product(s) and version(s).
- Describe what could happen.
- Describe who could cause it to happen and how.
- Offer means to address vulnerability.

Asking to see examples of past vulnerability disclosures might clarify how these requirements are satisfied, and the audience it was written for. After all, someone in your organization will have to read them and understand them.

Geo-political Risk Considerations

The U.S. Department of Commerce indicates that adversarial nations[9], such as Russia and China, that possess or have access to advanced technological capabilities are a significant risk to the United States and its allies. This was acknowledged by the 2022 National Defense Strategy[10], which states:

> "The PRC or Russia could use a wide array of tools in an attempt to hinder U.S. military preparation and response in a conflict, including actions aimed at undermining the will of the US public, and to target our critical infrastructure and other systems."

Jen Easterly, Director of the US Cybersecurity & Infrastructure Security Agency (CISA), stated that If China were to launch a military takeover of Taiwan, China "might very well" couple that invasion with cyberattacks on US infrastructure, "with the explosion of multiple gas pipelines, the mass pollution of our water systems, the hijacking of our telecommunication systems, the crippling of our transportation nodes… all designed to incite chaos and panic across our country and deter our ability to marshal military might and citizen will."[11] In addition to such attacks, China dominates the market.

In May 2023, China targeted the US through Guam. In has been reported by CISA that the Chinese-sponsored cyber group Volt Typhoon is targeting key US sectors such as communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and education.

By dominating the global critical infrastructure market (batteries, drones, and other technologies), China secures two advantages (1) Economic growth and (2) Exploitation of critical infrastructure to help prevail in wartime, especially by jeopardizing US public safety and disrupting defense-critical infrastructure. Domestic-critical infrastructure owners and operators can expect that US adversaries will continue to target grid technologies and seek to corrupt supply chains supporting US and allied infrastructure.

This document seeks to mitigate the risk. Presently, there are no mandatory or enforceable standards to ensure that hardware and software suppliers are measurably secure and have minimal exposures to geo-political risk in grid technology supply chains. For this reason, this section of the guidance document is geared toward providing examples of information that purchasing organizations may request from manufacturers to help obtain visibility into geo-political risk concerns:

1. **Manufacturing, Development or Assembly Location:** Information describing which countries or cities manufactured or developed specific technologies can help the purchasing organization determine the whereabouts of critical components of the product that can be implemented within their environment. Often SBOMs and HBOMs, respectively, can identify key components of the product that then can be mapped to locations. Understanding the component provenance or sourcing is a key step in understanding geo-political risk that can be linked to manufacturing, development, or assembly.
2. **Cyber Presence:** Often can be described as locations of the supplier's internet-facing infrastructure, such as web servers, DNS servers or IP address ranges where remote support is performed. Remote support services and capability provided by the vendor may often be described in service contracts. This information can provide insight and awareness into the purchasing organization's network or cybersecurity team in order to manage traffic or incidents originating from identified sources.

---

[9] https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list

[10] https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF

[11] https://www.cisa.gov/cisa-director-easterly-remarks-carnegie-mellon-university

3. **Financial Relationships:** Monitoring financial ties and partnerships provides insights into the supplier's business interests or potential sources of influence. By having a geo-locational mapping of each parent, child, or peer organization, the supplier provides insight into financial relationships, which can help inform the purchasing organization as to whether those relationships would impact the risk profile of the technology in question.

4. **Emphasizing Domestic Suppliers:** The Department of Energy [12] has established new incentives to ensure that grid technologies are sourced by domestic manufacturer. In addition, the Department of Treasury, and Internal Revenue Service have established programs to incentivize domestic clean energy manufacturing[13]. Purchasing organizations will be looking to determine if their suppliers have domestic manufacturing that fulfills federal incentives. As a result of these policies and federal tax programs, utilities should consider establishing incentives to emphasize domestic sourcing in their procurement processes.

---

[12] https://www.energy.gov/sites/default/files/2023-04/DOE%20DPA%20Roundtables%20and%20RFI%20Executive%20Summary%20FINAL%203-21-23.pdf

[13] https://home.treasury.gov/news/press-releases/jy1477

Product Scarcity Risk Considerations

In August of 2022, Congress passed, and the President signed into Law, the Inflation Reduction Act, which included \$500M[14] to execute the Defense Production Act (DPA). The DPA allows for the federal government to subsidize domestic production to increase the production of goods or services. The DPA was invoked to increase production of heat pumps, transformers, and other electric power grid components. The inclusion of transformers and electric grid components was in large part in response to the Electricity Subsector Coordinating Council Tiger Team on supply chain. The Tiger Team[15] found that the average delivery time for a distribution transformer is one year from the original purchase.

In addition, many factors, including the Russian Ukraine conflict, and RTO capacity markets, have caused critical shortages of fossil fuels, driving up prices for fossil fuels as the conflict ensues. This has created a surge in demand for wind, solar and energy storage capacity[16] -- on the order of 50 to 100 percent. One unforeseen consequence of the surge of renewable technologies is an increased reliance on China to supply key technologies that can support these emerging low-carbon demands on the global energy supply chain.

These supply chain and geo-political risks have created a unique set of complex choices for asset owners and suppliers. To help identify and coordinate efforts to mitigate product scarcity risks, the following recommendations are proposed for consideration during the utilities' supply procurement process:

- **Product or Component Availability Attestations:** Request product and key component availability or lead-time status of grid technologies as part of procurement activities. This may include requesting HBOMs that identify where key component partners source their technology.
- **Product or Component Change Alerts:** Require that the supplier discloses to the purchasing asset owner when a key product or product sub-component is no longer available or whether the product or subcomponent will be sourced by a different manufacturer or fourth-party supplier.
- **Sourcing Alternatives:** Procurement organizations should identify alternative product manufacturers that coincide with the procurement organization's functionality requirements, ESG practices and security controls.
- **Product availability Opt-out Clauses:** Ensure procurement contracts with suppliers provide the purchasing organization with a reasonable ability to limit or terminate the contract due to product availability issues, long lead-times or other delays.

---

[14] https://www.whitehouse.gov/briefing-room/statements-releases/2022/06/06/memorandum-on-presidential-determination-pursuant-to-section-303-of-the-defense-production-act-of-1950-as-amended-on-transformers-and-electric-power-grid-components/

[15] https://www.electric.coop/tiger-team-electric-co-op-leaders-join-effort-to-ease-supply-chain-problems

[16] https://www.woodmac.com/news/the-edge/how-the-russia-ukraine-war-is-changing-energy-markets/

Cloud Connectivity Product Risks

When certain grid technologies are implemented within an asset owner's environment, they might be implemented with a back-end communications infrastructure that introduces additional security and compliance risks. A specific physical device, appliance or piece of hardware may incorporate an application or operating system that can interact with or be hosted by the supplier or a cloud service provider (CSP). The diagram below (Figure 1), describes various common architectural designs of today's grid technologies.

The traditional environment reflects a typical on-premise installation where cloud connectivity risk is minimal. The virtual and container environment examples reflect how certain grid technologies could be hosted on-premise or in conjunction with a CSP in coordination with the supplier. It is advisable to determine via the procurement process as to whether the grid technology under consideration operates via a virtual or container environment hosted via the supplier or a CSP.

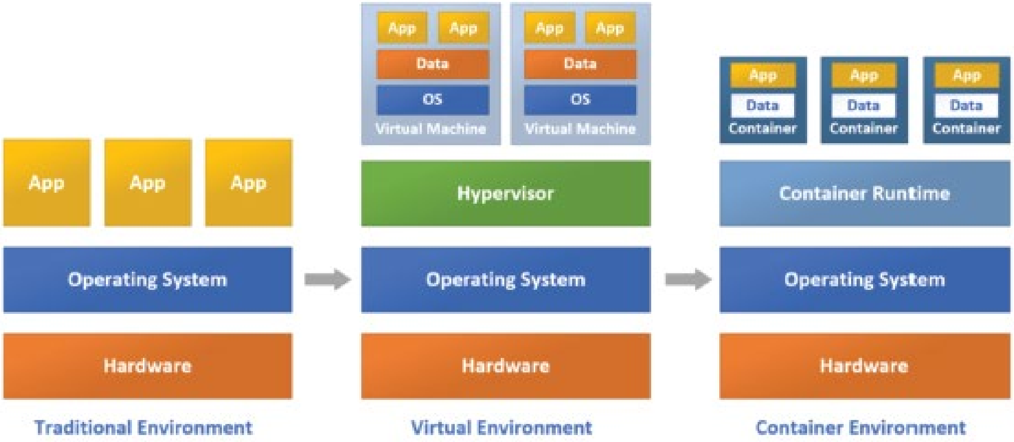


Figure 1: EPRI Research - Cloud Models[17]

To help identify and develop mitigation measures to address the risk of this type of product infrastructure, the asset owner and supplier should coordinate by considering the following practices:

1. Inquire whether the grid technology in question operates in either of the three operating environments (a virtual or container environment hosted via the supplier or a CSP).
2. For technologies that have a virtual or container environment, determine whether any of the architectural functions require off-site support or operations by the supplier or a CSP.
3. For the functions performed off-site, obtain the vendor's security and controls evidence, artifacts and attestations as described on page 1 of this document.

---

[17] https://www.epri.com/research/products/000000003002017577 - "Cloud concepts and security approaches that are unique to off-premise cloud implementation and provides foundational considerations for reference architectures to manage cloud service provider deployments for grid-edge applications, low-impact BES Cyber Systems located in the cloud and managed security services for low impact BES Cyber Systems."

Contributors

NERC gratefully acknowledges the contributions and assistance of the following industry experts in the preparation of this guideline. Contributions made are the views of the contributors and not necessarily those of the organizations they represent.

Name	Entity
Tobias Whitney	Fortress Information Security
Alan Kloster	Evergy
Andrea Koch	EEI
Andrew Ralph	Entergy
Betsy Soehren Jones	Fortress
Brian Russell	TrustThink
Byron Booker	Oncor
Cassie Crossley	Schneider Electric
Christine Ericson	Illinois Commerce Commission
Christopher Strain	FPL
Cordell Briggs	UTC
David James Earley	NATF
Frank Kapuscinski	RF
George Masters	Schweitzer Engineering Labs
Gregory Hardin	SERC
Jacque Mortenson	OTPCO
Jeffrey Sykes	Utility Services
Jimmy Ramirez	ERCOT
Jonathan Dashner	OSII
Ken Keels	NATF
Krista Koors	Burns & McDonnell
Lee Felter	MRO
Matt Nicklin	SIPC
Mayur Manchanda	FERC
Mike Prescher	Black & Veatch
Olga Oswalt	Sunflower
Seemita Pal	PNNL
Shari Gribbin	CNK Solutions
Teri Kelly	Northwestern
Tom Alrich	Tom AlrichLLC
Tom Duffey	Itegrity
Tom Hofstetter	NERC
Tony Eddleman	NPPD
Tope Odubanjo	NB Power
Tracie Bushman	Idaho Power
Wally Magda	WallyDotBiz LLC

Guideline Information and Version History

Guideline Information	
Category/Topic: Supply Chain	**Reliability Guideline/Security Guideline/Hybrid:** Security Guideline
Identification Number: SG-SCH-0923-X	**Subgroup:** Supply Chain Working Group (SCWG)

Version History

Version	Comments	Approval Date
0.1	Initial Draft submitted for 45-day comment	09/20/2023

Metrics

Pursuant to the Commission's Order on January 19, 2021, *North American Electric Reliability Corporation*, 174 FERC ¶ 61,030 (2021), reliability guidelines shall now include metrics to support evaluation during triennial review consistent with the RSTC Charter.

Baseline Metrics

All NERC reliability guidelines include the following baseline metrics:

- BPS performance prior to and after a reliability guideline as reflected in NERC's State of Reliability Report and Long-Term Reliability Assessments (e.g., Long Term Reliability Assessment and seasonal assessments).
- Use and effectiveness of a reliability guideline as reported by industry via surveys.
- Industry assessment of the extent to which a reliability guideline is addressing risks as reported via surveys.

Specific Metrics

The RSTC or any of its subcommittees can modify and propose metrics specific to the guideline to measure and evaluate its effectiveness, listed as follows:

- The SCWG will use survey responses to evaluate the extent to which industry is using the recommendations from this security guide to address incident response measures in contracts and other documents associated with its vendors and service providers, and whether those measures were effective.
- The SCWG will seek, through meeting announcements and committee member emails, cooperation from industry to identify and interview two to three entities who have used the guide as a reference in modifying their incident response program. The information exchanged will be anonymous and record which aspects and recommendations of the guide have provided improvement for cybersecurity programs.

Effectiveness Survey

On January 19, 2021, FERC accepted the NERC proposed approach for evaluating Reliability Guidelines. This evaluation process takes place under the leadership of the RSTC and includes:

- Industry survey on effectiveness of Reliability Guidelines.
- Triennial review with a recommendation to NERC on the effectiveness of a reliability guideline and/or whether risks warrant additional measures.
- NERC's determination whether additional action might be appropriate to address potential risks to reliability in light of the RSTC's recommendation and all other data within NERC's possession pertaining to the relevant issue.

NERC is asking entities that are users of Reliability and Security Guidelines to respond to the short survey provided in this link: Guideline Effectiveness Survey

Errata

N/A

Agenda Item 17
RSTC Meeting
September 20, 2023

Proposed Revisions to the NERC Rules of Procedure to Register Inverter-Based Resources

Action

Review the proposed revisions to the NERC Rules of Procedure (ROP) to register owners and operators of inverter-based resources (IBR) that are connected to and have a material impact in the aggregate to the Bulk-Power System (BPS)

Background

On November 17, 2022, the Federal Energy Regulatory Commission (FERC) directed NERC to submit a work plan describing how it plans to identify and register owners and operators of IBRs that are connected to and have a material impact in the aggregate to the BPS, but are not currently required to register with NERC under the Bulk Electric System (BES) definition.

On February 15, 2023, as amended in March 2023, NERC filed a Work Plan outlining concepts and milestones to achieve that directive. On May 18, 2023, FERC accepted the Work Plan.

Summary

NERC proposes revisions to Appendices 2, 5A, and 5B of the NERC ROP to accurately reflect and address non-BES, BPS connected IBRs (unregistered IBRs).[1]

- **Appendix 2 – Definitions Used in the ROP:** i) Adding the definitions of "Generator Owner – Inverter-Based Resources" (GO-IBR) and "Generator Operator – Inverter-Based Resources" (GOP-IBR) to mirror the Registry Criteria revisions proposed in Appendix 5B; and ii) revising the Reserve Sharing Group (RSG) definition for consistency with Reliability Standard Project 2022-01 Reporting ACE Definition and Associated Terms ("Project 2022-01").
- **Appendix 5A – Organization Registration and Certification Manual:** Making changes that conform with those in Appendix 5B and reducing legislative history.
- **Appendix 5B – Statement of Compliance Registry Criteria:** i) Adding GO-IBR and GOP-IBR as new functions to the Registry Criteria to register the unregistered IBRs; ii) clarifying the scope of registration in Section I of the Registry Criteria; iii) reducing legislative history; and iv) revising the RSG definition for consistency with Reliability Standard Project 2022-01.

---

[1] This proposal does not include distributed energy resources. Rather it only includes IBRs that are interconnected to the BPS. Nonetheless, NERC is reviewing potential impacts associated with DERs on the BPS.

Transmission Planning Energy Scenarios SAR

Action

Information

Background

The *2023 ERO Reliability Risk Priorities Report*[1] defines and prioritizes risks to the reliable performance of the bulk power system (BPS). The report highlighted the need to consider three transmission planning energy-related scenarios to mitigate risks to the BPS. To address these risks, the NERC Board of Trustees (during its November 16, 2022, meeting[2] and as part of 2023 work plan priorities) directed NERC to have the Standards Committee (SC) accept/authorize a standard authorization request (SAR). The fourth scenario addresses *cyber-informed transmission planning* that incorporates mitigating cyber security risks into transmission planning as a result of the NERC and Regional Entity white paper[3] on this topic. The objective is to modify the TPL-001-5.1[4] NERC Reliability Standard and/or create one or more new Reliability Standards focused on transmission planning analyses that apply energy-related scenarios that consider the following four areas of risk at minimum:

- Normal and extreme natural events[5]
- Natural gas/electricity interdependencies
- Distributed Energy Resource events
- Cyber-informed transmission planning

Summary

The transmission planning analyses will have specific cases called "benchmark events" for which multi-dimensional energy scenarios would be applied for study. When the modeled performance is results in cascading outages, uncontrolled separation, or instability, planners will develop a corrective action plan to mitigate the risk.

While this is a NERC and Regional Entity work product, the proposed SAR and Technical Justification was posted for a second time, which will end October 6, 2023. NERC and Regional staffs will consider comments before finalizing the two documents for presentation to the SC in November 2023. Once accepted by the SC, NERC Standards will determine the priority in relation to other Standards activities.

---

[1] https://www.nerc.com/comm/RISC/Related%20Files%20DL/RISC_ERO_Priorities_Report_2023_Board_Approved_Aug_17_2023.pdf

[2] https://www.nerc.com/AboutNERC/StrategicDocuments/2023_NERC_Work_Plan_Priorities_Board_Approved_November_16_2022.pdf

[3] Cyber-Informed Transmission Planning Roadmap for Integrating Cyber Security into Transmission Planning Activities, May 2023: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/ERO_Enterprise_Whitepaper_Cyber_Planning_2023.pdf.

[4] TPL-001-5.1 – Transmission System Planning Performance Requirements available at: https://www.nerc.com/pa/Stand/Reliability%20Standards/TPL-001-5.1.pdf.

[5] Extreme heat and cold weather events are being addressed by another initiative in response to FERC Docket RM22-10-000, Order No. 896, document number 2023-13286 at https://www.federalregister.gov/documents/2023/06/23/2023-13286/transmission-system-planning-performance-requirements-for-extreme-weather.

Standard Authorization Request (SAR) Focused on Transmission Planning Energy Scenarios

NERC Board of Trustees in its November 16, 2022 meeting directed NERC to submit a Standard Authorization Request (SAR) to the Standards Committee for authorization focused on transmission planning energy scenarios that shall consider the following at minimum:

- Normal and extreme events
- Gas-Electric interdependencies
- Distributed energy resource (DER) events

Transmission planning energy scenarios are a critical tool for ensuring the reliable and resilient operation of the electric grid. These scenarios provide a framework for understanding how the electric power system could evolve over time, taking into account a range of factors such as changes in technology, policy, and consumer behavior. By considering a range of possible futures, transmission planners can make informed decisions about how to build and operate the transmission system reliably to meet the needs of today and into the future.

One key benefit of energy scenarios is that they allow transmission planners to anticipate potential issues and develop strategies to address them before they occur. By considering a range of possible futures, transmission planners can identify potential risks and develop proactive and corrective action plans to mitigate them.

Team Composition

An ERO Enterprise team was formed to develop this SAR:

Name	Regional Entities/NERC
John Idzior	ReliabilityFirst
Neeraj Lal	NPCC
Gaurav Karandikar	SERC
Brad Woods	TexasRE
Dianlong Wang	MRO
Enoch Davies	WECC
Scott Barfield-McGinnis	NERC
Mohamed Osman	NERC
William Lamanna	NERC

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Transmission Planning Energy Scenarios

Mohamed Osman, Lead Engineer – Power System Analysis
Reliability and Security Technology Committee
September 20, 2023

RELIABILITY | RESILIENCE | SECURITY

Transmission Planning Energy Scenarios

- NERC Board of Trustees in its November 16, 2022 meeting directed NERC to submit a SAR for acceptance by the Standards Committee, focused on transmission planning energy scenarios that shall consider the following at minimum:
    - Normal and extreme events
    - Gas-Electric interdependencies
    - Distributed energy resource (DER) events
    - Cyber-Informed
- Order No. 896 – Extreme Heat and Cold
    - Effective June 23, 2023
    - Directive to complete by December 2024
    - Not specifically a part of this project, but could be addressed contemporaneously

What are Transmission Planning Energy Scenarios?

- Transmission planning energy scenarios refer to the process of ensuring adequate performance of the BPS for a given wide-area and analyzing potential future supply and demand scenarios:
  - Scenarios may include projections for electricity generation from different sources
  - Estimates of energy demand from various sectors
  - Assessments of potential changes in energy policies
  - Regulations
  - Technology advancements in how energy is generated or consumed

NERC TPL-001 Reliability Standard Review

- Does not explicitly define or require the study of energy scenarios
- There are no requirements for the study of extreme natural weather or other environmental events
- There is no consideration of a “wide-area” natural gas supply disruption or being curtailed during high demand
- Does not require the assessment of DER impacts to the BPS
- Does not require cyber-informed transmission planning approaches to mitigate reliability impacts that could result from cyberattacks

Related TPL Activities

Table 1: Related TPL Activities

Description		Fuel	Data	Energy Scenarios					Planning Models/Tools		Time Horizons (years)			CAP
Effort	Focus			Heat and Cold	Natural Events	Gas-Elec	DER	Cyber	Power Flow	Probabilistic	Ops (<1)	Near (1-5)	Long (6-10)	
TPL-001-5.1 (Extreme Only)	Performance during contingencies				X	X		X	X			X	X	
Energy Scenarios	Energy				X	X	X	X	X				X	X
Order No. 896	Energy			X					X				X	X
ERATF	Energy	X								X	X			
ERATF	Energy	X								X		X	X	
SPIDERWG	Data and parameters of DER		X						X			X	X	
SITES and SWG	Cyber security				Cyber-Informed Transmission Planning				X				X	X
Resource Adequacy	Forecasting and procurement to meet demand/load									X			X	

General Approach to the Scenarios

- Apply
  - Benchmark cases (steady-state & stability)
  - Energy scenarios
  - Sensitivity analyses
  - Model demand load response
- Benchmark Case Considerations
  - Wide-Area Impacts
  - Probabilistic Methods
  - Concurrent and correlated outages
  - Identify responsible entities
    - Coordination among entities and data sharing
- Method for Updating Cases
- Corrective Action

Normal and Extreme Natural Events

- Resource Variability – Major prior normal and extreme weather and/or meteorological projections:
  - Heat and cold temperature extremes
  - Solar and wind variability
  - Drought and flooding propensity
  - Fire and smoke propagation
  - Storms prone areas and other potential natural disasters and events
- Severe Weather Events:
  - Derechos, hurricanes, and tornadoes
  - Heat waves
  - Fires and cloud coverage
  - Winter storms

Natural Gas Interdependencies

- Gas Supply Disruptions
  - Pipeline maintenance
  - Severe weather events
  - Geopolitical tensions
- Electric Supply Disruptions
  - Electric power supply disruptions to the natural gas wellheads and compressor stations
  - Gathering and transport issues causing a reduction in flow/pressure below the level needed to operate BPS resources

Distributed Energy Resources

- High Penetration Scenarios
  - High consumer adoption
  - Variation of total power that is generated and consumed locally
  - Impacts other than "peak" and "off-peak"
- Variability and Intermittency
  - Gross/Net load swings
  - BPS balancing in real-time
- BPS Support
  - Transmission to Distribution (T-D)
  - Frequency response and reactive power
- Outage Scenarios
  - Weather events, equipment failures, common-mode loss, or other factors

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber-Informed

- CITPF enumerates thought processes for integrating cyber security concepts into transmission planning
- Mapping cyber security threats, vulnerabilities, and impacts to conventional transmission planning definitions using the following as a base set of starting contingencies
  - Outage of multiple BPS and non-BES) generators due to compromise of OEM
  - Outage of multiple DERs due to compromise of OEM
  - Outage of multiple BPS transmission substations due to compromise of devices through remote access capabilities
  - Outage of multiple Transmission to Distribution Interfaces due to compromised distribution control center
  - Outage of all DERs under control of a common DER aggregator

Standards Authorization Request (SAR)

- Scope
  - Establish benchmark event cases and energy scenarios
  - Define required performance criteria
  - Conduct studies and sensitivity analyses of assumptions
- Other Specific Considerations
  - Demand load response
  - Wide-area impacts and probabilistic methods
  - Concurrent and correlated outages
  - Periodicity for updating cases and refreshing studies
- Functional Entities
  - Identify specific responsible entities
  - Coordination among entities and data sharing
- Require Corrective Action Plans

Recommendation

Transmission Planning Suite

- TPL-001 (Planning)
- TPL-007 (GMD)
- Normal and Extreme Natural Events
- Gas-Electric Interdependencies
- Distributed Energy Resources
- Cyber-Informed Transmission Planning

Conclusion

- Benchmark energy scenario planning is needed for:
    - Normal and extreme natural events
    - Electric-gas interdependencies
    - DER impacts imposed on the BPS
    - Informed cyber issues related to cyberattacks
- Approach can be similar to TPL-007 (Geomagnetic Disturbance)
- Schedule
    - Comment Period August 22 – October 6
        - ○ Draft Technical Justification
        - ○ Draft SAR
    - Presentation to the SC – November 15
- Acknowledgements
    - ERO-Enterprise staff

Questions and Answers

Agenda Item 19
RSTC Meeting
September 20, 2023

Interregional Transfer Capability Study (ITCS)

Action

Information

Background

Congress passed the Fiscal Responsibility Act of 2023, which included a provision for NERC to conduct a study on the reliable transfer of electric power between neighboring transmission planning areas. NERC, in consultation with the Regional Entities and industry stakeholders, will conduct transfer capabilities studies for regional transmission areas in the United States and recommend transfer capability enhancements needed for reliability.

Who: NERC, in consultation with each Regional Entity and each transmitting utility in a neighboring transmission planning region.

What: A study of total transfer capability between transmission planning regions. In accomplishing this work, the study should include:

- "Current total transfer capability, between each pair of neighboring transmission planning regions."
- "A recommendation of prudent additions to total transfer capability between each pair of neighboring transmission planning regions that would demonstrably strengthen reliability within and among such neighboring transmission planning regions"; and
- "Recommendations to meet and maintain total transfer capability together with such recommended prudent additions to total transfer capability between each pair of neighboring transmission planning regions."

When: NERC must file with FERC within 18 months of enactment of the bill. Public comment period will occur when FERC publishes the study in the Federal Register. After submittal, FERC must provide a report to Congress within 12 months of closure of the public comment period with recommendations (if any) for statutory changes.

ERO study filing deadline: On or before December 2, 2024

Project Goals and Objectives

- Conduct a comprehensive study of existing interregional transfer capability across the United States (between each transmission planning region) to assess currently available transfer capability between neighboring areas and the future need for additional transfer capacity to ensure reliability under various system conditions including extreme weather
- Provide reliable and data-driven recommendations for "prudent" additions to the amount of electric power that can be moved or transferred between neighboring transmission planning regions
- Recommend approaches to achieve and maintain an adequate level transfer capability.

- Engage stakeholders and gather inputs, assumptions, and conditions from Regional Entities, industry, and the ITCS Stakeholder Advisory Group to ensure a comprehensive and inclusive study
- Identify expectations for next steps and continuing analysis to reinforce the Long-Term Reliability Assessment

General Approach

1. **Engage Executive Leadership Group:** For ERO-wide strategic leadership, concurrence on study design and approaches, and support for the project manager of this project. Form ERO project team that will be responsible for developing the overall project execution strategy, monitoring, and overseeing the project progress.
2. **Collaborate with Regional Entities and industry to collect necessary data and information:** Work closely with Regional Entities and industry stakeholders to gather relevant data, build system models, and reports required for the study. Develop input assumptions, including loads, resources, transmission topology, extreme weather conditions utilizing external consulting and industry expertise.
3. **Engage a Stakeholder Advisory Group composed of representation from all planning areas to gather inputs and ensure a comprehensive study:** Form a Stakeholder Advisory Group consisting of representatives from all planning areas to provide insights, expertise, and inputs to the study, study scope, and study results.
4. **Conduct comprehensive analysis and modeling of interregional transfer capability:** Perform detailed analysis and modeling of the transmission systems to assess the current and potential transfer capability between neighboring areas. Assumptions will need to be internally consistent and consider scenarios and conditions that impact long-distance power transfers. The study will also consider factors such as generation mix, load growth projections, various high-risk scenarios, and emerging environmental policy in the study.
5. **Evaluate existing transmission infrastructure, system constraints, and potential areas for improvement:** Assess the current transmission infrastructure, identifying system constraints, and identifying opportunities for improvement to enhance interregional transfer capability.
6. **Identify potential reliability challenges and propose solutions to enhance interregional transfer capability:** Identify existing transfer capability between transmission planning areas, potential reliability challenges associated with interregional transfers and recommendations to address them.
7. **Develop a final report with actionable recommendations for enhancing interregional transfer capability:** Compile all study findings, analysis, and stakeholder inputs into a comprehensive final report that provides actionable recommendations for improving interregional transfer capability based on a quantifiable and objective metric and criteria.

Deliverables and Schedule

1. **Finalized Study Framework:** Describes the overall framework and governance of the project, general scoping, objectives, and roles and responsibilities.
2. **Interim Progress Reports:** Regular updates on project milestones, findings, and emerging recommendations. (September 2023, then quarterly)

3. **Draft Study Report:** A preliminary report shared with stakeholders for review and feedback. (June 2024)
4. **Final Study Report:** A comprehensive report outlining the study method, findings, recommendations, and supporting analysis. (November 2024)

Agenda Item 20
RSTC Meeting
September 20, 2023

RSTC Charter Revisions

Action

Request comments.

Attachment 1: Clean Charter
Attachment 2: Redline Charter

Background

In November 2019, the NERC Board of Trustees (Board) approved creation of the Reliability and Security Technical Committee (RSTC) to replace the former Operating, Planning and Critical Infrastructure Protection committees to improve effectiveness and efficiency of the technical committees. The Board also approved the initial RSTC charter. In September 2021, the RSTC approved initial Charter revisions. The Board approved such revisions in November 2021. Every two years, the RSTC examines Charter revisions are appropriate. The latest biannual review identified certain administrative and clarifying improvements that would further support efficient operation of the committee.

Summary

The following clean and redline version of the Charter reflects administrative improvements and clarifications based on lessons learned over the past two years. In particular, these revisions reflect the following:

- Section 2 (RSTC Functions): Reference to the RSTC's efforts to prioritize work streams and reflect the RSTC's plan to present annual updates to the Strategic Plan at the Board's February Meeting.
- Section 3 (Membership):
  - Reflect that the outgoing chair may remain a non-voting member of the RSTC for one year to support continuity.
  - Reflect that for purposes of the Nominating Subcommittee (NS), the RSTC vice-chair shall recuse him/herself: (a) unless not seeking reelection; and (b) until the NS has voted to recommend the vice-chair for election to the chair position.
  - Clarify member terms in light of the RSTC's transition from the prior committee structure.
  - Clarify that a change in employment does not automatically require a member's resignation.

  Section 5 (Officers and Executive Committee): Reflect that the chair and vice-chair shall evaluate composition of the Executive Committee within six months of election.
- Section 6 (Subordinate Groups)
  - Clarify that subordinate groups shall seek officers from NERC membership sectors 1 through 12 to support sufficient expertise and diversity.
  - Reference the NERC Antitrust Guidelines and Participant Conduct Policy.

    - Fine tune language associated with review as to whether a Working Group or Task Force should be transitioned to a Subcommittee or Working Group respectively.
- Section 8 (RSTC Deliverables and Approval Processes):
    - Clarify expectations around RSTC deliverables (including Whitepapers and Standard Authorization Requests) to reflect the expectations posted on the RSTC webpage.
    - Recognize that after RSTC endorsement of any SAR, NERC Staff shall coordinate with the Standards Committee.

NERC Staff requests comments on the RSTC Charter over the next 30 days to facilitate final revisions for presentation to the Committee at its December Meeting. If approved by the RSTC, the updated Charter would be presented to the NERC Board at its Meeting in February of 2024.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability and Security Technical Committee Charter

~~November 2021~~February 2024

Approved by the NERC Board of Trustees: ~~November 4, 2021~~[TBD]

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities, is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is ~~divided into~~made up of six Regional Entities ~~boundaries~~ as shown ~~in~~ on the map and in the corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners/Operators participate in another.

MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	~~Western Electricity Coordinating Council~~WECC

Section 1: Purpose

The Reliability and Security Technical Committee (RSTC) is a standing committee that strives to advance the reliability and security of the interconnected BPS of North America by:

- Creating a forum for aggregating ideas and interests, drawing from diverse industry stakeholder expertise, to support the ERO Enterprise's mission;
- Leveraging such expertise to identify solutions to study, mitigate, and/or eliminate emerging risks to the BPS for the benefit of industry stakeholders, the NERC Board of Trustees (Board) and ERO Enterprise staff and leadership; and,
- Overseeing the implementation of subgroup work plans that drive risk-mitigating technical solutions.

Section 2: RSTC Functions

Create a forum for industry stakeholders to support NERC programs in the development of key ERO Enterprise deliverables.

- Facilitate and advocate information sharing among relevant industry stakeholders;
- Review and provide guidance in developing deliverables critical to ERO functions, such as Reliability Standards, reliability assessments, requests for data (pursuant to Section 1600 of the NERC Rules of Procedure Section (ROP)), Implementation Guidance, and other analyses, guidelines, and reports;
- Solicit and coordinate technical direction, oversight activities, and feedback from industry stakeholders;
- Disseminate ERO deliverables to industry to enhance reliability;
- Develop internal and review external requests for industry actions and informational responses;
- Develop appropriate materials, as directed by ERO functions or the NERC Board, to support ERO Enterprise functions; and,
- Coordinate with ERO staff and liaise with government agencies and trade associations.
- Provide technical input and analyses on operating and planned BPS reliability and security, emerging issues and risks, and other general industry concerns at the request of the NERC Board or NERC staff.

Develop a two-year strategic work plan to guide the deliverables of the RSTC and ensure appropriate prioritization of activities.

- Ensure alignment of the strategic work plan with NERC priorities,~~ERO~~ reports and analyses, including the NERC Business Plan and Budget, ERO Enterprise Long-Term Strategy, ~~Operating Plan~~, biennial Reliability Issues Steering Committee (RISC) ERO Reliability Risk Priorities report, State of Reliability report recommendations, Long-Term, Seasonal and Special Reliability Assessment recommendations and ongoing event analysis trends;
- Coordinate the objectives in the strategic work plan with the Standing Committees Coordinating Group; and,
- Obtain annual NERC Board approval. The RSTC will target presenting the strategic work plan to the Board at its February meeting, at the same time that the RSTC presents the full RSTC membership list in accordance with Section III below.

Coordinate and oversee implementation of RSTC subgroup work plans.

- Assign an RSTC member sponsor, as necessary, to subgroups to ensure alignment with RSTC schedules, processes, and strategic goals.
- Create and disband subcommittees, working groups and task forces to support ERO Enterprise functions;
- Harmonize and approve the work plans of subcommittees, working groups, and task forces with the strategic work plan; and,
- Track the progress of the subcommittees, working groups, and task forces to ensure that they complete assigned activities as outlined in their work plans and in alignment with the RSTC strategic work plan.

Advise the NERC Board of Trustees.

- Update the NERC Board semi-annually on progress in executing the strategic work plan; and,
- Present appropriate deliverables to the NERC Board.

Section 3: Membership

Representation Model

The RSTC has a hybrid representation model consisting of the following types of memberships:

- Sector members;
- At-large members; and,
- Non-voting members.

Two members shall be elected to each of the following membership sectors:

- Sector 1 - Investor-owned Utility;
- Sector 2 – State or Municipal Utility;
- Sector 3 - Cooperative Utility;
- Sector 4 - Federal or Provincial Utility/Power Marketing Administration;
- Sector 5 - Transmission-Dependent Utility;
- Sector 6 - Merchant Electricity Generator;
- Sector 7 - Electricity Marketer;
- Sector 8 - Large End Use Electricity Customer;
- Sector 9 - Small End Use Electricity Customer;
- Sector 10 - ISO/RTO; and,
- Sector 12 - Government Representatives.

Selection of at-large members will allow for better balancing of representation on the RSTC of the following:[1]

- Regional Entity and Interconnection diversity (i.e., goal of having at least one representative from each Interconnection and Regional Entity footprint);
- Subject matter expertise (Planning, Operating, or Security);
- Organizational types (Cooperatives, Investor-Owned Utilities, Public Power, Power Marketing Agencies, etc.); and,
- North American countries, consistent with the NERC bylaws (Canada, Mexico, and U.S.).

Upon expiration of his or her term as chair, the outgoing chair may remain a non-voting member of the RSTC for one year, in the interest of continuity.

Below is a breakdown of voting and non-voting membership on the RSTC:

Voting Membership	
Name	**Voting Members**
Sectors 1-10 and 12	22
At-Large	10

---

[1] *See,* NERC Sector 13 in the NERC Bylaws (2021).

Voting Membership	
Name	**Voting Members**
Chair and Vice-~~-~~Chair	2
Total	**34**

Non-Voting Membership[2]	
Non-Voting Member	**Number of Members**
NERC Secretary	1
United States Federal Government	2
Canadian Federal Government	1
Provincial Government	1
Former Chair	1
Total	**6~~5~~**

Member Selection

RSTC members are not required to be from organizations who are NERC members.

Members are appointed to the RSTC upon approval of the NERC Board and serve on the RSTC at the pleasure of the NERC Board.

1. **Affiliates**

   A company, including its affiliates, may not have more than one member on the RSTC. Any RSTC member who is aware of a membership conflict of this nature is obligated to notify the RSTC secretary within 10 business days. The RSTC secretary will in turn report the conflict to the RSTC chair.

   Members impacted by such a conflict, such as through a merger of organizations, must confer among themselves to determine which member should resign from the RSTC and notify the secretary and chair; however, if they cannot reach an amicable solution to determine who will remain, the Nominating Subcommittee will review the qualifications of each member and make a recommendation to the NERC Board for final approval.

2. **Election of Sector Members**

   NERC members in each sector will annually elect members for expiring terms or open seats using a nomination and election process that is open, inclusive, and fair. In the event that a sector has no nominations for one or both sector seats at the annual election, the RSTC will convert those empty sector seats to at-large seats until the end of the term.

   Sector elections will be completed in time for the Nominating Subcommittee to identify and nominate at-large representatives as well as for the secretary to send the full RSTC membership list to the NERC Board for approval at its annual February meeting.

   If an interim vacancy is created in a sector, a special election will be held unless it would coincide with the annual election process. If a sector cannot fill an interim vacancy, then that sector seat will remain vacant until the next annual election. Interim sector vacancies will not be filled with an at-large representative.

3. **Nominating Subcommittee**

---

[2] Upon recognition of NERC as the ERO, Mexican Government representation will be equitable and based approximately on proportionate Net Energy for Load.

The Nominating Subcommittee (RSTC NS) will consist of seven (7) members (the RSTC v~~V~~ice-c~~C~~hair and six (6) members drawing from different sectors and at-large representatives). Apart from the ~~V~~vice-c~~C~~hair, members of the RSTC Executive Committee (RSTC EC) shall not serve on the RSTC NS.

The NS members are nominated by the RSTC chair and voted on by the full RSTC membership.

The term for members of the NS is one (1) year.

The RSTC NS is responsible for (a) recommending individuals for at-large representative seats, and, (b) managing the process to select the chair and/or vice-~~-~~chair of the RSTC. The RSTC vice-chair shall recuse him or herself from this process (a) unless he or she is not seeking re-election, and, (b) until the RSTC NS has concluded a vote to recommend the vice-chair for subsequent RSTC election to the ~~-~~ chair position. At-large members on the RSTC NS shall recuse themselves from recommendations for at-large representative seats if they are seeking reappointment.

4. **Selection of At-Large Members**

The RSTC NS solicits and reviews nominations from the full RSTC and industry to fill at-large representative seats. After reaching consensus, the RSTC NS submits a recommended slate of at-large candidates to the Board at its annual February meeting for approval. To the extent practicable, the RSTC NS will balance the following criteria to select at-large members: (a) geographic diversity from all Interconnections and ERO Enterprise Regional Entities; (b) high-level understanding and perspective on reliability risks based on experience at an organization in a sector; and, (c) experience and expertise from an organization in the sector relevant to the RSTC.

The Board votes to appoint the at-large members.

5. **Non-Voting Members**

At the start of the annual RSTC nomination process the RSTC secretary will coordinate with entities entitled to non-voting membership to identify representatives for the non-voting seats.

6. **International Representation**

International representation on the RSTC shall be consistent with Article VIII Section 4 of the NERC Bylaws.

Member Expectations

RSTC members and the RSTC's subordinate groups are expected to act in accordance with this charter, as well as to accomplish the following:

- Adhere to NERC Antitrust Guidelines[3] and Participant Conduct Policy[4];
- Demonstrate and provide knowledge and expertise in support of RSTC activities;
- Where applicable, solicit comments and opinions from constituents and groups of constituents or trade organizations represented by the member and convey them to the RSTC;
- Respond promptly to all RSTC requests, including requests for reviews, comments, and votes on issues before the RSTC; and,
- During meetings, comply with the procedures outlined for that meeting and identified in this Charter. .

---

[3] https://www.nerc.com/pa/Stand/Resources/Documents/NERC_Antitrust_Compliances_Guidelines.pdf

[4] https://www.nerc.com/gov/Annual%20Reports/NERC_Participant_Conduct_Policy.pdf

Sponsor Expectations

Sponsors are expected to act in accordance with this charter, as well as to accomplish the following:

- Understand and advance the expectations of the RSTC, not those of their sector or other interest group;
- Assure that recommendations and action plans are designed for implementation;
- Support the subgroup Chair and Vice-Chair in seeing the big picture without directing the activities of the subgroup; and,
- Liaise with the RSTC.

Member Term

~~When the initial staggered, two- and three-year terms of RSTC members have expired , all subsequent terms~~Members shall serve a term of ~~will be~~ two years.

An RSTC member may serve a term shorter than two (2) years if:

- Two (2) members are simultaneously selected to a sector that did not have any existing members, in order to stagger their terms, one member will be assigned a one-year term and the second member will be assigned a two-year term.
- A member is selected to fill a vacant member seat between elections, the term will end when the term for that vacant seat ends.

There are no limits on the number of terms that members can serve.

Vacancies and Proxies

Membership vacancies may be filled between annual elections using the aforementioned selection process.

1. **Vacancies Created by the Member**

   In the event a member can no longer serve on the RSTC, that member will submit a written resignation to the RSTC chair or the secretary. A change in employment does not automatically require a member's resignation, if the member remains eligible to serve the membership sector he/she was elected to, and will be evaluated on a case-by-case basis.

2. **Vacancies Requested by the Chair**

   The chair may request any RSTC member who ceases to participate in the RSTC consistent with member expectations (above) and to the satisfaction of the chair, to submit a resignation or to request continuation of membership with an explanation of extenuating circumstances. If a written response is not received within 30 days of the chair's request, the lack of response will be considered a resignation. If the chair is not satisfied with a written response, the RSTC chair will refer the matter to the NERC Board.

3. **Vacancies Requested by the Board**

   RSTC members serve at the pleasure of the NERC Board. The NERC Board may initiate a request for resignation, removal, or replacement a member from the RSTC, as it deems appropriate or at the request of the RSTC chair.

4. **Proxies**

A voting member may select a proxy who attends and votes during all or a portion of a committee meeting in lieu of a voting member, provided that the absent voting representatives notifies the RSTC chair, vice chair, or secretary of the proxy. A proxy may not be given to another RSTC member. A proxy must meet the RSTC's membership eligibility requirements, including affiliate restrictions.

To permit time to determine a proxy's eligibility, all proxies must be submitted to the secretary in writing at least one week prior to the meeting (electronic transmittal is acceptable) for approval by the chair. Any proxy submitted after that time will be accepted at the chair's discretion.

Section 4: Meetings

Open meetings will be conducted in accordance with this Charter. The Chair may consult Robert’s Rules of Order for additional guidance.

Quorum

The quorum necessary for transacting business at meetings of the RSTC is two-thirds of the voting members currently on the RSTC’s roster and is determined once at each meeting.

If a quorum is not determined, the RSTC may not take any actions requiring a vote; however, the chair may allow discussion of the agenda items.

Voting

Actions by the RSTC will be approved upon receipt of the affirmative vote of two-thirds of the votes cast at any meeting at which a quorum is present. An abstention (“present” vote) does not count as a vote cast.

Voting may take place during regularly scheduled in-person meetings,~~,~~ via electronic mail, or via conference call/virtual meeting.

Refer to Section 7 for voting procedures.

Executive, Open and Closed Sessions

The RSTC and its subordinate groups hold~~s~~ meetings open to the public, except as noted herein. Although meetings are open, only voting members may offer and act on motions.

All meetings of the Executive Committee and the RSTC NS shall be conducted in closed session.

The chair may also hold closed sessions in advance of the open meeting with limited attendance based on the confidentiality of the information to be disclosed at the meeting. Such limitations should be applied sparingly and on a non-discriminatory basis. Any discussion of confidential information in a closed session shall be consistent with Section 1500 of the NERC ROP.[5]

Majority and Minority Views

All members of a committee will be given the opportunity to provide alternative views on an issue. The results of committee actions, including recorded minutes, will reflect the majority as well as any minority views of the committee members.

Action without a Meeting

Any action required or permitted at a meeting of the committee may be taken without a meeting at the request of the chair.

Such action without a meeting will be performed by electronic ballot (e.g., telephone, email, or Internet survey) and considered a roll call ballot. The secretary will announce the action required at least five business days before the date on which voting commences. As time permits, members should be allowed a window of ten (10) business days

---

[5] Section 1500 of the NERC ROP - https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/NERC%20ROP%20(With%20Appendicies).pdf

to vote. The secretary will document the results of such an action within ten (10) business days of the close of the voting period. Such action must meet the regular meeting quorum and voting requirements above.

Section 5: Officers and Executive Committee

Officers

The RSTC will have two officers – one chair and one vice-chair.

Officers shall be selected as follows:

- The RSTC NS solicits nominations for chair and vice-chair through an open nomination process. Self-nominations are permitted during the open nomination period.
- At the close of the nomination period, the RSTC NS will propose a chair and a vice-chair candidate. The full RSTC will elect the chair and vice chair.
- The chair and vice chair must be a committee member and shall not be from the same sector.
- The elected chair and vice-chair are appointed by the NERC Board.
- No individual may serve more than one term as vice chair and one term as chair unless an exception is approved by the Board.

Upon expiration of his or her term as chair, the outgoing chair may remain a non-voting member of the RSTC for one year, in the interest of continuity.

Secretary

NERC will appoint the RSTC secretary.

A member of the NERC staff will serve as the secretary of the RSTC. The secretary will do the following:

- Manage the day-to-day operations and business of the RSTC;
- Prepare and distribute notices of the RSTC meetings, prepare the meeting agenda, and prepare and distribute the minutes of the RSTC meetings;
- Facilitate the election/selection process for RSTC members; and,
- Act as the RSTC's parliamentarian.

Chair

The chair will direct and provide general supervision of RSTC activities, including the following:

- Coordinate the scheduling of all meetings, including approval of meeting duration and location;
- Develop agendas and rule on any deviation, addition, or deletion from a published agenda;
- Preside at and manage meetings, including the nature and length of discussion, recognition of speakers and proxies, motions, and voting;
- Act as spokesperson for the RSTC at forums inside and outside of NERC; and,
- Attend meetings of the NERC Board when necessary to report on RSTC activities.

Vice Chair

The vice chair will assume the responsibilities of the chair under the following conditions:

- At the discretion of the chair (for brief periods of time);

- When the chair is absent or temporarily unable to perform the chair's duties; or,
- When the chair is permanently unavailable or unable to perform the chair's duties. In the case of a permanent change, the vice chair will continue to serve until a new chair is nominated and appointed by the NERC Board.

Executive Committee

The RSTC EC shall consist of six (6) members:

- Chair;
- Vice-chair;
- Four (4) RSTC voting members selected by the RSTC chair and vice-chair with a reasonable balance of subject matter expertise in Operations, Planning, and/or Security and with consideration for diversity in representation (i.e., sectors, Regional Entities, Interconnections, etc.).
  - The RSTC chair and vice-chair shall evaluate composition of the RSTC EC within six months of their election as officers for the appropriate balance of technical expertise, geographical representation, and tenure.

The RSTC EC of the RSTC is authorized by the RSTC to act on its behalf between regular meetings on matters where urgent actions are crucial and full RSTC discussions are not practical. The RSTC shall be notified of such urgent actions taken by the RSTC EC within a week of such actions.~~–~~ These actions shall also be included in the minutes of the next open meeting.

Ultimate RSTC responsibility resides with its full membership whose decisions cannot be overturned by the EC. The RSTC retains the authority to ratify, modify, or annul RSTC EC actions.

After general solicitation from RSTC membership, the RSTC EC will appoint any sponsors of subgroups.

Section 6: RSTC Subordinate Groups

The RSTC organizational structure will be aligned as described by the NERC Bylaws to support a superior-subordinate hierarchy.

The RSTC may establish subcommittees, working groups, and task forces as necessary. The RSTC will be the responsible sponsor of all subordinate subcommittees, working groups, or task forces that it creates, or that its subordinate subcommittees and working groups may establish.

Officers of subordinate groups will be appointed by the chair of the RSTC. Where feasible, officers shall be selected from individuals employed at entities within NERC membership sectors 1 through 12 to support sufficient expertise and diversity in execution of the subordinate group's responsibilities.

Subcommittees, working groups, and taskforces will conduct business in a manner consistent with all applicable sections of this Charter, including the NERC Antitrust Guidelines[6] and Participant Conduct Policy[7].

Subcommittees

The RSTC may establish subcommittees to which the RSTC may delegate some of RSTC's functions. The RSTC will approve the scope of each subcommittee it forms. The RSTC chair will appoint the subcommittee officers (typically a chair and a vice chair) for a specific term (generally two years). The subcommittee officers may be reappointed for up to two additional terms. The subcommittee will work within its assigned scope and be accountable for the responsibilities assigned to it by the committee. The formation of a subcommittee, due to the permanency of the subcommittee, will be approved by the NERC Board.

Working Groups

The RSTC may delegate specific continuing functions to a working group. The RSTC will approve the scope of each working group that it forms. The RSTC chair will appoint the working group officers (typically a chair and a vice chair) for a specific term (generally two (2) years). The working group officers may be reappointed for one (1) additional term. The RSTC will conduct a "sunset" review of each working group every year. The working group will be accountable for the responsibilities assigned to it by the RSTC or subcommittee and will, at all times, work within its assigned scope. The RSTC should consider ~~promoting~~ transitioning to a subcommittee any working group that is required to work longer than two~~one~~ terms.

Task Forces

The RSTC may assign specific work to a task force. The RSTC will approve the scope of each task force it forms. The RSTC chair will appoint the task force officers (typically a chair and a vice chair). Each task force will have a finite duration, normally less than one year. The RSTC will review the task force scope at the end of the expected duration and review the task force's execution of its work plan at each subsequent meeting of the RSTC until the task force is retired. Action of the RSTC is required to continue the task force past its defined duration. The RSTC should consider ~~promoting~~ transitioning to a working group any task force that is required to work longer than two~~one~~ years.

---

[6] https://www.nerc.com/pa/Stand/Resources/Documents/NERC_Antitrust_Compliances_Guidelines.pdf

[7] https://www.nerc.com/gov/Annual%20Reports/NERC_Participant_Conduct_Policy.pdf

Section 7: Meeting Procedures

Voting Procedures for Motions

In-Person

- The default procedure is a voice vote.
- If the chair believes the voice vote is not conclusive, the chair may call for a show of hands.
- The chair will not specifically ask those who are abstaining to identify themselves when voting by voice or a show of hands. If the chair desires a roll call, the secretary will call each member's name.

  Members answer "yes," "no," or "present" if they wish to abstain from voting. As provided above, an abstention does not count as a vote cast.

Conference Call / Virtual[8]

- All voting shall default to being conducted through use of a poll.
- Where a need to record each member's vote is requested or identified, the RSTC may conduct voting via a roll call vote.

Commented [CC1]: Question for RSTC EC:

Consider fully virtual / fully in person approach

In-Person only for voting?

Minutes

- Meeting minutes are a record of what the committee did, not what its members said.
- Minutes should list discussion points where appropriate, but should usually not attribute comments to individuals. It is acceptable to cite the chair's directions, summaries, and assignments.
- All Committee members are afforded the opportunity to provide alternative views on an issue. The meeting minutes will provide an exhibit to record minority positions.

---

[8] Virtual meetings include those where virtual attendance is possible, such as a fully or partially virtual meeting.

Section 8: RSTC Deliverables and Approval Processes

The RSTC will abide by the following to approve, endorse, or accept committee deliverables.

Reliability Guidelines, Security Guidelines and Technical Reference Documents

Reliability Guidelines, Security Guidelines, and Technical Reference Documents suggest approaches or behavior in a given technical area for the purpose of improving reliability. Reliability Guidelines and Security Guidelines are not binding norms or mandatory requirements. Reliability Guidelines and Security Guidelines may be adopted by a responsible entity in accordance with its own facts and circumstances.

1. **New/updated draft guideline approved for industry posting.**

   The RSTC accepts for posting for industry comment (i) the release of a new or updated draft guideline developed by one of its subgroups or the committee as a whole; or (ii) the retirement of an existing guideline.

   The draft guideline or retirement is posted as "for industry-wide comment" for 45 days. If the draft guideline is an update, a redline version against the previous version must also be posted.

   After the public comment period, the RSTC will post the comments received as well as its responses to the comments. The RSTC may delegate the preparation of responses to a committee subgroup.

   A new or updated guideline which considers the comments received, is approved by the RSTC and posted as "Approved" on the NERC website. Updates must include a revision history and a redline version against the previous version.

   After posting a new or updated guideline, the RSTC will continue to accept comments from the industry via a web-based forum where commenters may post their comments.

   a. Each quarter, the RSTC will review the comments received.

   b. At any time, the RSTC may decide to update the guideline based on the comments received or on changes in the industry that necessitate an update.

   c. Updating an existing guideline will require that a draft updated guideline be posted and approved by the RSTC in the above steps.

2. **Review of Approved Reliability Guidelines, Security Guidelines and Technical Reference Documents**

   Approved Reliability Guidelines or Technical Reference Document shall be reviewed for continued applicability by the RSTC at a minimum of every third year since the last revision.

3. **Communication of New/Revised Reliability Guidelines, Security Guidelines and Technical Reference Documents**

   In an effort to ensure that industry remains informed of revisions to a Reliability Guideline or Technical Reference Document or the creation of a new Reliability Guideline or Technical Reference Document, the RSTC subcommittee responsible for the Reliability Guideline will follow an agreed upon process. Reliability Guidelines, Security Guidelines, and Technical Reference Documents shall be posted on the RSTC website.

4. **Coordination with Standards Committee**

   Standards Committee authorization is required for a Reliability Guideline or Security Guidelines to become a supporting document that is posted with or referenced from a NERC Reliability Standard. See Appendix 3A in the NERC's ROP under "Supporting Document."

Section 1600 Data or Information Requests[9]

A report requested by the RSTC that accompanies or recommends a Rules of Procedure (ROP) Section 1600 - Data or Information Request will follow the process outlined below:

1. This Section 1600 request, with draft supporting documentation, will be provided to the RSTC at a regular meeting.
2. The draft Section 1600 data request and supporting documentation will be considered for authorization to post for comments at the RSTC regular meeting.
3. A committee subgroup will review and develop responses to comments on the draft Section 1600 data request and will provide a final draft report, including all required documentation for the final data request, to the RSTC at a regular meeting for endorsement.
4. The final draft of the 1600 data request – with responses to all comments and any modifications made to the request based on these comments – will be provided to the NERC Board.

Other Types of Deliverables

1. **Policy Outreach**

   On an ongoing basis, the RSTC will coordinate with the forums, policymakers, and other entities to encourage those organizations to share reliability guidelines, technical reference documents and lessons learned to benefit the industry.

   Reports required under the NERC ROP or as directed by an Applicable Governmental Authority or the NERC Board: documents include NERC's long-term reliability assessment, special assessments, and probabilistic assessments. These reports may also be used as the technical basis for standards actions and can be part of informational filings to FERC or other government agencies.

2. **White Papers**

   Documents that explore technical facets of topics, ~~often~~ making recommendations for further action. They may be written by subcommittees, working groups, or task forces of their own volition, or at the request of the RSTC. Where feasible, a white paper recommending potential development of a standard authorization request (SAR) shall be posted for comment on the RSTC website. White papers will be posted on the RSTC webpage, after RSTC approval.

3. **Technical Reference Documents and Technical Reports**

   Documents that serve as a reference for the electric utility industry and/or NERC stakeholders regarding a specific topic of interest. These deliverables are intended to document industry practices or technical concepts at the time of publication and may be updated as deemed necessary, per a recommendation by the RSTC or its subgroups to reflect current industry practices. Technical reference documents and reports will be posted on the RSTC webpage, after RSTC approval.

4. **Implementation Guidance**

   Documents providing examples or approaches for registered entities to comply with standard requirements. The RSTC is designated by the ERO Enterprise as a pre-qualified organization for vetting Implementation Guidance in accordance with NERC Board -approved Compliance Guidance Policy. Implementation Guidance that is endorsed by the RSTC can be submitted to the ERO Enterprise for endorsement, allowing for its use in Compliance Monitoring and Enforcement Program (CMEP) activities.

5. **Standard Authorization Requests (SAR)**

---

[9] Section 1600 of the NERC ROP - https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/NERC%20ROP%20(With%20Appendicies).pdf. This process only applies to Section 1600 requests developed by the RSTC and its subordinate groups.

A form used to document the scope and reliability benefit of a proposed project for one or more new or modified Reliability Standards or definitions or the benefit of retiring one or more approved Reliability Standards.

Any entity or individual, including NERC Committees or subgroups and NERC Staff, may propose the development of a new or modified Reliability Standard. A SAR prepared by a subordinate group of the RSTC must be endorsed by the RSTC prior to presentation to the Standards Committee. Each SAR should be accompanied by a technical justification that includes, at a minimum, a discussion of the reliability-related benefits and costs of developing the new Reliability Standard or definition, and a technical foundation document (e.g., research paper) to guide the development of the Reliability Standard or definition. The technical foundation document should address the engineering, planning and operational basis for the proposed Reliability Standard or definition, as well as any alternative approaches considered to SAR development.

RSTC endorsement of a SAR supports: (a) initial vetting of the technical material prior to the formal Standards Development Process, and, (b) that sound technical justification has been developed, and the SAR will not be remanded back to the RSTC to provide such justification per the Standard Processes Manual.

After endorsement of any SAR, NERC Staff shall coordinate with the Standards Committee.

Review Process for other Deliverables

Deliverables with a deadline established by NERC management or the NERC Board will be developed based on a timeline reviewed by the RSTC to allow for an adequate review period, without compromising the desired report release dates. Due to the need for flexibility in the review and approval process, timelines are provided as guidelines to be followed by the committee and its subgroups.

A default review period of no less than 10 business days will be provided for all committee deliverables. Requests for exceptions may be brought to the RSTC at its regular meetings or to the RSTC EC if the exception cannot wait for an RSTC meeting.

In all cases, a final report may be considered for approval, endorsement, or acceptance if the RSTC, as outlined above, decides to act sooner.

Actions for Deliverables

1. **Approve:**

   The RSTC has reviewed the deliverable and supports the content and development process, including any recommendations.

2. **Accept:**

   The RSTC has reviewed the deliverable and supports the development process used to complete the deliverable.

3. **Remand:**

   The RSTC remands the deliverable to the originating subcommittee, refer it to another group, or direct other action by the RSTC or one of its subcommittees or groups.

4. **Endorse:**

The RSTC agrees with the content of the document or action, and recommends the deliverable for the approving authority to act on. This includes deliverables that are provided to the RSTC by other NERC committees. RSTC endorsements will be made with recognition that the deliverable is subject to further modifications by NERC Executive Management and/or the NERC Board. Changes made to the deliverable subsequent to RSTC endorsement will be presented to the RSTC in a timely manner. If the RSTC does not agree with the deliverable or its recommendations, it may decline endorsement. It is recognized that this does not prevent an approval authority from further action.