NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

MIDWEST RELIABILITY ORGANIZATION

NPCC, Inc.

RELIABILITY FIRST

SERC

TEXAS RE
Ensuring electric reliability for Texans

WECC

Cyber-Informed Transmission Planning

Roadmap for Integrating Cyber Security into Transmission Planning Activities

May 2023

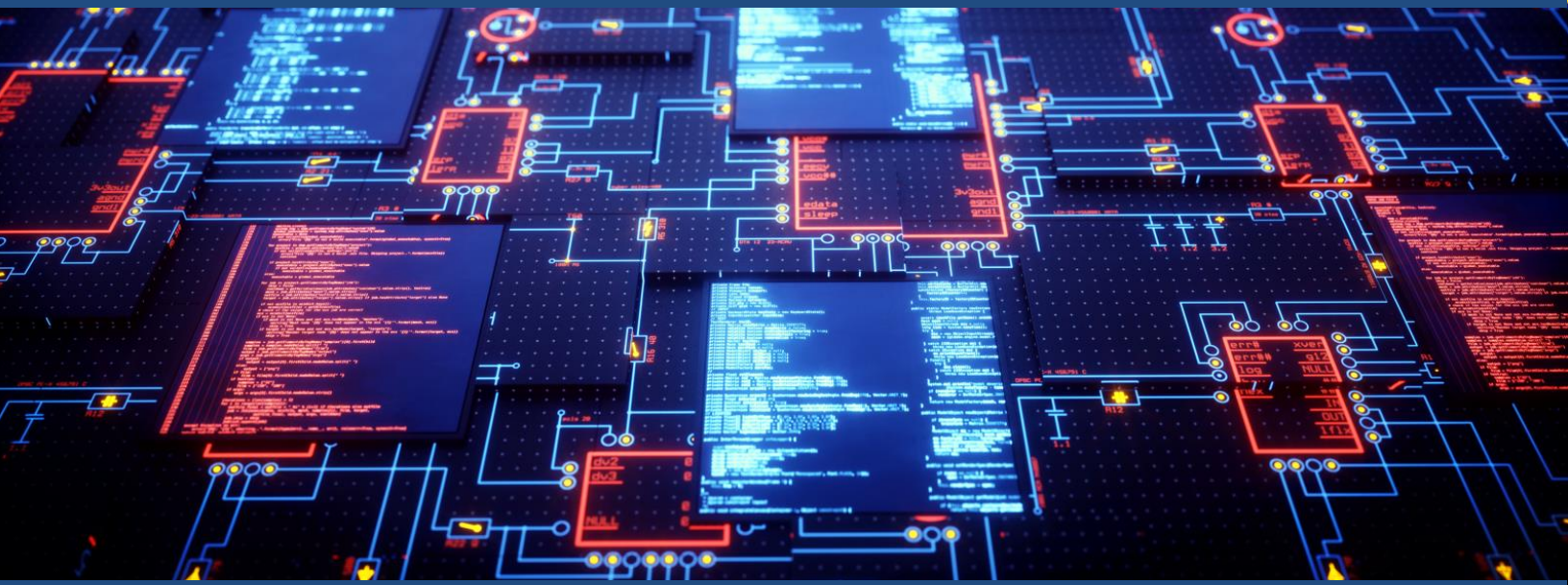


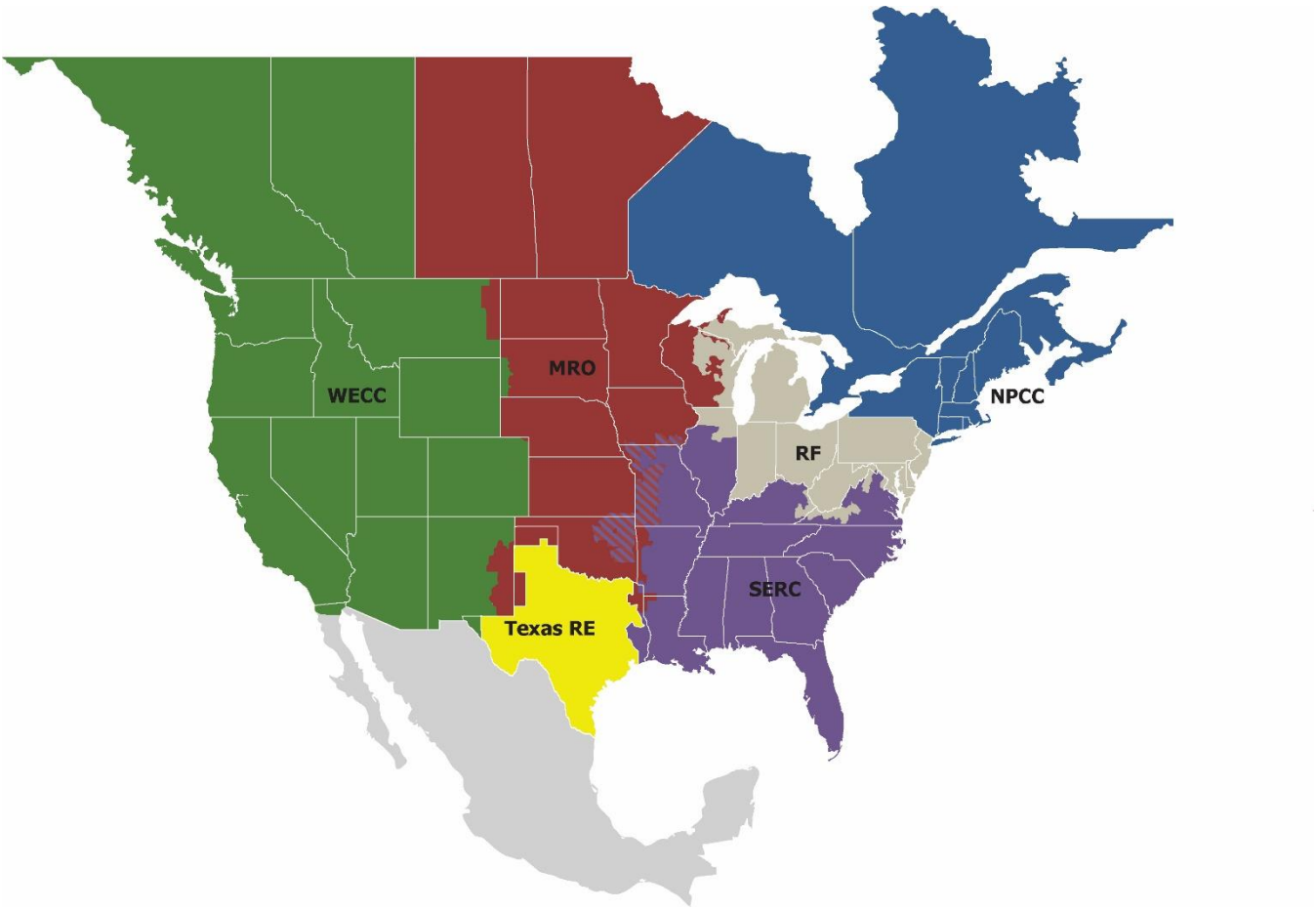
Table of Contents

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 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

Executive Summary

The rapidly evolving threat landscape is characterized by increasingly sophisticated cyber attacks that emphasize the need to strengthen the resilience of our critical infrastructure against potential catastrophic impacts on the BPS. NERC work plan priorities for 2023[1] include developing cyber-informed transmission planning approaches that incorporate cyber security risks into transmission planning activities to mitigate reliability impacts that could result from cyber attacks. Studying a wider range of contingencies associated with security threats will lead to a more resilient BPS by driving enhanced security controls and new perspectives on conventional transmission network upgrades. By incorporating security where it has traditionally not been in place, industry will be able to better ensure the effective reduction of risks to the reliability and security of the BPS.

This white paper introduces the cyber-informed transmission planning framework (CITPF) for including cyber security threats, particularly from coordinated attacks, into transmission planning studies that are most commonly conducted by Transmission Planners (TPs) and Planning Coordinators (PCs)—see **Figure 1.1** in the **0** for a graphic representation of this.

The CITPF is intended to drive investments in cyber security where warranted and can be used by various entities—NERC, Regional Entities, industry stakeholders, regulators, and policymakers—to perform reliability studies; these studies will uncover unacceptable risks to the BPS that should be addressed with appropriate mitigations.

Additionally, this white paper explores resilience measures that complement security controls by studying, identifying, and reducing the number of critical facilities and their attack exposure. The following are key focus areas that are vital to the successful integration of security concepts into transmission planning practices and processes and are covered in this white paper:

- Aligning terminology and definitions across security and engineering disciplines (see **Appendix A**)
- Mapping cyber security threats, vulnerabilities, and impacts to conventional transmission planning contingency definitions
- Analyzing the current state of cyber and physical security considerations (both implicit and explicit) in long-term planning studies and recommending enhancements to existing standards
- Introducing the CITPF and the thought processes for integrating cyber security concepts into transmission planning practices and processes
- Outlining a high-level roadmap for cyber security integration with long-term transmission planning practices, including recommendations for next steps

The ERO Enterprise suggests piloting the CITPF in collaboration with industry stakeholders to demonstrate its value while deriving insights for iterative improvement and refinement of the CITPF. Based on the technical foundation provided by this white paper, recommendations to make changes to NERC standards (particularly TPL-001) are to ensure that a broader set of reliability risks can be appropriately mitigated with transmission network upgrades and/or additional cyber security controls. These recommendations will be further informed and refined based on lessons learned from pilot projects conducted using the CITPF.

[1] https://www.nerc.com/AboutNERC/StrategicDocuments/2023_NERC_Work_Plan_Priorities_Board_Approved_November_16_2022.pdf

Introduction

Background on Security Integration

The *2021 ERO Risk Priorities Report*[2] highlighted that the electricity ecosystem is undergoing a rapid change in its resource mix, end-use loads, and technologies used to control and operate the grid. Grid transformation coupled with the changing threat landscape and the convergence of information technology (IT) and operational technology (OT), business practices, communication networks, and system resources is increasing the grid's attack surface, resulting in increased cyber and physical security risks. Industry must develop and implement new models, advanced tools and analytical capabilities, and new ideas around planning, designing, building, and operating a reliable and secure power grid moving forward.

In the past, industry focused on addressing silos between grid planning, design, and operations departments. Today, those groups work closely in their efforts to plan a reliable and resilient system and operate it in the face of unexpected events. However, with the increasing focus and risk from cyber security threats, the electric sector needs to explore ways to integrate security and engineering practices into the long-term planning, design, and operations horizons. While the electric industry is improving, many organizations have minimal collaboration and coordination between their engineering and security staff in a truly integrated manner. Neither side needs to become an expert in the other discipline; however, there are likely opportunities where increased collaboration and integrated processes can drive better business decisions, cyber-resilient long-term transmission plans, and enhanced BPS reliability and security.

> ***Security Integration:*** *The incorporation of cyber and physical security aspects into conventional planning, design, and operations engineering practices.*

In an effort to begin conversations around "security integration," NERC created the Security Integration and Technology Enablement Subcommittee (SITES)[3] in 2020 to focus on security integration as well as securely integrating emerging technologies on the BPS. SITES has primarily focused on technology enablement topics, including zero trust architectures in the electricity sector, cloud technology in the OT environment (particularly for real-time operations), and streamlining emerging technology deployment. SITES has not yet addressed ways in which TPs and PCs can more directly consider cyber security risks as part of their planning assessments. This paper complements the work that the SITES has conducted to-date and aligns with their work plan.

NERC also collaborated with the Institute of Electrical and Electronics Engineers (IEEE) Power and Energy Society (PES) and published an IEEE technical report (TR105)[4] on security integration. NERC and IEEE jointly identified security integration as a high priority topic for both organizations to tackle together, and they initiated a joint task force to introduce the concepts of security integration. The effort specifically addresses topics pertaining to possible threats to the electricity sector, integrated planning approaches, integrated equipment design, integrated system operations, and securely integrating emerging technologies. This white paper builds upon the work done by the TR105 team that developed the IEEE technical report.

[2] https://www.nerc.com/comm/RISC/Documents/RISC%20ERO%20Priorities%20Report_Final_RISC_Approved_July_8_2021_Board_Submitted_Copy.pdf
[3] https://www.nerc.com/comm/RSTC/Pages/SITES.aspx
[4] https://resourcecenter.ieee-pes.org/publications/technical-reports/PES_TP_TR105_PSCC_120622.html

The *2022 ERO Work Priorities* and the *2023 ERO Work Priorities*[5] include security integration as a key focus area. In particular, this white paper supports one specific focus area in the *2023 ERO Work Priorities*:

> *"Develop cyber-informed planning approaches documented in technical reports or other guidance material to study, identify, and reduce the number of critical facilities and attack exposure/impact."*

The roadmap that this white paper provides is intended to serve as a foundational cornerstone for future incorporation of security concepts into transmission planning practices in a more holistic manner. It is intended to lay the groundwork for establishing cyber security risk scenarios that should be modeled, studied, and mitigated (where applicable) as part of BPS planning assessments. This white paper also advocates for enhancing security controls where unacceptable reliability risks are identified. These efforts require close coordination between transmission planning engineers, security professionals, and the system design and operations teams. This white paper also describes NERC standards revisions to enhance current industry security practices moving forward. Multiple Regional Entities have started exploring security integration concepts; this white paper brings those practices together, introduces new ideas, and presents the CITPF for future planning assessments that leverage the lessons learned thus far.

Conventional Transmission Planning Activities

TPs and PCs are responsible for assessing the long-term reliability of the BPS within their respective planning footprints while coordinating their plans with other TPs and PCs within the larger Interconnection. TPs and PCs have various groups or departments within their respective organizations that perform the functional activities of transmission planning; however, TPs and PCs generally perform the following activities:

- Interconnection and modeling requirements management
- Model development, validation, management, and maintenance
- Transmission project development, launch, and coordination
  - Business case development for strategic projects
- Relay planning (in some cases)
- Telecommunications planning (in some cases)
- Remedial action scheme design and performance studies
- Interconnection studies and interconnection queue management—generator, line, and load
- Transmission service request studies
- System reliability planning assessments
  - Steady-state, dynamic, short-circuit, electromagnetic transient, power quality (e.g., harmonics), and geomagnetic disturbance studies
  - Local, regional, interregional, and system-wide reliability studies
  - Generation retirement studies
  - Grid resilience studies
  - Seasonal preparation and readiness studies
  - Asset management studies

[5] https://www.nerc.com/AboutNERC/Pages/Strategic-Documents.aspx

- Available transfer capability analyses
- Design of safety nets—underfrequency and undervoltage load shedding programs
- Operations support
  - Assist system operations during grid emergencies or extended outages
  - Identification and development of operational procedures

Figure I.1 highlights fundamental aspects of transmission planning activities. TPs and PCs rely on accurate models, sufficient tools, and tool capabilities to simulate and study the reliability impacts of specific outage conditions or other scenarios. These studies enable appropriate and suitable reliability decisions, such as developing corrective action plans, planning infrastructure investments in the form of transmission upgrades, or developing new or revised operational procedures. Cyber attacks and their impacts on the BPS need to be mapped to the tools and capabilities available to TPs and PCs such that quantitative analyses of BPS reliability can be conducted.

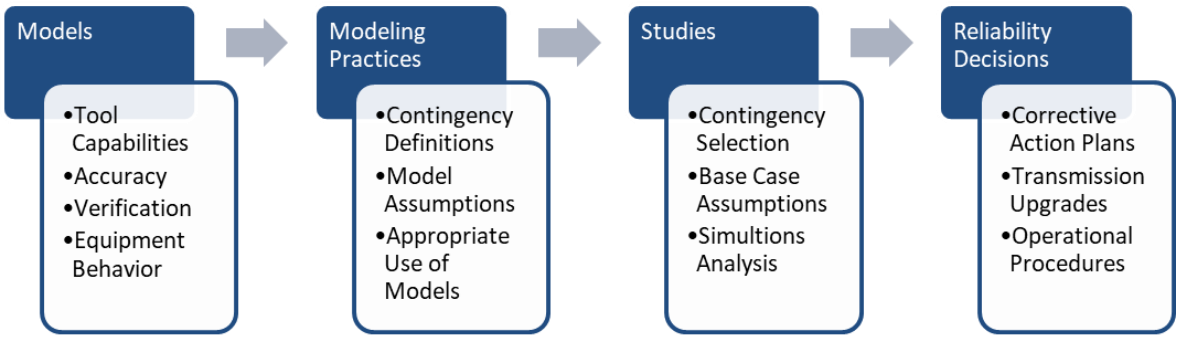


Figure I.1: Fundamental Steps of Transmission Planning Activities

Integrating Cyber and Physical Security into Transmission Planning

Historically, the functional activities performed by TPs and PCs (described previously in the **Conventional Transmission Planning Activities** section) have not considered cyber and physical security threats in much detail. More recently, the NERC CIP-014 standard was introduced after the Metcalf substation attack to ensure critical infrastructure was protected with physical security measures. Similarly, TPL-001 was updated to account for possible cyber risks but only as extreme events with no necessary mitigating measures or corrective action plans required if reliability issues are identified. More recently, FERC directed NERC to conduct a study that evaluated the adequacy of CIP-014,[6] the required risk assessments called for in the standard, and whether a minimum level of physical security protections should be required for all BPS transmission stations and substations as well as primary control centers. In each of these examples, the paradigm is shifting toward studying risks to BPS reliability from security-related threats. However, while the concept of physical security threats continues to be elevated, the ERO Enterprise also believes that planners should study cyber security contingency events which may require corrective action plans if an agreed upon level of reliability is not met (e.g., instability, uncontrolled separation, cascading outages).

Historically, the lack of collaboration between transmission planning engineers and security teams is partly because planners work mostly with the design engineers in developing new projects. After grid planners identify the possible corrective action plans needed, they establish the necessary upgrades and work with design engineering to develop transmission upgrade projects. Most organizations have closer ties between the design engineering departments (e.g., protective relaying, control system design, telecommunications design, construction, field service) and security departments. However, those connections also have room for improvement despite being more common than ties

[6] *N. Am. Elec. Reliability Corp.,* Docket No. RD23-2-000 (Dec. 15, 2022) (delegated letter order).

between grid planners and security teams. These relationships are illustrated in **Figure I.2** and highlight that these three groups need to work in an integrated fashion–from analysis to project inception through project design and execution–to foster security integration.

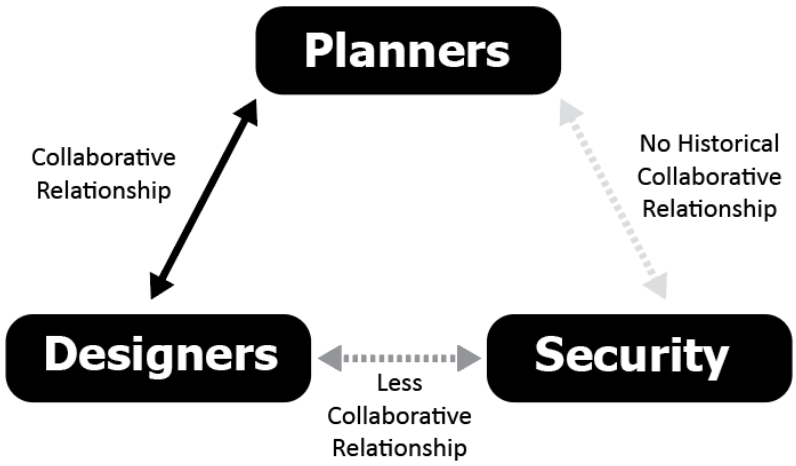


Figure I.2: Ties between Business Functions

This white paper focuses specifically on the following questions:

- How can cyber security risk be incorporated into conventional transmission planning practices and how can long-term planning assessments more directly consider cyber security risk to the BPS?
- What additional data sources, tool uses or enhancements are needed to perform cyber-security related studies?
- What specific cyber security risk scenarios should be included in planning assessments?
- Can a framework be established to map cyber security risks to BPS reliability studies?
- Can industry define a "cyber security contingency" as part of a planning assessment and quantify potential impacts of a compromise?
- How should the "cyber security contingency" definitions be updated, and within what time frame, for use in planning assessments?
- Can possible cyber security risks affect the single largest credible contingencies studied by grid planners, and what mitigations could or should be in place to limit the extent of those contingencies?
- Should the Adequate Level of Reliability[7] definition be modified to more effectively include concepts of security risk? How could and should these enhancements drive mitigating security controls?
- What coordinated attacks on the electric grid (i.e., BPS, distribution networks, and end-use loads) could pose significant BPS reliability risks? How can the impact of those compromises be studied in planning assessments?
- Can these concepts be tested on real-world systems to understand how the proposed CITPF performs and to identify any possible security risks that could be mitigated through corrective action plans?
- What efforts can reduce the costs of securing facilities by including physical and cyber security components in the design phase?

[7] https://www.nerc.com/docs/pc/Definition-of-ALR-approved-at-Dec-07-OC-PC-mtgs.pdf

Security Integration Analogy: Wildfire Preparedness

In an effort to drive home the points regarding security integration, consider utility wildfire preparedness and the similarities it can have with security integration. An entity cannot predict exactly where the next fire will start but knows that the risk is high in some areas. Fires can be attributed to natural causes, accidents, or to malicious acts. Regardless of cause, the utility needs to be prepared to ensure reliability in the face of this omnipresent threat and to be prepared to mitigate the impacts to end-use customers when the grid is compromised.

To prepare for these conditions, utilities can use monitoring and situational awareness tools, communication with internal and external partners, and other capabilities to prepare for these events and respond. In addition, utilities can go further in studying the electrical impacts of possible fire threats; they can explore fire boundaries and areas of "segmentation" where fires are unlikely to jump between. They can explore possible outages of affected facilities within a given zone to identify effects on end-use customers. They can also coordinate with firefighters to ensure safety, reliability, and resilience for any key assets that could be affected. These studies may be able to prepare the system for possible threats and also allow for more rapid recovery from outages. Lastly, these studies may identify areas where fire prevention reinforcements or other capital projects may be necessary to ensure the reliability of the BPS during these events.

This analogy mirrors the concepts of cyber security, incident response, and proactive planning to mitigate the potential impact posed by cyber threats. One can replace wildfires with cyber security threats and the narrative and theme are generally the same. This white paper focuses on the last part of honing in on the studies that can be conducted in the transmission planning time horizon to prepare and posture the system to be more cyber resilient.

Focus on Coordinated Attacks

Compromise of high-impact facilities, such as control centers, are the most notable risk to BPS reliability since a bad actor could compromise or affect many different assets across the system simultaneously. Hence, these environments are protected with multiple layers of security controls to minimize the risk of cyber threats. However, a coordinated cyber attack[8] across multiple lower impact assets on the BPS can also pose a significant BPS reliability risk due to the aggregate impact that a compromise of multiple assets could have on the grid. The BPS is designed to withstand the loss of one or two elements at any time; however, the BPS is not designed to withstand outages or compromises of many assets that are not electrically linked to one another. Therefore, a central focus of this white paper is exploring how coordinated cyber attacks could be studied by TPs and PCs to identify risks that warrant additional security controls or infrastructure enhancements.

NERC and industry stakeholders reviewed the low impact BES Cyber System (BCS) criteria (per CIP-002[9]) and noted "…low impact BES Cyber Systems may introduce BES reliability risks of a higher impact where distributed low impact BES Cyber Systems are used for a coordinated attack." In their report,[10] the Low Impact Criteria Review Team (LICRT) recommended "…enhancing the existing low impact category to further mitigate the coordinated attack risk." As part of the deliverable, the team also ranked coordinated attack methods based on ease of execution, potential impact to operations, and probability of occurrence. The following are the ranking results:

[8] A cyber attack that simultaneously, or nearly simultaneously, negatively impacts multiple facilities
[9] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf
[10] https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC_LICRT_White_Paper_clean.pdf

- **High Risk Category**
  - **Unauthorized Remote Access:** Management access by an unauthorized party for malicious intent initiated from an external system with any available communication means, including compromise of known or unknown access methods, insecure configurations, or system vulnerabilities
  - **Malicious Software:** Software that enables unauthorized malicious behavior on a target system, such as spyware, ransomware, logic bombs, worms, trojans, or key loggers
- **Medium Risk Category**
  - **Supply Chain Common Service Attack:** Compromise of a service organization that has business relationships with multiple partner organizations to enable the malicious actor to gather sensitive data, initiate unauthorized remote access, deliver malicious code, or initiate any other attack against partner organizations
  - **Supply Chain Compromise:** An attack against suppliers that provide products and/or services in order to initiate a malicious campaign against one or more target organizations
  - **Unauthorized Internal Access by a Single Actor:** Physical access by an unauthorized party or by a party abusing their existing access for malicious intent initiated from an internal system, thus bypassing any communication network perimeter remote access controls (The attacker then uses any communication means available to launch a coordinated attack by compromising or operating other systems at multiple locations.)
- **Low Risk Category**
  - **Denial of Service:** A remote attack that interrupts normal operation, typically by saturating communications (shared or otherwise), interrupting system process capabilities, or initiating a system failure
  - **Data Manipulation:** Malicious modification of data, typically at the application protocol level, to hide, mislead, or initiate unauthorized changes to target systems
  - **Unauthorized Internal Access by Multiple Actors:** Simultaneous physical access at multiple sites by unauthorized parties or by multiple parties abusing their existing access for malicious intent. This attack method requires multiple individuals at multiple locations working in a coordinated fashion toward a single purpose.

The primary risk of these coordinated attacks is the aggregate impact they could have on the BPS if successfully carried out across a number of assets. Disparate threat vectors exploiting different vulnerability types across different OT systems is unlikely to have a simultaneous impact across many different assets. However, common vulnerabilities that could be exploited across multiple assets throughout the BPS could pose significant risk. Compromise of transmission or generation control centers or other critical facilities could result in catastrophic consequences; however, those are medium impact or high-impact BCSs with a comprehensive set of mitigating security controls under NERC Critical Infrastructure Protection (CIP) standards. On the other hand, compromise of generator manufacturers, software vendors, or relay manufacturers that affect many different low impact BCSs could pose an equally impactful risk to BPS reliability. Furthermore, compromise of large distribution control centers could also result in a significant loss of service to end-use customers and have adverse impacts on the overall BPS. The goal of this roadmap is to explore how TPs could study these impacts in planning assessments to proactively identify and possibly mitigate areas of risk. NERC Project 2023-04,[11] which focuses on modifications to CIP-003, may potentially reduce the risk of some coordinated attacks. However, the duration of the project and its specific outcome is not yet known. Therefore, it is essential for TPs to study and address these risks in the meantime to ensure that the BPS

[11] https://www.nerc.com/pa/Stand/Pages/Project-2023-04-Modifications-to-CIP-003.aspx

remains resilient against potential cyber threats. Furthermore, the framework recommends exploring additional coordinated attack scenarios that could go beyond the security controls within scope for modifications to CIP-003.

Understanding Limitations in Current Planning Practices

The concept of a coordinated cyber attack and its impact on BPS reliability is not currently or generally studied as part of standard industry practices. TPL-001 planning assessments include a set of simulated outage events that must be studied, and CIP-014 physical security risk assessments include the loss of an entire substation. However, beyond the "extreme events" section of TPL-001, any concept of a coordinated attack across multiple assets, owners, or operators of the BPS is generally not considered.[12] This is predominantly due to the relative newness of cyber threats to OT communication networks and equipment as well as the traditional focus on environmental contingency events rather than cyber events. In addition, industry has not developed a common modeling and study framework that could be used to drive investments in BPS infrastructure or additional cyber security controls. **Table I.1** illustrates the types of contingencies currently studied by TPs and the wide range of possible security events that are not presently studied. Note that red across all three columns for a given scenario indicates the highest existing risk and a need for study.

Table I.1: Gaps in Transmission Planning Studies Regarding Cyber Attacks

Scenario	Do Planners Study?	Risk of Coordinated attack?	Gap in Mitigating Controls?
Transmission			
Misoperation or outage of a single line or device (e.g. relay, transformer)	YES		
Misoperation or outage of multiple components of single substation (e.g., breaker failure)	YES		
Misoperation or outage of remedial action scheme (RAS)	YES		
Misoperation or outage of a single substation	YES		
Misoperation or outage of multiple entire substations	NO	YES	YES
Compromise of Transmission Operator (TOP) control center	NO	YES	NO
Generation			
Misoperation or outage of a single generator, bus, or control	YES		
Misoperation or outage of multiple elements at a single generation facility	YES		
Misoperation or outage of a single generation facility	YES		
Misoperation or outage of multiple generation facilities	NO	YES	YES
Compromise of a Generation Operator (GOP) control center	NO	YES	NO
Distribution			
Misoperation or outage of a single Transmission–Distribution (T–D) interface	YES		
Outage of multiple T–D interfaces	NO	YES	YES
Misoperation or outage of multiple distributed energy resources or demand response (e.g., centralized control of many resources)	NO	YES	YES

[12] While TPL-001 includes "cyber attack," it does not create a standard definition for how a cyber attack should be studied via simulation.

Chapter 1: Cyber-Informed Transmission Planning Framework

The term "cyber-informed transmission planning" is used herein to refer to ways in which cyber security can be integrated into the transmission planning process. This requires cross-departmental collaboration and a fundamental framework that can be used as a starting point to enable a conversation.

This chapter outlines an adaptable CITPF (see **Figure 1.1**) in which planning engineers performing long-term planning assessments can engage with cyber security professionals and design engineering teams to study and analyze cyber security risks and any possible compromises that could occur and lead to outages of BPS elements. One goal is to establish a clear level of reliability that the BPS is designed to that is more inclusive of potential cyber security risks that could adversely affect BPS reliability. Beyond this design basis, security professionals and network operators will need to rely predominantly on recovery and restoration rather than prevention.

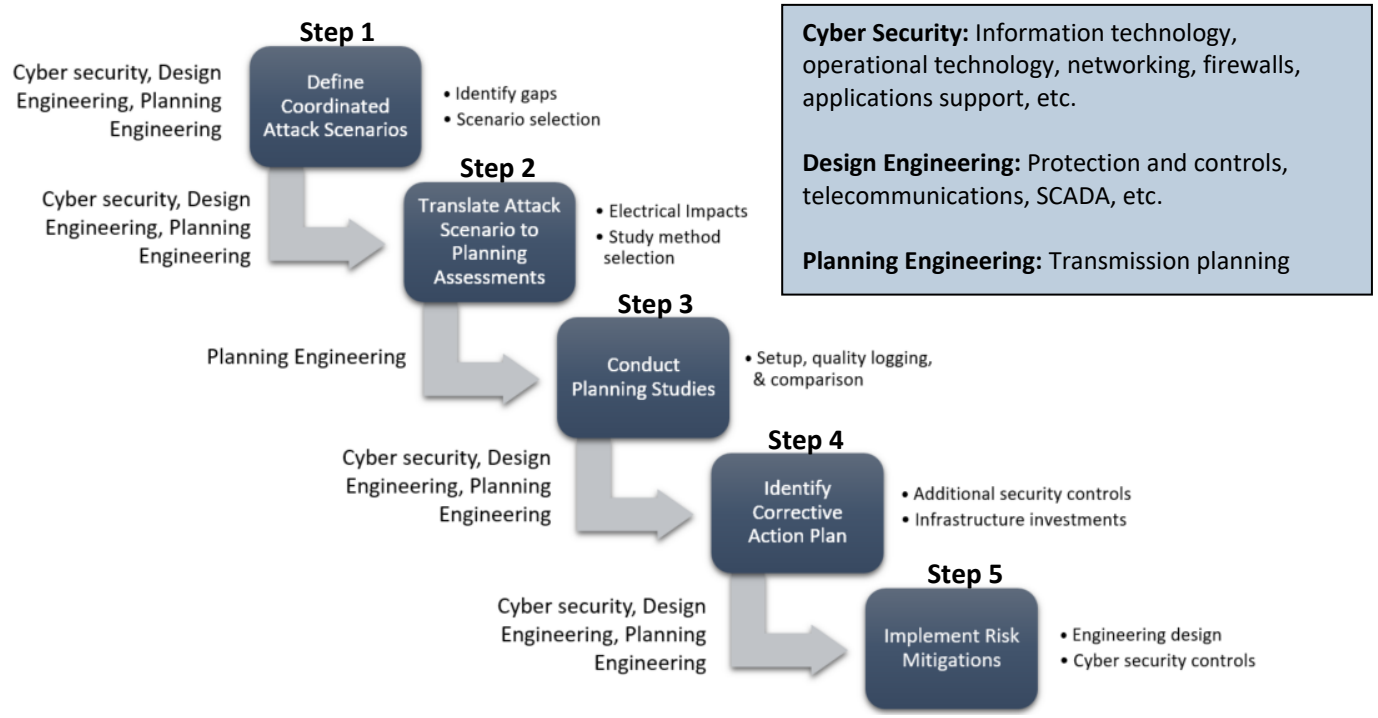


Figure 1.1: Cyber-Informed Transmission Planning Framework (the CITPF)

At a high level, the CITPF (**Figure 1.1**) includes the following steps:

- **Step 1: Define Coordinated Attack Scenarios**
  This step defines the scenarios that TPs can use to develop contingencies in their planning studies. In particular, the aggregate risk of multiple affected elements caused by common security control gaps is of primary concern.
- **Step 2: Translate Attack Scenario to Planning Assessments**
  TPs can collaboratively work with design engineers and security professionals to determine possible affected BPS elements (e.g., substations, lists of specific elements) for each attack scenario considered by using them similarly to conventional planning contingencies.

- **Step 3: Conduct Planning Studies**
  With defined contingency definitions (attack scenarios) and contingency lists (affected assets), TPs can use planning models, study tools, and conventional planning criteria to analyze performance (e.g., thermal, voltage, stability) of the BPS in a quantitative manner.
- **Step 4: Identify Corrective Action Plan**
  TPs, design engineers, and cyber security professionals can work collaboratively to analyze the outcomes of the planning studies and determine if any mitigations are necessary for identified reliability issues. This could involve implementing additional cyber security controls at specific locations or it may involve building additional infrastructure to eliminate the criticality of specific BPS facilities.
- **Step 5: Implement Risk Mitigations**
  Cyber security and design engineering teams can work together to implement necessary security controls to mitigate identified risks. Unacceptable quantified risks to the BPS should be mitigated with "defense-in-depth"[13] strategies that may involve security controls beyond the minimum requirements established in NERC CIP standards. Mitigations can be shared with the planning department to eliminate the credibility (or feasibility) of possible attack scenarios (i.e., contingencies) in future studies.

Repeated use of the CITPF should result in iterative improvements to the overall process across multiple departments in the organization, which is the overall intent of "security integration." Likewise, documenting risk mitigations and lessons learned from the CITPF will be crucial to ensuring success. The following sections describe each CITPF step in more detail.

Step 1: Define Coordinated Attack Scenarios

Coordinated cyber attacks can be incorporated into planning assessments when they are understood, clearly defined, modeled, and simulated to study their impact on BPS performance. The inclusion of cyber attacks as credible contingencies in the long-term planning horizon establishes which events the system will be designed to withstand; security professionals and network operators will need to rely on recovery and restoration activities for cyber attacks that go beyond that design basis. Security vulnerability assessments often focus on individual assets, communication networks, or systems. However, coordinated attacks or attacks engineered with a single common software platform could have a significantly greater adverse impact on BPS reliability than attacks on individual systems. These coordinated attacks could span across large portions of the BPS, potentially affecting a vast number of assets.

A challenge for TPs and cyber security professionals is using appropriate judgement to determine which threats or attack scenarios to consider and to identify which assets could be affected given the large number of possible permutations. Attack scenarios may be prioritized by identifying existing security control gaps in equipment technical standards, regulatory standards, or security framework implementations (e.g., security maturity levels). Entities can also perform their own internal risk assessments by using available threat intelligence to make an independent selection of attack scenarios for study. Industry risk assessments, such as those provided by NERC, the Electricity Information Sharing and Analysis Center (E-ISAC), and the Cybersecurity & Infrastructure Security Agency (CISA),[14] highlight present and emerging risks to the BPS and can be used to inform transmission planning studies. Threat intelligence provided by these sources represents trending vulnerabilities or actual attacks observed in the electricity sector, other interdependent industries (e.g., telecommunications, natural gas), or the global cyber landscape at-large.

The LICRT report highlighted coordinated attacks associated with potential control gaps for BCS classified as low impact per NERC CIP standards. Additionally, facilities that do not fall within the thresholds of categorization for NERC CIP applicability potentially share a lack of mitigating security controls. For example, the lack of required

[13] Appendix A
[14] https://www.cisa.gov/shields-up

authentication controls for low impact BCS has been identified as an area of risk. This gap in security controls can be associated with a high risk of compromise for BCS with remote access capabilities; therefore, this could be a high priority scenario for study by TPs.

Table 1.1 provides example scenarios that TPs could study because they could have the potential to cause outage of multiple elements beyond what is traditionally studied in conventional planning assessments—including multiple substations, multiple generation assets, or significant loss of load at the distribution level. Each scenario has a potential coordinated or aggregate impact on multiple facilities that exceeds what is currently defined in the list of required contingencies in the NERC standards. Each row in the table represents an example scenario for study and provides the suggested input data to gather, assess, and use to derive the output (i.e., outaged elements for the study) to be used in **Step 2** of the CITPF. Note that these scenarios will not necessarily apply to every entity, and there are likely other scenarios each entity could determine to be worthy of study (e.g., scenarios involving large loss of load through compromise of electric vehicle charging systems).

Table 1.1: Framework Step 1—Prioritized Attack Scenarios for Contingency Study

Study	Coordinated Attack Scenario	Necessary Inputs for Study	Expected Outputs
Study 1	Outage of multiple BPS (low impact BCS and non-BES) generators due to compromise of OEM	• Original equipment manufacturers (OEM) make and model of generation equipment • OEM Penetration of planning region • List of facilities with OEM equipment	List of outaged generators
Study 2	Outage of multiple Distributed Energy Resources (DERs) due to compromise of OEM	• OEM make and model of generation equipment • OEM Penetration of planning region • Aggregate amount of DERs by OEM	Aggregate MW capacity of outaged DERs
Study 3	Outage of multiple BPS (low impact BCS and non-BES) transmission substations due to compromise of devices through remote access capabilities	• List of Substations with interactive remote access • Subset of above list without multifactor authentication • List of substations that allow access between locations without segmentation and/or security controls	List of outaged transmission substations
Study 1–3 Alternative	Manipulation[15] rather than outage of multiple asset classes as described in Study 1–3 above	See Study 1–3 above, and identify control parameters modifiable within equipment under study	Lists in Study 1–3 above; list of modified parameter(s)
Study 4	Outage of multiple Transmission to Distribution Interfaces[16] (T–D Interfaces) due to	• List of distribution entities • List of distribution substations • List of T–D interfaces	List of outaged T–D interfaces

[15] For example, injection of an auxiliary active power command, rapid enabling and disabling of power factor control, or altering turbine-governor gains or time constants.

[16] A T–D interface is the electrical point, commonly a transformer, where the transmission system ends and the distribution system begins.

Table 1.1: Framework Step 1—Prioritized Attack Scenarios for Contingency Study			
Study	**Coordinated Attack Scenario**	**Necessary Inputs for Study**	**Expected Outputs**
	compromised distribution control center		
Study 5	Outage of all DERs under control of a common DER aggregator	• List of DER aggregators in TP/PC footprint • General location and MW capacity of DERs under control of each DER aggregator	Aggregate MW capacity and location of outaged DERs

The following subsections will provide additional considerations regarding the necessary input information to develop credible attack scenarios, the necessary output data that would be passed to transmission planning engineering, and additional descriptions for each coordinated attack scenario proposed in **Table 1.1**.

Scenario Inputs

TPs and PCs, with consultation from available cyber security teams, should consider the following when gathering the appropriate input data for any attack scenario and associated study:

- Conduct surveys of OEMs used across their footprint
- Use publicly available data sources (e.g., EIA-860)[17] as well as data requested from Transmission Owners (TO), Generator Owners (GO), Distribution Providers (DP), and any other entity within the TP/PC footprint
- Leverage threat intelligence sources (e.g., E-ISAC, CISA, InfraGard) and national vulnerability database(s) (e.g., NIST NVD[18] or the *CISA Known Exploited Vulnerabilities Catalog*[19]) to develop studies with credible risk by selecting OEMs or specific equipment models with known vulnerabilities and/or being actively targeted by threat actors
- Use scenarios and sensitivity analysis where data is unavailable or insufficient to identify thresholds where instability, uncontrolled separation, or cascading outages would occur (e.g., determining how much generation loss could occur in a particular area or Interconnection)
- Use conservative assumptions[20] regarding known security control gaps, such as those identified in the LICRT report, when information is not available
- Keep the collection of security control information from entities general and high level. The collection of confidential data, such as BES Cyber System Information (BCSI), is unnecessary and should be avoided. However, consider appropriate security controls needed to protect the data as necessary.

Scenario Outputs

The output of **Step 1** of the CITPF will commonly consist of a list of affected assets. **Table 1.2** shows a hypothetical example of such an output. Different scenarios identified for study may result in different data for the **Step 1** outputs. However, the data should be usable by a TP in **Step 2** for translation into transmission planning models and software (with a focus on physical BPS elements).[21] TPs and PCs should consider the following recommendations to create the **Step 1** outputs for use in **Step 2**:

[17] https://www.eia.gov/electricity/data/eia860/
[18] https://nvd.nist.gov/
[19] https://www.cisa.gov/known-exploited-vulnerabilities-catalog
[20] This is due to existing limitations with planning tools regarding representing the potential networking links between devices and equipment.
[21] For example, breakers, buses, transmission circuits, or generators

- Input data can be filtered to system elements most relevant to the attack scenario being studied (i.e., narrow down system elements by using OEM equipment with the greatest penetration in the area).
- If the scenario requires generalization of impacted assets (e.g., percentages of compromised relays, wind turbines), planners should use engineering judgement[22] or consult with cyber security professionals to determine outages by making estimations in an appropriate manner. For example, if location data is lacking for a wind turbine OEM with known vulnerabilities, surveyed OEM penetration data can be used as an estimated percentage in the study to distribute outaged turbines across the TP/PC's footprint.
- Outage of entire facilities can be assumed from significant outage of devices within that facility. For example, where most or all relays are assumed to be compromised at a substation, planners can simplify the outaged element to the entire substation. For ease of study and due to the many permutations of a cyber security compromise, making such assumptions is reasonable and efficient for planning assessments.

Table 1.2: Example Generation Assets Outaged due to OEM Compromise

Plant	Nameplate Rating	Asset Type	Asset OEM	Physical Location	County
Odessa	40	Wind Turbine	ACME	Parker Rd.	Bradshaw
Round Rock	35	Wind Turbine	ACME	Jim Crystal	Festus
Firewater Creek	25	Wind Turbine	ACME	Overland Park	Denton
Blue Mound	15	Wind Turbine	ACME	Blue Ridge Creek #1	Mells
Blue Mound	4	Wind Turbine	ACME	Blue Ridge Creek #2	Mells
Fredericksburg	60	Wind Turbine	ACME	521 Country Rd 349	Harris
Small Valley	30	Wind Turbine	ACME	101 Hwy 6 North	Montague
White Water	50	Wind Turbine	ACME	425 W. Ridge Ln	McCabe
Big Rock	25	Wind Turbine	ACME	6 Round Way	Hill
Flat Hills	15	Wind Turbine	ACME	1 Ever After Way	Brown
Shenandoah	22	Wind Turbine	ACME	400 Smokey Mountain Way	Brody
Selah Mountain	5	Wind Turbine	ACME	200 North Selah Dr.	Titus

Coordinated Attack Scenario Descriptions

Table 1.3 expands each of the scenarios outlined in **Table 1.1.** Scenario descriptions are expanded and detailed guidance is given for each study's inputs and outputs along with applicable technical details. Details provided in the tables are intended to complement engineering judgment and assumptions to better enable engineers in conducting these studies.

[22] Document how that judgement is applied so it can be understood in an assessment or reviewed and improved upon.

Table 1.3: Prioritized Attack Scenarios for Contingency Study—Detailed	
Study 1: Outage of Multiple BPS Generators Due to OEM Compromise	
Scenario Description	OEM compromise could lead to malicious software being introduced into generator equipment or communication networks that result in widespread outage of affected assets. Low impact BCS or non-BES generators may use similar OEMs across many assets and lack mitigating cyber security controls.
Input	• Review comprehensive list of OEMs for generating assets (e.g., wind turbines, inverters, excitation systems, turbine-governors, plant SCADA systems) • Identify OEM similarities across assets and owners that could pose significant BPS reliability risks if compromised • Survey GOs in the TP/PC footprint to understand security controls (e.g., is multifactor authentication utilized for remote OEM maintenance/control?) • Filter the facilities lacking the following controls: ▪ Malicious code detection ▪ Multifactor authentication of remote access ▪ Active remote access session management • Determine sensitivity studies regarding the amount of affected assets (e.g., percentage of total OEM capacity)
Output	List of low impact BCS and non-BES generators (or generating facilities) with a common OEM and high risk of outage due to lack of critical security controls
Technical Details	See **Appendix D** for a detailed example of a specific OEM compromise
Study 2: Outage of Multiple DERs Due to OEM Compromise	
Scenario Description	OEM compromise could lead to malicious software introduced into DERs across a large geographic footprint that result in widespread outage of these assets. DERs are often Internet-connected and may use similar OEMs across many physical assets. Retail-scale DERs (e.g., rooftop solar PV systems) often lack sufficient security controls.
Input	• Determine MW capacity of DERs installed in the TP/PC footprint • Gather data regarding OEMs for DERs in that footprint • Identify MW capacities by OEM • Determine sensitivity studies regarding amount of affected assets (e.g., percentage of total OEM capacity) • Compare scenarios and sensitivity analysis to identify thresholds for system design (e.g., largest credible contingency in area)
Output	List of aggregate DER MW capacities with a common OEM that could be simultaneously outaged
Technical Details	Engineering judgment and assumptions are needed in situations where lack of data on individual DERs is available (likely fairly common); use conservative assumptions

Table 1.3: Prioritized Attack Scenarios for Contingency Study—Detailed	
Study 3: Outage of Multiple BPS Transmission Substations Due to Remote Access	
Scenario Description	Remote access capabilities to substation equipment and communication networks with insufficient security controls could lead to the introduction and spread of malicious software[23] across multiple assets. Low impact BCS or non-BES stations are of primary concern due to a common lack of mitigating cyber security controls.
Input	• Survey TOs to identify transmission substations in the planning region with allowed remote access into the substation network • Survey TOs in TP/PC footprint to understand security controls (e.g., is multifactor authentication utilized for remote access?) • Filter the facilities lacking the following controls: ▪ Malicious code detection ▪ Multifactor authentication of remote access ▪ Active remote access session management
Output	List of outaged low impact and non-BES substations allowing remote access with insufficient multifactor cyber security controls.
Technical Details	Consider steady-state and dynamic simulations and vary the time of outage in the dynamics; engineering judgement to investigate numerical instability issues may be needed.
Study 1–3 Alternative: Manipulation Rather than Outage	
Scenario Description	Compromise could result in manipulation of assets, not just outage of assets. Therefore, TPs and PCs could explore specific control modes, settings, or protections that could impact the same list of assets identified in Studies 1–3 in this table.
Input	• Consider Steps in Studies 1–3 above. • Identify the control mode or parameter changes of greatest concern to BPS reliability. This can include, but is not limited to, the following: ▪ Generator Controls ▪ DER Inverter settings ▪ Protection system settings ▪ BESS controls
Output	List of affected assets identified in the Studies 1–3 in this table Types of parameters, controls, or protections to modify in the study.

[23] Adversaries may not need to introduce malware to achieve desired goals. Adversaries may utilize existing tools, techniques, and capabilities native to the environment once a presence is established. This technique is known as "living off the land binaries and scripts."

Table 1.3: Prioritized Attack Scenarios for Contingency Study—Detailed	
Technical Details	Thorough documentation of the process for manipulation created during the study is necessary. For inspiration, TPs should review large disturbances in their area to find common controls that may result in greater concern to BPS reliability.
Study 4: Outage of Multiple T–D Interfaces (Delivery Points) Due to Compromised Distribution Control Center	
Scenario Description	Compromise of a distribution control center with insufficient security controls could lead to outage of T–D interfaces, causing significant and sudden load loss on the system.
Input	• Select a distribution entity (i.e., DP) • Map to a list of distribution substations for a given entity • Model T–D interface
Output	A list of outaged or modified T–D interfaces associated with similar distribution control centers operated by the distribution entity
Technical Details	Distribution system modeling will differ across areas/coordinated discussion required for appropriate modeling. Engineering judgement of coordination for where the load is served from the BPS Consider for both 50/50 and 90/10[24] demand level assumptions.
Study 5: Outage of DERs under Control of Common DER Aggregator	
Scenario Description	A future case study involving compromise of a DER aggregator's virtual power plant system could lead to malicious software introduced into DERs across a large geographic footprint that result in widespread outage of these assets. NERC CIP standards and controls are currently not applicable to DER aggregators, which may be likened to generation control centers in the near future. Additionally, retail-scale DERs (e.g., rooftop solar PV systems) often lack sufficient security controls.
Input	• Determine DER aggregators operating within the TP/PC footprint. • Determine MW capacity of DERs managed by a DER aggregator in the TP/PC footprint • Identify MW capacities by OEM • Determine sensitivities regarding amount of affected assets (e.g., percentage of total OEM capacity) • Compare scenarios with known "breaking points" for system design (e.g., largest credible contingency in the area)
Output	List of aggregate DER MW capacities with a common OEM that could be simultaneously outaged
Technical Details	Engineering judgment and assumptions (use conservative assumptions) are needed in situations where data on individual DERs is unavailable (likely a common occurrence)

Additional Coordinated Attack Scenarios

TPs and PCs are encouraged to identify and study additional cyber attack scenarios[25] in collaboration with cyber security professionals while considering the following:

[24] The terms "50/50" and "90/10" refer to the certainty of the associated demand forecast. "50/50" indicates a 50% likelihood that actual demand will exceed the forecast. "90/10" indicates a 10% likelihood that actual demand will exceed the forecast.

[25] **Appendix C** contains a more in-depth process where resources are available

- Identify common uses of technology, services, or system design across generation, transmission, or distribution assets (e.g., remote access including third-parties, standard design packages, telecommunication networks, IT/OT architectures)
- Leverage available threat intelligence for known vulnerabilities or security control gaps and filter attack scenarios based on existing implementation of security controls and build a set of questions to sample the security posture of entities within the TP/PC footprint regarding specific security controls in place
- Focus on attack scenarios that exceed existing planning criteria contingencies and identify the assets that are outaged or manipulated for each scenario

In addition, TPs and PCs may consider internal tabletop exercises to identify the most severe contingencies or feasible combination of contingencies from a coordinated attack. This should be based on the prevalence or lack of implemented security controls within the planning area. Contingencies may be simulated separately and only combined if there are no reliability issues identified in the single contingency simulation.[26] It may be unnecessary to simulate a more severe contingency to identify a reliability risk in the planning assessment if a less severe contingency has already identified a need for corrective action plans.

Step 2: Translate Attack Scenario to Planning Assessments

Translation of the attack scenario information from **Step 1** into information used by TPs is needed in order to conduct planning assessments. This includes the following two mappings:

- The list of affected assets (output) from **Step 1** to a contingency definition simulated in a planning assessment
- The specific attack scenario to appropriate study methods

Map Affected Assets to Contingency Definitions

The result of **Step 1** is a list of affected assets at one or more locations for each specific attack scenario. The list of affected assets for each attack scenario can then be appropriately mapped to elements in the planning model. The list of affected assets from **Step 1** should generally include physical BPS elements; however, it may include electronic assets (e.g., RTUs, protective relays, switches, routers) that would need to be mapped to these physical elements.

TPs will likely need input and guidance from design engineering and security teams if provided a list of electronic assets. For example, the planner will need to understand which physical BPS assets could be outaged from unexpected operation of that device if a certain protective relay was compromised. Similarly, if the affected asset is a router or switch in the substation, then the planner may need input from security and design engineering teams to understand whether the entire station or only specific assets in the station would be outaged. Using conservative but reasonable assumptions and engineering and security judgment is recommended. Collaboration across departments is needed, including gathering of substation one-lines, communications, protection and control, and other types of diagrams.

Existing transmission planning models used in commercially available software tools do not have sufficient information to automatically define cyber-related contingencies. However, TPs can leverage more manual options for tracking commonalities between elements. Most tools have unused or additional data fields for each element that can be used to add additional information, particularly for a cyber contingency. These fields could be populated with a threat identifier or specific attack scenario for easy tracking of which elements are involved in which scenarios. This could facilitate easier tracking and development of cyber contingency definitions.

[26] Generally, it is not worthwhile to attempt to simulate every permutation or combination of compromised elements. Rather, use engineering judgement to prioritize reasonable but conservative bookends for the most significant cyber security contingencies.

For clarity, a planner will need to map the list of affected BPS elements to base case identifiers, such as the following (see **Figure 1.2**):

- Bus number(s)
- Element name(s)
- Element identifier(s)
- Contingency action(s) (e.g., open line, disconnect generator, change set point value)

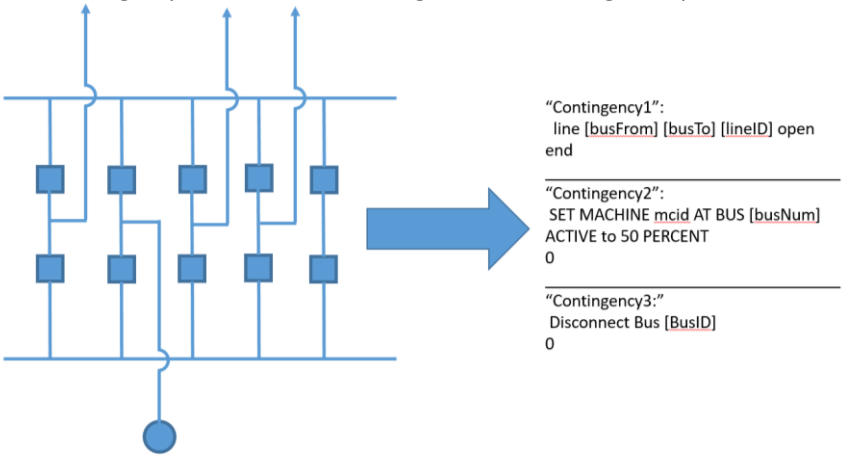


Figure 1.2: Map Affected Assets to Planning Assessment Contingencies

Collaboration between TPs, design engineers and cyber security professionals may identify common system designs that are vulnerable to coordinated cyber attacks. These coordinated cyber attacks may result in similar or identical outages across the system (e.g., relays compromised through a vendor supply chain vulnerability). Therefore, the TP may elect to study the worst-case outage at each facility that may incorporate that design (e.g., all relays compromised so the entire substation is outaged). The TP could then review the results of the analysis and propose corrective action plans where BPS performance issues have been identified.

Map Attack Scenario to Study Methods

TPs need to determine an appropriate study method (i.e., type of simulation to perform) for each attack scenario. Most commonly, steady-state contingency analysis and dynamic simulations would be used to study reliability impacts for these types of contingencies. Planners need to work with security professionals to determine the expected time scale for each attack scenario (e.g., instantaneous, seconds, minutes, hours)[27] and should consider the worst-case feasible scenario. For example, simultaneous outages of all affected assets will generally yield the worst possible reliability impacts. However, the threat may not be feasibly executed instantaneously; therefore, some understanding of timing may be necessary. Longer-term compromises may warrant use of steady-state contingency analysis tools rather than dynamic simulations. The following considerations provide general guidance:

- As a first step, conduct a worst-case steady-state contingency analysis:
  - If the simulation converges, a dynamic simulation should be performed to ensure first swing stability.
    - If the simulation diverges[28] (e.g., unsolved, numerical instability.), a dynamic simulation is needed to study this event in more detail:[29]

[27] Understanding potential cyber attack time scales drives specific engineering assumptions and the study methods used
[28] Assuming that the system divergent is due to system conditions rather than a poorly set up steady-state case
[29] The rationale behind needing a dynamic simulation for these instances can be found in CIP-014 CMEP Practice Guide - Link

  - If the dynamic simulation is stable, this may be due to incorrect modeling or study assumptions between the steady-state and dynamic simulations and these discrepancies should be explored in more detail.
- If any of the dynamic simulations performed above are unstable, this should raise the risk level and possible need for a corrective action plan. Further studies may be conducted exploring the sequencing of outages due to compromises. This type of study is a sensitivity analysis to determine groupings of elements that play a critical role in the unreliable performance issues identified.

TPs should use engineering judgement to determine the need for either steady-state or dynamic analysis beyond the contingencies studied in either TPL-001 or CIP-014.

Step 3: Conduct Planning Studies

Planning studies generally consist of steady-state, dynamic, and short-circuit analyses that apply predefined contingencies and analyze BPS electrical quantities against a set of performance requirements. For example, an N-1 contingency may result from a fault on a transmission circuit and then that circuit may be removed from service, assuming that protection systems operate as designed or with backup protection. Planners use models of the power system to conduct these simulations.

Studying the electrical impacts of a cyber security compromise is similar to any other transmission planning assessment. The complication lies in the steps preceding the planning study in terms of defining a credible cyber security threat and converting that to a defined contingency. Once these prerequisites are met, planners conduct their assessments just as any other analysis. However, TPs should consider the following when conducting these studies:

- **Base Case and Simulation Setup:** Planners should ensure their predisturbance base case has high quality models, accurate data inputs, and appropriate assumptions. Cases used for other reliability studies, such as annual transmission planning (TPL-001) assessments, could be used to study possible cyber threats. Scenario development may involve using other software to produce generation dispatch and system loading patterns. Important factors to consider and possibly explore sensitivity studies around include transmission path flows, generation dispatch, load composition, system constraints and conditions, and long-duration outage assumptions. Simulation software tools will also need to be configured appropriately to handle larger contingencies than typically studied in TPL-001 planning assessments (similar to how CIP-014 risk assessments are set up).
- **Model Benchmarking/Quality Checks:** Planners need to ensure that the case passes standardized no-disturbance tests and other quality checks to ensure it is ready for simulation.
- **Conducting Studies (Running Simulations):** This step includes running simulations for the contingencies defined in prior steps. Types of studies may differ (e.g., steady-state power-flow versus dynamic simulation) based on the types of cyber threats of concern (e.g., loss of generation, loss of transmission substations).
- **Logging Results and Comparing Results to Performance Criteria:** Determining how to compare results against performance criteria and establishing the "pass" criteria against the "fail" criteria are crucial. The following criteria are recommended for assessing cyber threats and their impact to the BPS:
  - Do not allow instability, uncontrolled separation, or cascading
  - Firm transmission service may be interrupted if the scenario setup allows for it[30]

[30] For example, firm transmission service may not be interrupted for the loss of a single generation unit. As many cyber attack scenarios are expected to outage more than one generation unit, the interruption of firm transmission service may be warranted. Refer to TPL-001 for examples of when this is commonly considered acceptable: https://www.nerc.com/pa/Stand/Reliability%20Standards/TPL-001-5.pdf

- Apply TPL-001 performance criteria[31] for these contingencies
  - Consider not allowing non-consequential load loss[32]
- Do not allow underfrequency load shedding or overfrequency tripping
- Consider allowing system adjustments between discrete steady-state cyber contingencies based on the specific attack scenario

If the agreed upon performance criteria are violated, corrective action plans may be called for to meet the design goals. Planners will need to use engineering judgment in the analysis of simulation results, particularly related to possible simulation crashing or other abnormal results. Since these types of contingencies may not have been historically studied, it is important to consider study results carefully to differentiate between possible reliability issues and numerical instability of the simulations that may be a result of software or algorithm challenges. Study results that do not meet the predefined performance criteria should be considered in the subsequent step of the CITPF. The list of credible cyber attack scenarios that lead to performance criteria violations will provide insight into the attack vectors where additional security controls or network upgrades could be utilized to reduce the likelihood of the occurrence of these attacks or mitigate their associated risks. Moreover, implementing just one extra security control at select locations or across the studied system could reduce the risk from multiple studied cyber attack scenarios.

Step 4: Identify Corrective Action Plan

Once the planning assessment has been conducted (simulations performed, results analyzed, BPS performance quantified) the next step is identifying whether corrective action plans may be needed to mitigate possible BPS reliability risks. In conventional transmission planning processes, predefined contingencies under normal operations (those that are mandated to be studied) resulting in violations of established BPS performance requirements must be mitigated with corrective action plans in accordance with NERC Reliability Standards or to adhere to federal, state, or contractual obligations. The ERO Enterprise believes this approach should also be used with cyber-induced contingencies. **Chapter 2** will address NERC standards, particularly TPL-001, which should be enhanced to ensure that a broader set of cyber contingencies that result in reliability risks can be appropriately mitigated with transmission network upgrades and/or additional cyber security controls.[33]

> ***Mitigating Cyber Security Risks with Corrective Action Plans***
> *The ERO Enterprise believes the more likely contingencies induced by cyber security events that could result in instability, uncontrolled separation, or cascading outages should be pro-actively mitigated with a Corrective Action Plan. The ERO Enterprise is proposing expanding the set of possible contingencies to encompass a broader set of possible cyber security events. NERC standards, particularly TPL-001, should be enhanced to ensure that a broader set of cyber contingencies that could result in reliability risks can be appropriately mitigated with transmission network upgrades and/or additional cyber security controls.*

TPs often drive a significant amount of capital projects for the electric power industry as they identify necessary grid enhancements to meet performance requirements for future grid conditions. However, to date, TPs have not widely

[31] Acceptable oscillation damping, voltage thresholds, transient voltage recovery, frequency response, etc.
[32] Consequential versus non-consequential load loss is determined by whether the isolating mechanism (e.g., a protective relay) also would trip load due to configuration (i.e., consequential) or just would isolate a fault and subsequent tripped load (non-consequential). When studying the threats described in this framework, load tripped by threats breaching the security perimeter of the electrical facilities and dropping load should not be an indication of "good" performance. This is analogous to not allowing for non-consequential load loss in typical studies for the faults they isolate and would incentivize stronger security controls in order to isolate compromised electrical facilities.
[33] Currently, the standard does not require a Corrective Action Plan as contingencies that are defined as "a result of a successful cyber attack" are considered an extreme event. The requirements currently also only address Cascading, as opposed to a full set of planning criteria.

or comprehensively considered the necessary enhancements to address cyber security threats that may result in instability, uncontrolled separation, or cascading on the BPS. Therefore, it is important that TPs help quantify the electrical impacts of likely cyber security threats and help drive additional capital projects to minimize those risks. TPs should work with design engineers and cyber security professionals to determine the likelihood and impacts associated with these risks. As security is an integral component of overall BPS reliability, security-based capital projects should receive ample consideration by TPs in their establishment of transmission network upgrades. This is becoming increasingly important as cyber security risk continues to be a top concern for the electric utility industry.[34]

While TPs are suited to identify possible transmission network upgrades in order to mitigate BPS performance issues, they will need to work with cyber security and design engineering teams to determine possible enhancements to security controls and adequately identify relevant corrective action plans. Transmission network upgrades may be able to lower the criticality of (or de-risk) any one location or element on the grid and therefore could serve as a long-term solution. On the other hand, cyber security enhancements could be significantly more cost effective than transmission network upgrades in some cases. Therefore, TPs and PCs need to balance which solution is most suitable for each identified reliability issue. If the cyber security enhancements do not mitigate the outage scenario but modify it in some way (e.g., Internal network security monitoring (INSM) is implemented thus improving detection and response times and lowering the threshold of assumed impacted assets), TPs should review the model assumptions in order to conduct a modified study to ensure reliability issues have been mitigated.

Corrective action plans could include, but are not limited to, the following:

- Infrastructure enhancements
  - Transmission reinforcements (e.g., line reinforcements, new substations, reactive devices)
  - Infrastructure to allow for the implementation of restoration/resiliency plans (e.g., installation of temporary tower structure to reroute lines around an applicable substation)
  - Eliminating the criticality of certain assets through transmission network upgrades
  - Increased interregional transfer capability
- Controls and protections enhancements
  - Additional remedial action schemes
  - Additional safety nets (e.g., modifications to underfrequency, undervoltage load shedding programs)
  - Modifications to protection and control systems
- Operating procedures enhancements
  - Enhanced operating procedures coordinated among operators, operations engineers, planners, and cyber security professionals
  - Enhanced system restoration procedures for blackstart during a cyber security compromise
  - Additional contingency reserves
  - Changes to maintenance or outage schedules
- Cyber security program enhancements
  - Additional cyber security controls at specific locations or footprint-wide as seen in **Table 1.4**
  - Improved baseline security controls for BCS assets beyond what is required through standards (e.g., independent risk assessments, asset lists for low impact assets)

[34] https://www.nerc.com/comm/RISC/Documents/RISC%20ERO%20Priorities%20Report_Final_RISC_Approved_July_8_2021_Board_Submitted_Copy.pdf

- Improved OT communication network segmentation (e.g., group intelligent electronic devices, isolate non-critical systems)
- INSM
- Intrusion detection systems and intrusion prevention systems
- Enhanced cyber incident response programs for OT (e.g., decoupling of IT/OT communication networks, disconnection of non-critical systems during cyber attacks, system restoration processes)
- Enhanced physical access controls protecting cyber systems

Table 1.4: Mitigating Controls for Coordinated Attack Methods[35]

Coordinated Attack Methods	Mitigating Cyber Security Controls
Supply Chain Common Service Attack	• Authentication • Malicious code detection • Encryption • Use of private communication networks • Change Control/Baseline Monitoring
Supply Chain Product Compromise	• Software integrity and authenticity verification • Software Bill of Materials (SBOM) • Malicious code detection • Procurement risk evaluation • Change Control/Baseline Monitoring
Unauthorized Remote Access	• Authentication • Malicious code detection • On-demand session authorization • Session logging, monitoring, and termination • Change Control/Baseline Monitoring
Malicious Software	• Malicious code detection • Change Control/Baseline Monitoring
Unauthorized Internal Access by a Single Actor	• Malicious code detection • Physical access controls • Audit logging • Change Control/Baseline Monitoring
Data Manipulation	• Encryption • Use of private communication networks
Denial of Service Attack/Distributed Denial of Service Attack	• Encryption • Distributed denial of service protection services
Unauthorized Internal Access by Multiple Actors	• Malicious code detection • Physical access controls • Audit logging • Change Control/Baseline Monitoring

[35] These mitigating controls are also called out in the low impact criteria review team report

Corrective action plans may need to be approved by public state/provincial regulators and other governing boards, but given the elevated risk profile for cyber security, it is imperative that appropriate security controls to mitigate potential risks to the BPS are considered and incentivized. The concept here is that TPs should consider cyber security enhancements (possibly beyond the NERC CIP standards) as viable solutions to mitigate risk in addition to the traditional transmission system upgrades typically developed.

Cost is a critical factor for transmission infrastructure improvements that reduce the risk of successful cyber attacks, and cost will undoubtedly be one of the top considerations for determining corrective action plans whether the plans include reducing the criticality of an identified asset(s) or the comprehensive implementation physical or cyber security controls. Costs between such measures may vastly differ; however, other factors can and should be considered when choosing which risk mitigations to implement. For example, planners should consider future transmission projects and how a corrective action plan that relies on new transmission infrastructure could relate to those efforts. While implementing new transmission infrastructure to mitigate security risks is more costly than implementing additional security controls, security controls would not be able to add more renewable enablement, support resource adequacy, contribute to reduction of emissions, or other potential benefits.[36]

Step 5: Implement Risk Mitigations

Cyber security and design engineering teams should oversee the incorporation of mitigating security controls identified as part of corrective action plans. Mitigation of cyber and physical security risks to the BPS should align with a "defense-in-depth"[37] strategy that may involve implementing security controls beyond the minimum requirements established in NERC CIP standards (even if they meet the performance criteria). Implemented security controls that mitigate cyber risks associated with planning studies may be used to filter out potential attack scenarios or impacted assets in future iterations of cyber-informed transmission planning studies. The following are considerations for the implementation of mitigation measures:

- **New Facilities**
  - Full support from leadership, including cross-departmental support, is required in order to be successful.
  - More effective security control implementations are achieved by considering security requirements and features early in the development lifecycle of the projects.
  - Security teams and design engineers can address constraints prior to implementation and incorporate the relevant controls for identified risk.
  - Equipment choices can favor expanded security feature offerings from vendors that support encryption, authentication, input validation, logging and log forwarding, sufficient physical port allocations, hardened systems, etc.
  - Communication network designs that feature segmentation—including demilitarized zones (DMZs), topologies that support traffic analysis points, secure gateways, proxies, software defined communication networks, INSM, etc.
  - Deployed security control methods should be incorporated into all future facility design plans.
- **Existing Facilities**
  - Full support from leadership, including cross-departmental collaboration, is required in order to be successful.
  - Alignment with external entities, such as regional trade organizations or other owners of jointly owned facilities, is necessary.

[36] ESIG Webinar: Multi-value Transmission Planning for a Decarbonized Future; Telos Energy
[37] See **Appendix E** for further discussion of defense-in-depth and cyber security controls

- Effective project management is needed for larger deployments across many assets.
- These facilities will require engineering design and security team assessments to identify constraints, such as flat or congested OT communication network architectures, legacy equipment lacking in device level security controls, port exhaustion, space constraints for new networking and cyber security equipment, or other OT constraints (e.g., safety and uptime requirements).
- Selection of controls should be based on available resources and effectiveness if restricting factors prevent implementation of several identified security measures.
- Security and engineering teams can create plans for retrofitting systems to address the most pertinent controls, such as multifactor authentication for all interactive remote access (vendor or otherwise), INSM, logging and alerting, authorization procedures, or added physical access controls.

Selection of security controls and the order of implementation rely on several factors, including, but not limited to, the following:

- Control effectiveness
- Cost benefit analysis
- Criticality and number of the assets requiring new controls
- Ease of implementation

Technology solutions are available for OT communication networks that can provide automated inventory, vulnerability tracking, and anomalous network communication activity detection and response. These types of security measures may be deployed in a passive manner in many instances, reducing the risk to time-sensitive or latency-dependent communication network traffic flows. In some instances, offline traffic analysis can be leveraged as a proof of concept. Pilot projects can be used to develop the processes and experience necessary to roll out a coordinated and effective implementation plan. Outside resources can also be leveraged when internal resources as not sufficient. These may include third party service providers for risk assessments, project management services, system design and implementation, or INSM services.

Security improvements may also be achieved through additional controls within the IT communication networks that are integrated with and support OT systems and functions. Additional controls assessment, therefore, should not be limited to just OT systems. Entities can also consider participating in programs that enable shared intelligence to identify cyber threats and track trends through programs like the Cybersecurity Risk Information Sharing Program (CRISP),[38] which offers "… near real-time delivery of relevant and actionable threat information…," for IT communication networks. The CRISP program is a partnership between the Department of Energy (DOE) and the Electric Information Sharing and Analysis Center (E-ISAC) and entities are encouraged to participate.

Additional resources are also available through CISA[39] to reduce cyber attack surfaces and vulnerabilities thereby improving the cyber security posture for an organization. These resources include, but are not limited to, the following:

- **CSET**: Free tool to evaluate an organization's security posture
- **KEV Catalog:**[40] Used to track vulnerabilities that have been actively exploited
- **Cyber Hygiene Vulnerability Scanning:** Free internet facing services scanning

[38] https://www.eisac.com/s/crisp
[39] https://www.cisa.gov/free-cybersecurity-services-and-tools
[40] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

- **CISA Validated Architecture Design Review:** Assessment based on NIST standards and industry best practices. Assessments can be conducted on IT or OT infrastructures (ICS-SCADA)
- **S.O.S:** Get your Stuff Off Search is a guide to reducing the attack surface of Internet-facing devices

Chapter 2: Integrating Security with Transmission Planning

Chapter 1 outlined the CITPF, which is used for conducting transmission planning studies of cyber attack scenarios–particularly coordinated attacks–that could result in instability, uncontrolled separation, or cascading on the BPS. It also described how TPs can work collaboratively with engineering design and security teams to determine appropriate corrective action plans where needed. This chapter describes additional opportunities for security integration into existing transmission planning standards, the adequate level of reliability (ALR) definition, and regional coordination activities.

Integrating Security into the Adequate Level of Reliability Definition

The "adequate level of reliability" term is used in Section 215 of the Federal Power Act[41] that specifies what standards the ERO can develop and enforce. The NERC Board of Trustees approved a definition of ALR in May 2013, and NERC subsequently submitted an informational filing regarding the definition.[42] The ALR definition is primarily used to guide NERC standards development; NERC technical committees also use it when addressing emerging reliability risks and prioritizing workload.

ALR is the state that the design, planning, and operation of the Bulk Electric System (BES) will achieve when the five defined reliability performance objectives are met. While one of the ALR performance objectives does mention "cyber security events" and "malicious acts," the ERO Enterprise believes that the ALR definition should be expanded to further integrate security as a critical component to BPS reliability given the omnipresent and rapidly evolving cyber and physical security threat landscape. While many cyber security-related activities already occur currently in support of ALR despite not being represented in the current definition, the following updates to the ALR definition are proposed:

- Cyber security events should not be considered "low probability" given the current and projected future threat landscape. ALR performance objectives should support (rather than deter) BES owners and operators to apply economically justified and practical measures to mitigate the adverse reliability impact[43] on the BES from cyber threats. As highlighted in this roadmap, corrective action plans should be expanded to recognize enhancements to security controls as potential solutions that mitigate performance risks posed by credible cyber security-related contingencies.
- The reduction of the number of critical BPS facilities is a viable strategy to mitigate the overall impact of cyber and physical security threats to the reliability of the BPS. This concept applies to both physical and cyber security threats posed to the BPS.
- A new ALR performance objective should be added to ensure that adverse reliability impacts on the BES from physical and cyber security events are managed to an appropriate level through mitigating security controls. The proposed performance outcome of this objective is to manage security vulnerabilities of the people, processes, and technology that support operation of the BES.
- A new ALR assessment objective should be added that reflects the security incident response capability to determine operational readiness of the BES for cyber and physical attack preparation, detection, containment, eradication, and restoration. In the case of region-wide physical and cyber security incidents, there is a need for incident response efforts at both the individual entity level as well as a coordinated multi-organizational level (i.e., through E-ISAC, and county, state, or other regional coordination).

The rationale for ALR assessment objectives should be updated to reflect that security professionals working in support of the BES might have a need for the resulting assessment data.

[41] Federal Power Act, 16 U.S.C §§ 791-825r

[42] https://www.nerc.com/pa/Stand/Resources/Documents/Adequate_Level_of_Reliability_Definition_(Informational_Filing).pdf

[43] Defined in the NERC Glossary of Terms as "the impact of an event that results in BES instability or Cascading."

The update of the ALR definition to more thoroughly encompass cyber and physical security will ensure alignment with NERC Reliability Standards enhancements as well as risk mitigation activities within the NERC technical committees.

Recommended Enhancements to NERC Reliability Standard TPL-001

"Steady state and stability performance extreme events" in the currently effective version of NERC TPL-001[44] defines the set of contingencies requiring study that "are expected to produce more severe System impacts on…portion[s] of the BES." These events must be studied and "an evaluation of possible actions designed to reduce the likelihood or mitigate the consequences of the events(s)" must be conducted; however, corrective action plans do not have to be developed to actually mitigate these more severe events. Unlike other defined contingencies in TPL-001, any adverse BPS performance issues caused by "extreme events" do not need to be mitigated, just studied. Furthermore, TPL-001 currently only includes the study of "loss of two generating stations resulting from…a successful cyber attack." Otherwise, TPL-001 does not include any explicit requirement for studying the electrical impacts of credible cyber attacks. Notably, the following two shortfalls need to be addressed with the currently effective version of TPL-001:

- Only the loss of two generating stations must be studied for studying cyber attacks.
- Any adverse BES performance issues identified need not be corrected, just studied.

The goal of TPL-001 is to plan a BES that will operate reliably over a broad spectrum of system conditions and follow a wide range of probable contingencies. While successful cyber security attacks are less frequent than environmental contingencies, the latent risk and increasing presence of cyber security threats lead the ERO Enterprise to reconsider whether and what type of cyber attacks should be considered "extreme events," compared to those that should be considered under "normal operations." The ability of the BPS to withstand and be resilient to individual and coordinated cyber attacks is critical to overall BPS reliability moving forward. As described in the CITPF, it is possible to evaluate coordinated attack scenarios that could have a widespread adverse impact on BPS performance (well beyond the outage of two generating facilities).

Coordinated cyber attacks will generally result in more severe BPS reliability impacts than conventional contingencies studied as part of TPL-001, including P4, P5, P6, and P7 contingencies. While less likely, they could occur and should be studied and mitigated where economically feasible; the economic consequences of a successful cyber security event can be significant. Mitigations implemented to reduce or eliminate the risk of a successful coordinated cyber attack may involve deploying additional cyber security controls as the most cost-effective solution. Hardening the security posture of the BPS is akin to transmission reinforcements to mitigate electrical issues and can be particularly effective when constraints on transmission reinforcement (e.g., permitting challenges, costs) may prove too challenging. In some cases, however, transmission network infrastructure investments could eliminate the criticality of any one element, location, or transmission network segment on the BPS as part of a multi-value project. As discussed in the CITPF, appropriate mitigations should weigh the costs and benefits of both transmission infrastructure investments and mitigating security controls. Regardless, understanding the BPS reliability impacts of potential cyber security attacks will help inform transmission planning decision-making activities.

Given these factors, the ERO Enterprise recommends the following actions be taken to enhance the concept of cyber-informed transmission planning in annual transmission planning assessments:

- TPL-001 should be enhanced to include cyber attack scenarios in long-term planning assessments that focus more on possible coordinated attacks.[45]

[44] https://www.nerc.com/pa/Stand/Reliability%20Standards/TPL-001-4.pdf
[45] This can also be applicable to the potential for coordinated physical security attacks.

- The attack scenarios described in **Chapter 1** establish a minimum set of scenarios that TPs and PCs should include in their planning assessments; additional scenarios should also be explored by industry.
- TPL-001 should encourage the effective mitigation (i.e., corrective action plans) of any widespread BPS performance issues caused by credible cyber (and physical) security attacks. This will require considering possible mitigating security control enhancements in addition to conventional transmission infrastructure upgrades.

Adoption of these enhancements will bring cyber-informed transmission planning concepts into alignment with the current threat landscape and the gravity of cyber security threats moving forward. It is imperative that cyber security be more holistically integrated with grid planning concepts to adequately and effectively mitigate possible security risks posed to the BPS.

Relationship to Physical Security and Possible Next Steps

The primary focus of white this paper is to develop cyber-informed transmission planning approaches that would support a more cyber-resilient BPS and potentially reduce the number of critical facilities and their attack exposure. It is also worth briefly describing the linkage between this effort and the physical security standard, CIP-014, and recent NERC studies on the effectiveness of that standard. Similar to cyber security attacks, physical attacks on grid infrastructure could adversely affect BPS reliability and could result in instability, uncontrolled separation, or cascading failures if severe enough. The purpose of CIP-014 is to "identify and protect Transmission stations and Transmission substations and their associated primary control centers that if rendered inoperable due to physical attack could result in instability, uncontrolled separation, or cascading within an Interconnection." These stations are deemed critical based on the electrical impact they have on the overall BPS if compromised. Transmission planning studies (steady-state and dynamic simulations) are conducted, per the risk assessments in Requirement R1 of the standard, to identify those stations. These risk assessments explore the electrical impacts of outage of an entire BPS station or substation. Specific voltage classes and size thresholds are used to determine which stations are in scope for the studies.[46]

TOs that identify a critical BPS station (and TOPs of associated control centers) must conduct an evaluation of potential physical security threats and vulnerabilities for each asset. They also must develop and implement a documented physical security plan that covers the threats and vulnerabilities identified for those assets. The security plans must focus on resilience or security measures designed to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities; coordination with law enforcement; timely execution of physical security enhancements at identified locations; and provisions to evaluate evolving physical security threats at those locations. The goal of the CIP-014 standard is to reduce the likelihood of a successful physical security compromise at certain stations and associated control centers deemed critical based on planning assessments. While CIP-014 does not currently require the development of corrective action plans that would reduce the criticality of the station or substation, it contemplates that entities may choose to implement such resiliency measures to enhance their ability to mitigate the risk and impact of a physical attack. In the FERC proceeding that sought approval of CIP-014,[47] NERC stressed that resiliency measures—including modifications to system topology or the construction of new facility to lessen the criticality of a particular facility—would ultimately make it more difficult for the perpetrator of a physical attack to cause significant harm to the BPS.

[46] Some TO footprints include significant 138 kV transmission networks that could have a widespread impact on BPS reliability if compromised. Those stations are not presently included in CIP-014 risk assessments. They are also deemed low impact BCS due to their voltage class. This could lead to potential cyber and physical security risks, particularly when considered in aggregate.

[47] *Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard CIP-014-1*, at 42-43, Docket No. RM14-15-000 (May 23, 2014); *Comments of the of the North American Electric Reliability Corporation in Response to Notice of Proposed Rulemaking*, at 26-27, Docket No. RM14-15-000 (Sept. 8, 2014).

FERC issued an order in December 2022 that directed NERC to conduct a study to evaluate (1) the adequacy of the applicability criteria for CIP-014; (2) the adequacy of the required risk assessments; and (3) whether a minimum level of physical security protections should be required for all BPS transmission stations, substations, and primary control centers.[48] In its report, NERC found that the objective of CIP-014 appropriately focuses limited industry resources on risks to the reliable operation of the BPS associated with physical security incidents at the most critical facilities. Additionally, based on studies using available data, the CIP-014 applicability criteria is broad enough to capture the subset of applicable facilities that TOs should identify as "critical." The filing also highlighted additional specificity is needed in CIP-014 regarding the types of analyses conducted in the risk assessments. Lastly, while NERC is not recommending an expansion of the CIP-014 applicability criteria at this time, NERC found that, given the increase in physical security attacks on BPS substations, there is a need to evaluate additional reliability, resiliency, and security measures designed to mitigate the risks associated with those physical security attacks across the BPS. NERC recommended holding a technical conference in coordination with FERC to explore these topics in more detail.

Consistent with the findings in that study, this report also highlights that establishing a design basis for eliminating the criticality of BPS substations or assets will help create a grid that is more resilient to cyber and physical attacks moving forward. The ERO Enterprise recommends that this topic be included as part of the resilience discussion at the upcoming technical conference. This discussion will help the ERO Enterprise determine an effective path forward in this area that will reduce the criticality of any one station or asset on the BPS as specified in the 2023 ERO Work Plan Priorities.[49] It will be important to consider the following topics:

- Physical security protections around stations and substations likely do not provide adequate protection to prevent an attack on the circuits leaving a station; however, outage of those circuits can have the same electrical effect as rendering the station itself inoperable. Circuits are not protected with the same physical security measures, so they introduce a vulnerability in substation-centered physical security plans.
- Enhanced physical security plans help the system recover from instability, uncontrolled separation, or cascading; however, eliminating the criticality of a station will mitigate the electrical risk in the first place and reduce overall risk of unreliable operation of the BPS as a whole.
- Elimination of the criticality of certain stations or substations can also support broader transmission planning activities and can be coupled with other network upgrades for reliability or economic reasons. Additional build-out of transmission infrastructure should consider the incremental benefits of reducing station or substation criticality.
- Stations or substations deemed critical from a physical security perspective have the same risk from a cyber security perspective. A cyber security compromise that affects a critical substation could render it inoperable and result in instability, uncontrolled separation, and cascading. The CIP standards reduce the likelihood of a successful compromise; however, elevated attention from a cyber security perspective is warranted for these stations unless transmission upgrades result in the station not being deemed critical.

Coordinating Regional or Interconnection-Wide Planning

Regional, interregional, or interconnection-wide transmission planning groups conduct large-scale reliability studies to identify BPS performance issues that span larger areas beyond any one TP or PC footprint. These activities seek to develop large-scale transmission network upgrades that ensure a reliable and economic BPS. These types of groups are well suited to consider the CITPF and to conduct pilot studies that could help TPs and PCs identify possible cyber attack scenarios that could have a significant adverse impact on BPS reliability. The ERO Enterprise is involved in these types of groups and welcomes coordination with industry stakeholders in these forums to help drive these concepts forward in the near future.

[48] https://www.nerc.com/FilingsOrders/us/Pages/2022FERCOrdersRules.aspx
[49] https://www.nerc.com/AboutNERC/StrategicDocuments/2023_NERC_Work_Plan_Priorities_Board_Approved_November_16_2022.pdf

Chapter 3: Recommended Next Steps

Table 3.1 lists the recommendations from this white paper and the applicable entities to address each recommendation. The goal is to outline steps needed to advance cyber-informed transmission planning as part of the NERC Security Integration Strategy.[50] This includes collaborative efforts across the electricity ecosystem, including the ERO Enterprise, registered entities, and other supporting organizations, such as service providers, hardware and software vendors, and security organizations.

Table 3.1: Recommendations and Applicable Entities Next Steps

#	Recommendation	Applicable Entities
1. Enhancing Security Integration Across the Electricity Ecosystem		
1.1	**Enhance Security Integration:** Industry is increasingly seeing a need to holistically integrate cyber and physical security professionals with engineering teams across the full spectrum of the electric ecosystem from system planning and design to grid operations and maintenance practices. Industry collectively is strongly encouraged to advance these concepts of security integration proactively to prepare for a more digitalized grid of the future. Elevating security teams across any organization requires consistent support from the executive teams and sufficient time for these teams to work organically.	ERO Enterprise, registered entities, hardware and software vendors, third-party service providers, etc.
1.2	**Engage and Share with E-ISAC:** Industry stakeholders are strongly encouraged to engage with the E-ISAC as well as to participate in Regional Entity security groups for increased security awareness and information sharing as well as to leverage best practices. Sharing information is the best way for the E-ISAC and its government partners to spot new security trends and provide additional context to threats facing the system.	
2. Enhancing and Implementing Cyber-Informed Transmission Planning		
2.1	**Adopt the CITPF:** TPs and PCs are strongly encouraged to consider the CITPF and adopt the cyber-informed transmission planning concepts into their business practices. TPs and PCs can play an integral role in studying possible cyber attack scenarios that could have significant adverse impacts on BPS reliability. TPs and PCs can then work with affected asset owners (TOs, GOs, DPs, etc.) to drive additional or enhanced cyber security controls into future grid capital projects, including future infrastructure early in the design phase. This will enable asset owners to achieve additional funding mechanisms (e.g., through capital projects) to mitigate these risks where warranted.	TPs, PCs, TOs, GOs, DPs
2.2	**Refining Cyber Attack Scenarios:** TPs and PCs should use the studies outlined in the CITPF introduced in this white paper and continue to refine and develop a set of credible cyber attack scenarios that should be studied as part of annual planning assessments. These studies can inform enhancing the overall security posture of the BPS and will require collaboration across multiple stakeholders and organizations. Future multi-value capital projects (both electrical and cyber security controls) may be able to enhance the overall reliability, resilience, and security of the BPS more proactively than current practices today.	TPs, PCs

[50] https://www.nerc.com/comm/Documents/NERC_Security_Integration_Strategy_2022.pdf

Table 3.1: Recommendations and Applicable Entities Next Steps		
#	**Recommendation**	**Applicable Entities**
2.3	**Gathering Necessary Information for Studies:** With the list of credible attack scenarios developed, TPs and PCs should solicit necessary information from applicable entities to determine the extent of these possible attacks and refine their contingency definitions with this data. After refinement, TPs and PCs can conduct BPS reliability studies by using these contingencies to determine appropriate levels of risk.	TPs, PCs
2.4	**Cyber-Informed Transmission Planning Pilot:** The ERO Enterprise should conduct pilot projects by working collaboratively with registered entities and other stakeholders to test, validate, and implement the concepts outlined in this white paper. Findings from these pilots should be used to inform appropriate next steps in terms of codifying any enhancements to transmission planning practices and applicable NERC standards modifications.	NERC, Regional Entities, industry stakeholders
3. Future Enhancements to NERC Reliability Standards TPL-001 and CIP-014		
3.1	**Future Enhancements to TPL-001:** After the completion of pilot projects, the ERO Enterprise recommends enhancements to TPL-001 to incorporate the concepts of cyber-informed transmission planning into annual planning assessments and the overall transmission planning process. Currently, cyber attack is only considered an "extreme event" and not given the due diligence it deserves in today's modern world. Therefore, cyber contingencies derived from probable attack scenarios[51] should be developed by TPs and PCs, and the results of reliability studies should inform proactive risk mitigation through the deployment of security controls or transmission system upgrades where needed. TPs and PCs can help drive cyber security investments in areas where risk, particularly across multiple entities, can pose a significant risk to BPS reliability. Enhancements to TPL-001 should include (and be further informed by the pilot projects) the following: • Moving some of the cyber attack contingencies out of the extreme events table and into the main contingency table of the standard to clearly establish a design basis for cyber attack scenarios • Considering a new category of coordinated cyber attack contingencies in the main contingency table that can be studied uniformly by TPs and PCs • Allowing for TPs and PCs to tailor cyber attack scenarios based on local or regional needs and risks • TPs and PCs developing criteria for when and how entities (TOs, GOs, DPs, etc.) mitigate cyber attack risks for scenarios that warrant corrective action plans	NERC, Regional Entities
3.2	**Physical Security Considerations:** In alignment with NERC's recent filing on CIP-014, the ERO Enterprise recommends that the upcoming technical conference regarding physical security protections should also include considerations for eliminating the criticality of substations through modifications to system topology to improve the overall resilience of the BPS moving forward.	NERC, Regional Entities

[51] The goal is not to require TPs to study all cyber attack scenarios; however, threat intelligence combined with engineering judgement based on entity circumstances, experience, and risk reduction should be applied for the development of scenarios to be studied. The minimum set of required scenarios, and incorporation into any revised standards, would be determined by a future standards drafting team.

Table 3.1: Recommendations and Applicable Entities Next Steps		
#	**Recommendation**	**Applicable Entities**
4. Other Related Activities		
4.1	**Security Integration for Blackstart Studies:** This white paper does not address the reliability studies conducted for blackstart testing; however, the ERO Enterprise has identified opportunities for improvement regarding coordination between security and engineering disciplines in the area of system restoration under credible cyber attacks. EOP-005 requires the development, testing, sharing, coordination, and training of a restoration plan, both typically including steady-state and dynamic stability studies to ensure system performance criteria is met during restoration. EOP-005 is not prescriptive regarding the necessary details for such analysis; however, guidance should be developed to strengthen security integration in this area, particularly regarding recommendations and lessons learned for analysis of restoration plans considering serious cyber security compromise (and the possible unavailability of electronic networks, parts of the transmission system, communications, applications, and resources). These plans should be informed by both physical and cyber security assessments.	NERC Security Integration and Technology Enablement Subcommittee (SITES) and NERC Security Working Group (SWG)
4.2	**Simulation Tools Enhancements:** Current transmission planning models and simulation platforms do not represent the interrelation between BPS assets, protection systems, communications networks, security network architectures, equipment manufacturer information, fuel type, and other dependencies. Therefore, engineers and security professionals can make assumptions based on engineering and security judgment to develop attack scenarios. However, planning assessments could use automated contingency definitions in the future if this data is readily available and input into simulation programs. This will require significant enhancements to both engineering and security data with appropriate controls in place to secure this information. Regardless, it is something that industry should strive to accomplish in the coming years, particularly around supporting the development of cyber contingencies.	Simulation Software Vendors
4.3	**Secure Planning Assessment Models and Studies:** The models used to conduct TP and PC reliability studies contain detailed information about the connectivity of all elements on the BPS. The ERO Enterprise strongly recommends that all TPs and PCs ensure that these models are only provided to entities with a need-to-know basis and are not publicly posted or shared without adequate nondisclosure agreements in place. It is imperative that access to this data be protected with adequate security controls moving forward; compromise or corruption of this data could result in inaccurate reliability studies conducted by TPs and PCs. Generally, these models do not contain information that would be considered BCSI,[52] so the NERC CIP standards are not applicable. However, industry should develop and adopt guidelines around best practices for securing this information.	TPs, PCs, MOD-032 Designees, NERC SITES, NERC SWG

[52] Data may be classified as Critical Energy/Electric Infrastructure Information and should be protected according to its classification

Appendix A: Common Terms and Definitions

The following terms are defined for use in this white paper to ensure a common understanding between engineering and security professionals. The goal is to have a uniform and consistent means of describing both engineering and security topics to avoid confusion across disciplines.

Specific Terms Used in This White Paper

- **Roadmap:** The foundational plan for future incorporation of security concepts into transmission planning practices in a more holistic manner
- **Cyber-Informed Transmission Planning Framework (CITPF):** The adaptable concept and structure for transmission planning engineers to conduct long-term planning assessments that incorporate cyber security risks to improve the reliability and resilience of the BPS

Commonly Used Security Terms

The following terms and definitions are obtained from various sources:[53, 54, 55]

- **Attack:** Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself
- **Compromise:** The unauthorized disclosure, modification, substitution, or use of sensitive data (e.g., keys, metadata, other security-related information) or the unauthorized modification of a security-related system, device or process in order to gain unauthorized access
- **Cyber Security:** Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation
- **Cyber Threat:** Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service
- **Defense-in-depth:** Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization
- **Demilitarized Zone (DMZ):** A perimeter network or screened subnet separating an internal network that is more trusted from an external network that is less trusted
- **Industrial Control System (ICS):** An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes
- **Information Technology (IT):** Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.

  In this definition, equipment is used by an executive agency if the executive agency uses it directly or it is used by a contractor under a contract with the executive agency that requires the following:

[53] https://csrc.nist.gov/glossary
[54] https://www.nerc.com/files/glossary_of_terms.pdf
[55] Based on SANS definition: https://www.sans.org/blog/nation-state-threat-actors-from-a-security-awareness-perspective/

- The use of such equipment
- The use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product

The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

- **Intelligent Electronic Device:** Any device incorporating one or more processors with the capability to receive or send data/control from or to an external source (e.g., electronic multifunction meters, digital relays, controllers)
- **Interactive Remote Access:** User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol

  Remote access originates from a cyber asset that is not an Intermediate system and not located within any of the responsible entity's electronic security perimeter(s) or at a defined electronic access point. Remote access may be initiated from the following:

  - Cyber assets used or owned by the responsible entity
  - Cyber assets used or owned by employees
  - Cyber assets used or owned by vendors, contractors, or consultants (Interactive remote access does not include system-to-system process communications.)
- **Mitigation:** A decision, action, or practice intended to reduce the level of risk associated with one or more threat events, threat scenarios, or vulnerabilities
- **Nation-State Threat Actor:** Highly trained, motivated, resourced, and mission-focused threat actors working within the legal guidelines of their own country
- **Operational Technology (OT):** Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment)

  These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.
- **Programmable Logic Controller:** A solid-state control system that has a user-programmable memory for storing instructions for the purpose of implementing specific functions, such as I/O control, logic, timing, counting, three mode (PID)[56] control, communication, arithmetic, and data and file processing
- **Risk:** A measure of the extent to which an entity is threatened by a potential circumstance or event and typically a function of the following:
  - The adverse impacts that would arise if the circumstance or event occurs
  - The likelihood of occurrence
- **Security Control:** A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements
- **Supervisory Control and Data Acquisition (SCADA):** A system of remote control and telemetry used to monitor and control the transmission system

[56] There are three basic controller modes, the proportional controller (P), the integral controller (I), the derived controller (D). A PID controller controls a process through three parameters: Proportional (P), Integral (I), and Derivative (D).

Typical uses of SCADA include power transmission, distribution, and pipeline systems. SCADA was designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that must be used (such as phone lines, microwave, and satellite). Usually shared rather than dedicated.

- **Threat Actor:** An individual or a group posing a threat
- **Vulnerability:** Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source

Comparison and Clarification of Select Definitions

This section describes definitions used by both engineering and security disciplines to illustrate the differences and provide clarity on their use.

Contingencies

The term "contingency" is generally used to refer to the same concept (i.e., the loss of an asset, element, or system) but is used in very different contexts between TPs and security professionals:

- **Transmission Planning Context:** TPs model and study the outage of BPS elements and refer to the outage as a contingency (e.g., the loss of a transmission line, transformer, generator). A contingency definition defines the specific elements affected during the simulated event. Contingency definitions can include changes in status (i.e., off/on), changes in control set points, changes in protection settings, and many other ways in which an element could be modified, manipulated, or disconnected. TPs then conduct studies to identify whether the BPS meets specific performance criteria (e.g., voltage levels, thermal overloads, stability) for the specified contingency studied. These studies assume specific demand levels, generation patterns, and dispatch scenarios in addition to the contingency applied. Contingency analysis is a term used in transmission planning referring to automated tools and functions built into simulation platforms that will execute these studies for planners. Figure A.1 shows a "contingency solution" window in the tool that is used to select the study parameters and engineering assumptions that go into the analysis.

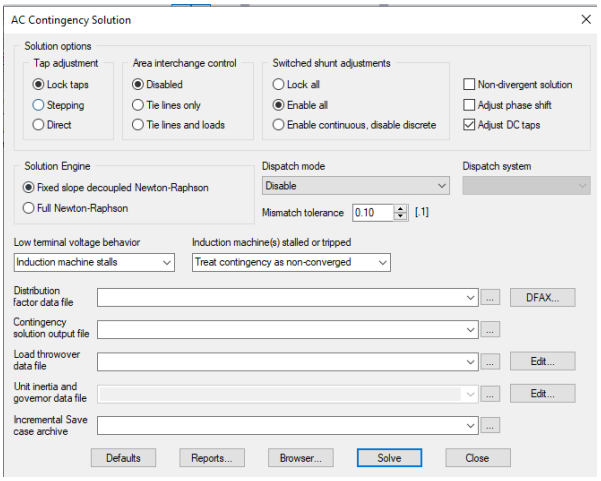


Figure A.1: Example Simulation Tool Contingency Solver [Source: PSS®E]

- **Cyber Security Context:** Cyber professionals view contingency planning as a combination of business continuity planning, incident response, and disaster recovery planning. The goal of business continuity planning is to provide a quick, calm, and efficient response in the event of an emergency and to enhance a company's ability to recover from a disruptive event promptly. The key is minimizing the impact of disruptive events such that business continuity is not broken. If a disruptive event breaks business continuity, then disaster recovery takes over.[57] Business continuity planning includes assessing risks to organizational processes and creating policies, plans, and procedures to minimize the impact of those risks; maintaining the continuous operation of a business in the event of a disruptive event; and planning for disaster recovery (a separate but related process) in the event business processes have stopped. This includes four main steps: project scope and planning, business impact assessment, continuity planning, and approval and

[57] Source: CISSP (ISC) 2 Certified Information Systems Security Professional Official Study Guide 7th Ed.

implementation. Disaster recovery planning addresses scenarios not sufficiently covered by the business continuity plan. For example, a business continuity plan may require a hot backup server for a critical software application to ensure a business process continues to function in the event of the loss of a server. This business continuity process would likely fail in the event the computer room housing the two servers were to be lost in a natural disaster. This is where disaster recovery planning comes in and most likely includes a plan to restore or relocate the computer room.

Both contexts consider the "contingency" as the loss of one or more assets, elements, or systems. Each discipline then plans either to withstand that loss or to recover from the loss expeditiously.

Control

The term "control" refers to different concepts within engineering and security disciplines. The following is a brief description of the differences:

- **Cyber Security Context:** This is a technical, administrative, or physical mechanism inserted into a process with the objective of detecting, preventing, or mitigating cyber threats and attacks. Mechanisms range from physical controls including security guards and surveillance cameras, technical controls (including firewalls), and multi-factor authentication to administrative controls, including cyber security awareness training and cyber incident response plans.
- **Engineering Context:** This is a logical or mathematical process by which information, data, or signals can be processed from an input to output (see **Figure A.2**). Related to control theory, the engineering controls study and dictate the parameters, logic switch positions, and filters to design an interface that allows a controller to dictate behavior to a system and incorporates feedback through sensor arrays.

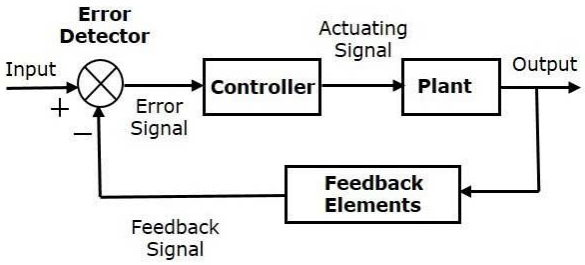


Figure A.2: Example of Engineering Control Block Diagram

Impact

The term should be understood in the context of the section in which it is used in the paper. Generally, for transmission planning engineers, impact means the electrical effects that an event (i.e., a contingency) has on the BPS, generally in terms of quantities defined by voltage, frequency, loading levels, stability margins, etc. While in security terms the definition is, "magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability."

Network

The term "network" is potentially ambiguous. The meaning is different between the security and engineering realms. Throughout this white paper, the terms "transmission network" and "communication network" have been used to provide clarity when necessary and alleviate any potential confusion for the reader. From an IT security perspective, NIST defines the term as follows:

> "*Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.*"

While from an engineering perspective, the term described the transmission system, its topology, and the various components that comprise the system (e.g., transformers, lines, substations, switching equipment).

Risk

Engineers most commonly define risk by using the basic tenets of likelihood and consequence:

$$Risk = Likelihood\ of\ Occurrence * Consequence\ of\ Occurrence$$

However, cyber security professionals will often describe risk with slight differences to that basic calculation. An initial cyber risk calculation could look like this:

$$Cyber\ Risk = Consequence * Threat * Vulnerability$$

NIST defines cyber security risk as "an effect of uncertainty on or within information and technology. Cyber security risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation."[58]

Dragos defines industrial cyber risk for OT/ICS communication networks as "The potential loss of life, injury, damaged assets, financial loss, and other harm from the failure or misoperation of digital technologies and communication networks used for operational capabilities."[59]

$$Industrial\ Cyber\ Risk = Consequence * \frac{Threat * Vulnerability}{Resilience}$$

All of these definitions of risk can be used appropriately so long as the context is clearly defined.

[58] https://csrc.nist.gov/glossary/term/cybersecurity_risk
[59] https://www.dragos.com/resource/industrial-cyber-risk-management/

Appendix B: Recommendation from IEEE–NERC Security Project

IEEE and NERC jointly published a technical report[60] that outlined the concept of security integration with respect to transmission planning, design engineering, system operations, and emerging technologies. The report provided a high-level overview and introduction to the topic and laid a foundation for future work in this area. The report included a chapter on integrating cyber and physical security into long-term transmission planning. The following concepts are introduced in that report and addressed in this white paper:

- Identifying security-related threats posed to the BPS, developing risk-based criteria to evaluate the adverse reliability impacts of these threats, and to develop mitigations (transmission upgrades, operating plans, or mitigating security controls) where appropriate
- Enhancing industry study of coordinated cyber attacks on the BPS and determining which coordinated attacks warrant enhanced security controls to mitigate due to their BPS reliability impacts
- Supporting enhanced cyber security investments on the BPS where a credible compromise could result in unreliable operation of the BPS, specifically to mitigate instability, uncontrolled separation, and cascading outages
- Consideration of cyber (and physical) attacks on the BPS and the impacts they could have on long lead-time equipment
- Focus on communications systems and the adverse impact to BPS reliability that could be posed by maliciously disabling protection systems, remedial action schemes and other critical systems that could affect multiple BPS elements, and studying the effects of delayed clearing for multiple BPS elements beyond current planning practices
- Studying the manipulation in addition to the outage of equipment that could adversely impact BPS reliability and equipment integrity
- Studying the widespread compromise of DERs as a credible coordinated cyber attack scenario, particularly as the penetration of DERs grows across North America and because many DERs are directly connected to the internet with minimal mitigating security controls
- Leveraging CIP-014 studies to identify critical stations or substations and to ensure sufficient cyber security controls are implemented for these locations and minimizing the number of critical locations on the BPS through multi-value transmission system upgrades in conjunction with mitigating security controls
- Securing transmission planning data due to the criticality and confidentiality of the data contained within planning base cases, contingency definitions, etc. (Transmission planning data should be protected at the same level as other BCSI.)
- Expanding TP understanding of the connectivity of electronic devices that control BPS elements that could be affected by a single or coordinated cyber attack, particularly focusing on the connectivity and controllability of assets from entities that are not NERC related registered entities

  This includes a focus on vendor and equipment manufacturer access and controllability of assets across the BPS and incorporating those potential threats in the transmission planning studies.
- Publishing educational material that supports cross-departmental understanding of both engineering and security practices in a holistic manner, specifically focused on enhancing collaboration and coordination among departments and entities

[60] https://resourcecenter.ieee-pes.org/publications/technical-reports/PES_TP_TR105_PSCC_120622.html

Appendix C: In Depth Alternate Step 1

This appendix describes a more detailed process for **Step 1** (in Chapter 1). Limitations to the described process include the unavailability of cyber security staff to work with TPs or the unavailability or infeasibility of collecting technical data associated with specific TO, TOP, GO, and GOP facilities in the planning footprint. In such cases, chosen attack scenarios can be simplified to root cause (i.e., type of threat) and potential system impacts (translatable to contingencies) for broad study of the scenario across an area. Understandably, mitigating cyber security controls prescribed from a resulting study may likewise be broad and generalized to address the threat(s) associated with the attack scenario. As a result, security vulnerability assessments may be identified as a high-priority follow-up activity to develop further details and better inform subsequent studies to provide a more comprehensive analysis. Studying generalized high-level cyber security scenarios and analyzing the results should still enable planners to identify and address potential reliability impacts within their areas. The remainder of this chapter assumes security professionals and engineering team resources are available to conduct the more detailed alternate **Step 1** process.

Known threat vectors should be a focusing lens of an organizational (individual) or regional (collaborative) effort intended to identify electrical impacts needed by planners in their studies. The threat vector is used to scope a vulnerability assessment of communication networks, systems, and assets most likely to be exploited as part of a cyber attack, including the targeted electrical system components. Vulnerability assessment results can be further filtered to those assets and impacts that can be reasonably studied and are relevant to TPs, thus identifying unique contingencies related to cyber threats not traditionally studied. **Figure C.1** illustrates this concept.

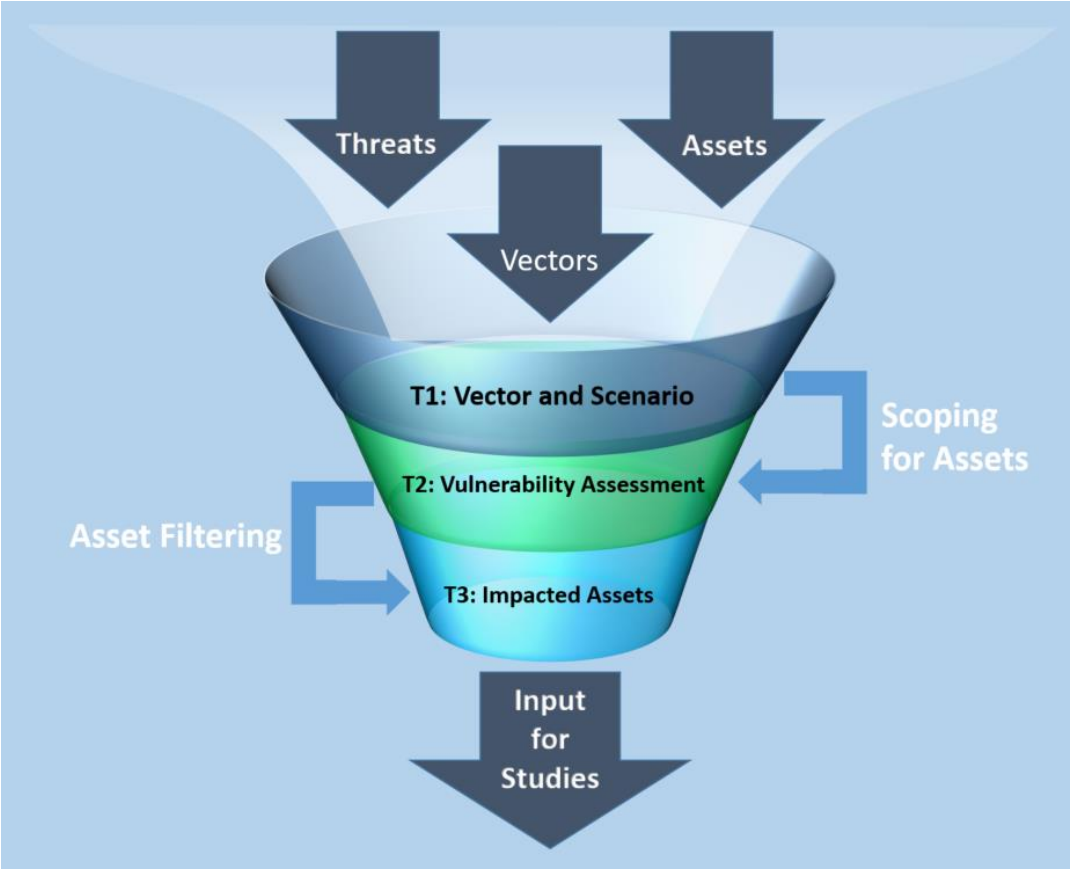


Figure C.1: Tasks 1–3 Threat Vector and Attack Scenario, Scoping, and Impacted Assets

Task 1: Threat Vector and Attack Scenario Selection

This task can be broken down into two sub-components: selecting threat vectors and developing accompanying attack scenarios along with their associated kill chains.

Select Threat Vector

Industry risk assessments provided by NERC, E-ISAC, CISA, and others may highlight present and emerging threats to the BPS that could be useful in deriving valuable studies by TPs. These threats represent trends of vulnerabilities or actual attacks observed in the electric sector, other interdependent industries (e.g., telecommunications, natural gas), or the global cyber landscape at-large. Threat vectors may be prioritized by identifying existing security control gaps in equipment technical standards, regulatory standards, or security frameworks. Entities can also perform their own internal vulnerability assessments by using available threat intelligence to make an independent selection of threat vectors to consider.

Cyber Threat Contingencies

Cyber security professionals review credible threats, attack vectors, and possible compromise scenarios in conjunction with conducting scoped cyber security vulnerability assessments to identify and document possible impacted assets. This step defines a set of scenarios that TPs can then use to develop "contingencies" in their planning studies. In particular, the aggregate risk to affected elements caused by common security control gaps is of primary concern.

To avoid redundancy with currently required transmission planning studies,[61] threat vectors that could result in the outage of multiple elements at one location or across multiple locations should be selected. To assist in this effort, **Table 1.1** (in Chapter 1) identifies some prioritized attack scenarios for contingency study. Additionally, multiple threat vectors may present potential overlap in impacts to power system assets. Where impact overlap can be identified between multiple threat vectors and there is clear applicability of those threat vectors to the system or assets within the planner's scope, those threat vectors may be grouped in a single study and developed uniformly into contingencies in **Step 2.** While this allows efficiency gains, consideration of each individual threat vector may be relevant to recommending mitigating controls during the creation of corrective action plans.

Scenario and Kill Chain Development

After a threat vector is selected, an attack scenario should then be produced to add levels of detail on how the threat vector leads to impact of BPS assets. Resources like the Lockheed Martin Cyber Kill Chain®[62] framework and MITRE ATT&CK® Matrix for ICS[63] tool are available to assist in developing a hypothetical kill chain. These tools can support scoping the vulnerability assessment conducted in **Task 2**. A comprehensive kill chain can also aid in identifying mitigating security controls to address unacceptable reliability risks.

Task 2: Scoped Vulnerability Assessment

Conducting vulnerability assessments requires dedicated cyber security professionals or third-party expertise. Additionally, the entity conducting the assessment must own the assets under consideration in order to have access to the necessary data input sources for the evaluation. Alternatively, a collaborative effort between multiple entities should be conducted where possible. Publicly available resources are available for evaluating vulnerability assessment efficacy, such as NIST SP 800-115.[64] The following items are necessary to conduct effective vulnerability assessments:

- **Scope:** Evaluate the threat vector and attack scenario against the following to scope the appropriate communication networks, systems, and assets to include in the vulnerability assessment:

[61] Mandatory studies defined in the currently effective version of NERC TPL-001 and CIP-014
[62] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
[63] https://attack.mitre.org/matrices/ics/
[64] https://csrc.nist.gov/publications/detail/sp/800-115/final

  - Asset groupings—physical locations and logical communication network segments
  - Shared design interdependencies (shared telecomm, power sources, HVAC, protection and control, manufacturers and support access)
  - Associated software, hardware, and communication protocols
- **Inputs:** Obtain the following data as assessment input:
  - Assets list including function and criticality
  - Data flows
  - Communication network architectures
  - Existing security controls
- **Outputs:** Perform vulnerability assessment, producing the following outputs:
  - Lists of vulnerable assets (network devices, servers, workstations, HMI, relays, etc.)
  - Associated vulnerabilities
  - Control gaps or identified weak controls

Task 3: Impacted Assets

The final task is to filter the vulnerability assessment results down to only the impacted assets that a planner needs to conduct a planning simulation. Hardware, software, and related architectural designs may all have vulnerabilities identified in the preceding step. These components and associated systems should be ranked in terms of criticality to the BPS functionality they provide. This provides the first potential filter of the data set as overall results may need to be filtered to align with planning requirements necessary to perform the related studies. After all, a planner cannot study loss of all BPS elements at once. This cyber-informed transmission planning endeavor is attempting to locate the cutoff for cyber attacks that is both beyond currently studied contingencies and below extremely complex and impossible to study contingencies.

In order to reduce complexity and enable valuable study inputs, existing security controls should be used to further filter out particular attack scenarios and associated impacted elements. For example, if the asset being considered is a NERC CIP medium-impact BCS (e.g., a substation asset) with external routable connectivity, then required multifactor authentication controls would reasonably filter out an attack scenario that attempts to remotely compromise a system with stolen credentials alone. Another filter set may include identification of common mode vulnerabilities, such as use of the same third-party vendor across multiple assets. Where a number of assets may use the same wind turbine manufacturer and have the same remote support contracts and mechanisms in place, other assets may be filtered from a relevant supply chain compromise attack scenario due to the absence of this vendor equipment and remote support capabilities.

For modeling purposes, the loss of availability impacts should be prioritized over the loss of visibility or control impacts. System state change is not necessarily a consequence of loss of visibility or control but may accompany them. Therefore, the question is whether human intervention to restore system state is dependent on visibility and control (very likely) and if it is reasonably feasible to address that dependency with a study. Furthermore, the mitigation efforts resulting from studying loss of availability impact may also mitigate visibility and control impacts from the same threats. Loss of availability of electrical assets presents planners with clear effects to system states; therefore, it is the most straightforward type of impact to model.

Once existing security controls and other applicable filters are applied and the remaining assets are ranked for criticality, the associated assets can be mapped to electrical impacts should they be compromised through the selected and vetted attack scenarios. The activities in this step are dependent on both cyber security professionals

and engineering teams. The output of this step is a list of elements that a planner can outage as a result of any one (or combined) hypothetical cyber security attack.

Example of Cyber Attack Scenario

Wind energy generation plants contract with wind equipment manufacturers, and these OEMs often have remote access to the generation sites that they use for performing maintenance and other functions necessary for normal plant operations. A supply chain compromise of a wind OEM vendor may result in the malicious use of the legitimate remote access implementations, resulting in a potential aggregated compromise of multiple generation plants.

The hypothetical attack scenario is as follows:

- A phishing email is sent to an OEM that contains links to a malicious site.

OEM staff active directory communication network credentials are compromised.

Attackers gain access to an IT enterprise network and compromise an active directory domain controller.

VPN credentials that allow remote access to OEM client sites are stolen.

Attackers are able to remotely access OEM client wind generation plants.

Malicious software is remotely installed at some percentage of OEM client sites.

The malicious software is designed to shutdown turbines at a given date regardless of active communication network connectivity.

After shutdown, the malicious software also overwrites the controller firmware and reboots the device, preventing it from functioning.

The above attack scenario results in some percentage of the OEM client's wind turbines shutting down, resulting in a contingency for TPs to study. **Table 1.2** (in Chapter 1) shows a hypothetical list of wind generation assets affected in the scenario.

A similar hypothetical plant-level attack scenario is graphically represented in **Figure C.2.** The attack scenario is also mapped to the MITRE ATT&CK for ICS in **Figure C.3**. This process creates a cyber kill chain, which security professionals can use to identify, prioritize, and place mitigating security controls.

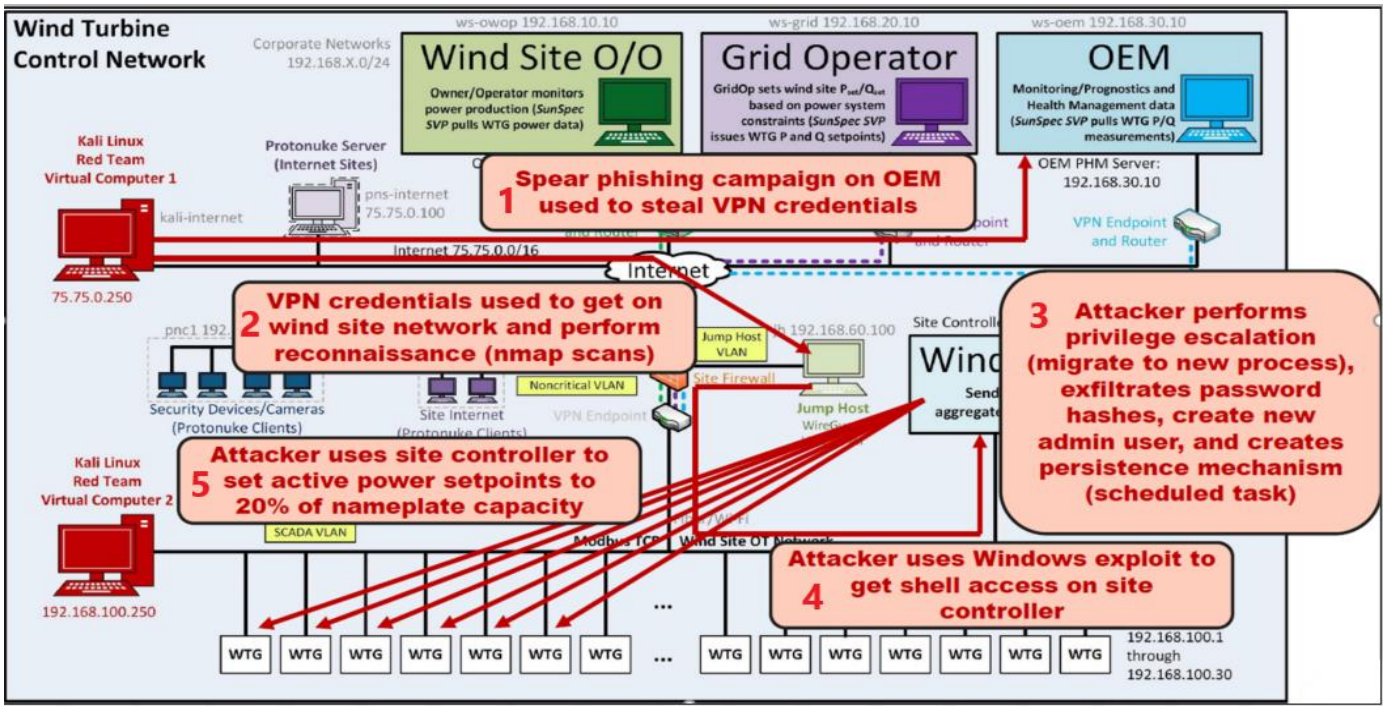


Figure C.2: OEM Remote Access Exploited—Wind Generation Asset [Source: Sandia]

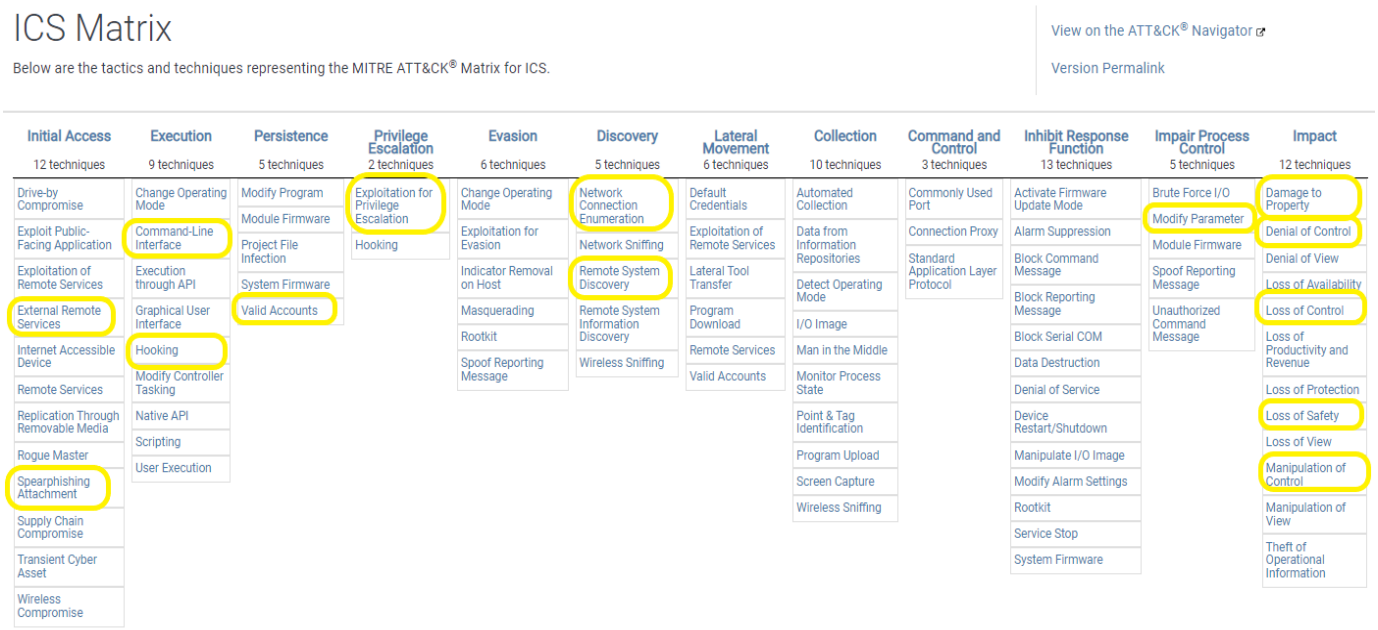


Figure C.3: OEM Remote Access Exploited Mapped to MITRE ATT&CK for ICS[65]

[65] https://attack.mitre.org/matrices/ics/

Appendix D: Example Study of Wind Turbine OEM Compromise

Study 1 from **Table 1.1** (of Chapter 1) of **Step 1** in the CITPF highlights the potential threat of OEM compromise, particularly for facilities that allow remote vendor access. In essence, a supply chain compromise could affect a significant number of generation facilities if the vendor (OEM) is compromised and a bad actor maliciously leverages authorized remote access. This study was selected as an illustrative example here due to risks identified with coordinated attacks affecting multiple low impact BCS that result from control gaps in the NERC CIP standards.

The ERO Enterprise conducted a high-level review of wind turbine OEMs across North America to explore the potential aggregate risks posed. This section briefly describes the steps taken to translate the potential security threat into data necessary for a transmission planning study as outlined in **Chapter 1**.

The following observations were drawn from the study:

- Generation assets are typically low impact BCSs; however, as the NERC LICRT team indicated a risk of a coordinated attack having a significant aggregate impact on multiple facilities exists.
- GOs or GOPs may allow remote access capability for OEMs either through maintenance or service agreements that allow the OEM to perform firmware updates, to transmit files or other information, and to monitor the status of assets across the OEM footprint.
- While the remote access capability is relevant to multiple types of inverter-based generation (i.e., wind, solar PV, battery energy storage systems), wind turbine manufacturer data was readily available via NERC Generation Availability Data System-Wind and EIA Form 860.[66]
- The data sources were used to identify the aggregate capacity of various wind turbine OEMs across each Interconnection and proved that the installed capacity of certain wind turbine OEMs greatly exceeds the resource loss protection criteria in each Interconnection (see **Table D.1** and **Figure D.1**). Given the plausible attack scenario, a credible situation existed to study the electrical impact of the compromise of these facilities in greater detail:
  - A worst-case scenario where OEM remote access to every generation asset allowed for propagation of malicious software is possible. Although it is unlikely that every facility allows remote access and that every wind turbine is producing power at a given time, a capacity factor[67] of 0.25 was used to estimate the amount of turbines producing power at the time of a potential compromise. These estimates still exceeded the resource loss protection criteria for each Interconnection, demonstrating the gravity of the risk posed.
- This potential risk was identified by analyzing security control gaps and identifying the number of assets exposed to the risk. While specific security controls at any specific generation facility were not known for this specific study, **Figure D.2** and **Figure D.3** show simplified example network architecture diagrams that illustrate strong and weak control implementations.

[66] NERC GADS will gather solar PV inverter information in the 2024 time frame and EIA Form 860 does not have an inverter manufacturer field capturing capacity of solar PV nor battery energy storage system data.
[67] Wind Energy Factsheet - Center for Sustainable Systems

Table D.1: Capacity of Wind OEMs by Regional Entity							
OEM	Eastern Interconnection (MW)			Texas Interconnection (MW)		Western Interconnection (MW)	Total (MW)
	MRO	NPCC	RF	SERC	Texas RE	WECC	
1	23,053	968	7,370	1,679	17,067	6,627	56,763
2	16,622	2,429	4,384	1,110	5,904	7,584	38,032
3	14,120	152	2,048	528	5,787	5,678	28,313
4	920	0	200	0	3,681	399	5,200
5	444	0	0	0	1,703	639	2,785
6	1655	0	132	0	182	150	2,119
7	244	0	338	0	0	949	1,531
8	98	125	400	0	0	145	768
9	399	0	0	0	299	0	698
10	0	0	0	0	0	535	535
11	110	0	0	0	362	0	471
12	150	0	139	0	0	0	289
13	30	0	0	66	0	0	96
Total*	57,843	3,673	15,011	3,382	34,984	22,707	137,600

* Totals may differ slightly from table due to rounding

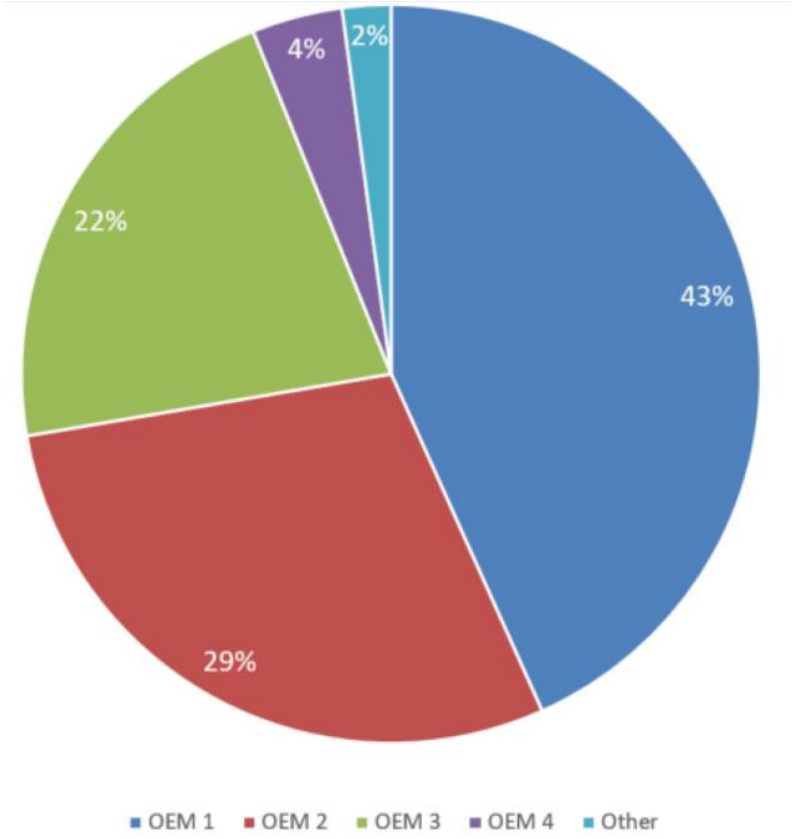


Figure D.1: Wind Turbine OEM Capacity across NERC Footprint

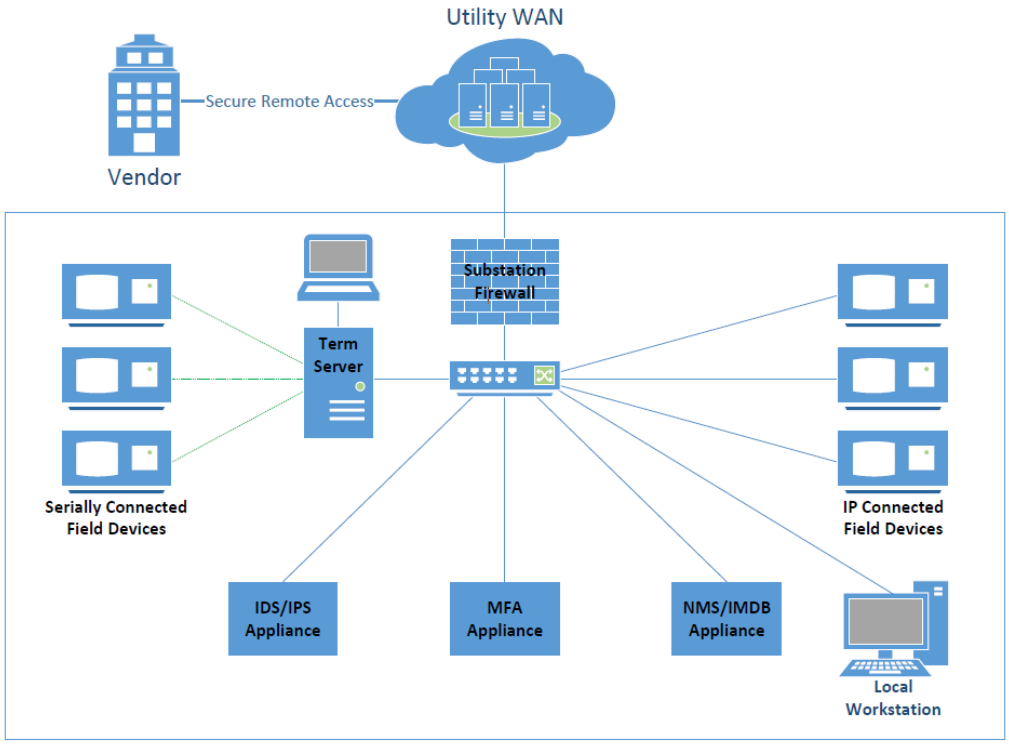


Figure D.2: Generic Diagram of Strong Security Controls at a Wind Generation Plant

Figure D.3 highlights a lack of security controls, particularly multi-factor authentication for vendor remote access, which poses a risk to BPS reliability from a credible coordinated attack. This high-level assessment illustrates a potential risk of coordinated attack through equipment manufacturers; however, each TP and PC would need to understand specific GO and OEM practices within their footprint in order to complete a more detailed study of possible risks to BPS reliability. This will require the TPs and PCs to conduct surveys or use other data from these entities where necessary. Potential data points collected from GOs/GOPs and OEMs that could be used to assess possible risks include, but are not limited to, the following:

- The impact rating of BCSs for each location
- OT security controls in place
- Third-party or OEM remote access capabilities at each location
- The following OEM-centered data points:[68]
  - Internal security program maturity
  - Material procurement and supply chain risk management processes
  - Security awareness and training of employees
  - Identity and access management processes
  - Patching processes
  - Incident response plans
  - System recovery plans
  - Vulnerability management and vulnerability reporting processes
  - Change management procedures

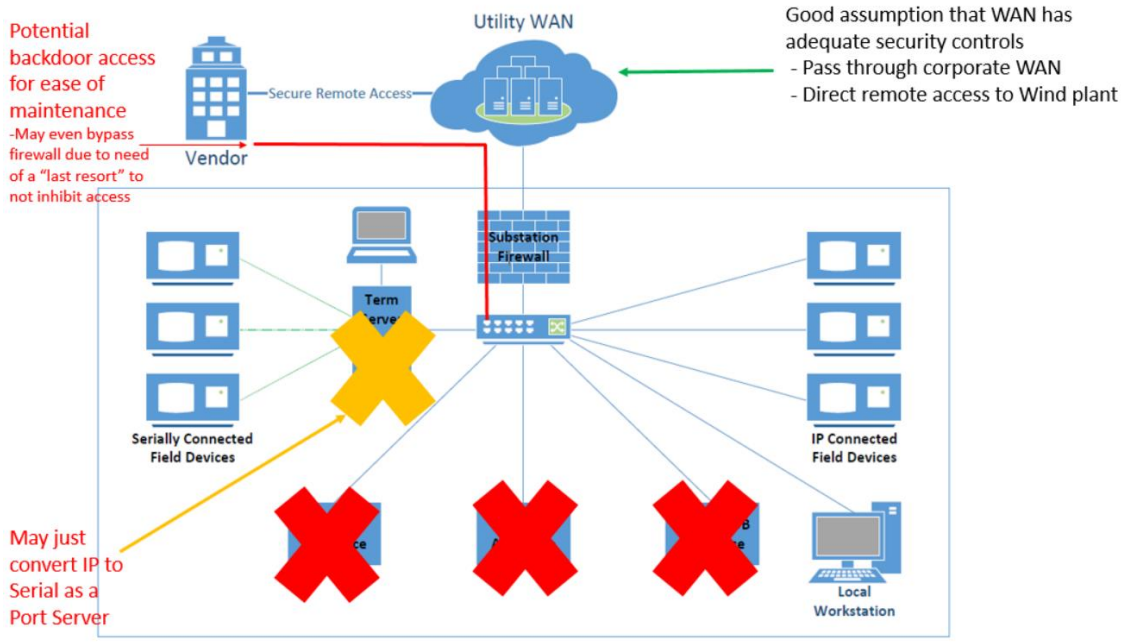


Figure D.3: Generic Diagram of Weak Security Controls at a Wind Generation Plant

[68] The GO may query the OEM or the TP/PC may query the OEM for a broader-level understanding of security practices in place.

Appendix E: Defense-in-Depth and Cyber Security Controls

There is no "silver bullet" for cyber security. The threat landscape is constantly changing, and adversaries are continually gaining new abilities to exploit vulnerabilities. Defense-in-depth is a strategy used in many industries where multiple layers of protections are implemented to defend a specific asset, system, or environment from compromise. For example, power system protection leverages this concept regarding primary and backup protection as well remedial action schemes and safety nets. This defense system is also used in the security space to ensure there are multiple layers of security controls in place to protect assets, communication networks, and associated critical systems. If any one line of defense fails or is compromised, additional layers can help ensure that threat actors are stopped before significant adverse impacts are realized. In the event of a breach, additional layers of defenses serve to impede the progress of adversaries, allowing for longer detection times for defenders. Defense-in-depth is an effective concept that enables a strong cyber security posture and may include security controls and concepts, such as those found in **Figure E.1**.

Figure E.1: Defense-in-Depth Components

The degree to which defense-in-depth is achieved can vary greatly based on regulatory requirements, the type of environment, and the personnel available to implement the controls. NERC CIP standards establish the minimum set of security controls needed to protect the BES. Predicated on a BCS classification system, entities are required to accomplish security objectives set forth in the standards. Generally, BCS are classified as low, medium, or high impact.[69] As an overview, **Table E.1** describes the necessary security measures applicable to low-, medium-, and high-impact BCSs. The table also provides a comparison of the security controls for each classification of BCS. Defense-in-depth strategies for an overall utility and a more detailed discussion of specific implementation considerations for substations are also discussed below.

Note: Increased cyber risk exists where security controls are not in place.

[69] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf

Table E.1: Security Controls per NERC CIP BCS Classification		
Security Measures	**Low Impact**	**Medium/High Impact**
Cyber Security Policies	✓	✓
Security Awareness and Training	✓	✓
Physical Security Controls	!	✓
Electronic Access Controls	!	✓
Incident Response Program	!	✓
Removable Media/Transient Device Controls	!	✓
Personnel Risk Assessments (Background checks)	✗	✓
Access Management Program (Authorization/Revocation)	✗	✓
Electronic Security Perimeter	✗	✓
Remote Access Management (Multifactor Authentication, Encryption, etc.)	✗	✓
System Security Management (Patching, Ports, Services, Malicious Code Detection)[70]	✗	✓
Security Event Monitoring	✗	✓
Recovery Plans	✗	✓
Configuration Change Management	✗	✓
Vulnerability Assessments	✗	✓
Information Protection	✗	✓
Supply Chain Risk Management	✗	✓

✓ Indicates comparable security controls that meet the security objectives

! Indicates partial implementations of security controls with one or more gaps in a security objective

✗ Indicates a lack of comparable security controls to achieve a security objective

As shown in **Table E.1**, several categories of security controls are not required for low impact BCS. Alternatively, if the category is addressed for lows, the required controls are not as robust as those for high- or medium-impact BCSs. For example, although inbound/outbound electronic access controls are required for communications entering or leaving the low impact BCSs, there is no requirement for multifactor authentication for remote access. Similarly, the physical security controls for lows are not as robust. For example, logging and alerting of physical access attempts into a low impact BCS is not required. These requirement differences are based on the consequences to the BES if such an individual asset was to be compromised. In the increasingly converging IT and OT space, lines of communications, compute, storage, transport of data and remote control are being increasingly integrated. These

[70] Low impact BCSs do not require malicious code detection within the BCS; however, malicious code detection is required for transient cyber assets and removable media prior to use (i.e., temporary devices plugged into a low impact BCS/BCA, such as maintenance laptops or removable storage.

realities inherently increase the attack surface of these critical systems. The risk of coordinated attack across multiple low impact BCSs is present and represents opportunities for improving the security posture of the electric power system.

Defense-in-Depth Concepts

In addition to technical controls, defense-in-depth includes internal controls, such as governance, security policies, asset management programs, supply chain procurement processes, and others. **Figure E.2** shows a high-level example of defense-in-depth achieved through technical controls in a hypothetical environment; a facility is connected to the control center through the firewall. IP-connected field devices, local workstations, a terminal server, serial-connected field devices, switches, several security devices are shown along with communication network segmentation. The following are examples of technology controls that contribute to defense-in-depth:

- **Firewall:** Configured access control lists with out of band management, whitelisted IPs for management nodes, default deny all policies, periodic reviews of configured policies, malicious code detection licensing
- **Remote Access:** Secure architectures that include a demilitarized zone, intermediate systems, and encryption along with a protocol break at the intermediate system
- **Jump Host:** Provides a network isolated and hardened intermediate system for remote access purposes only
- **Session Monitoring:** Remote access session monitoring and termination capabilities (not shown)
- **Multifactor Authentication:** A multifactor authentication appliance or server provides multifactor authentication for access to networked resources; this is critical for secure remote access implementations.
- **Communication Network Segmentation:** Devices may be physically and/or logically segmented to establish network boundaries where security controls can be deployed to manage traffic between segments (e.g., firewall access control lists)
- **Internal Network Security Monitoring:** Monitoring of communication networks for malicious content (e.g., malware and adversary lateral movement over the communication network), alerting on the presence of malicious communications, network traffic baselining (e.g., ports, protocols), automated asset inventories (e.g., hardware, software, firmware), logging and log protection
- **Authentication Server:** Active directory, lightweight directory access protocol, remote authentication dial-in user service, or terminal access controller access-control system
- **Security Information and Event Management:** Collects log data from various devices, identifies activity that deviates from the norm with real-time analysis, and sends alerts

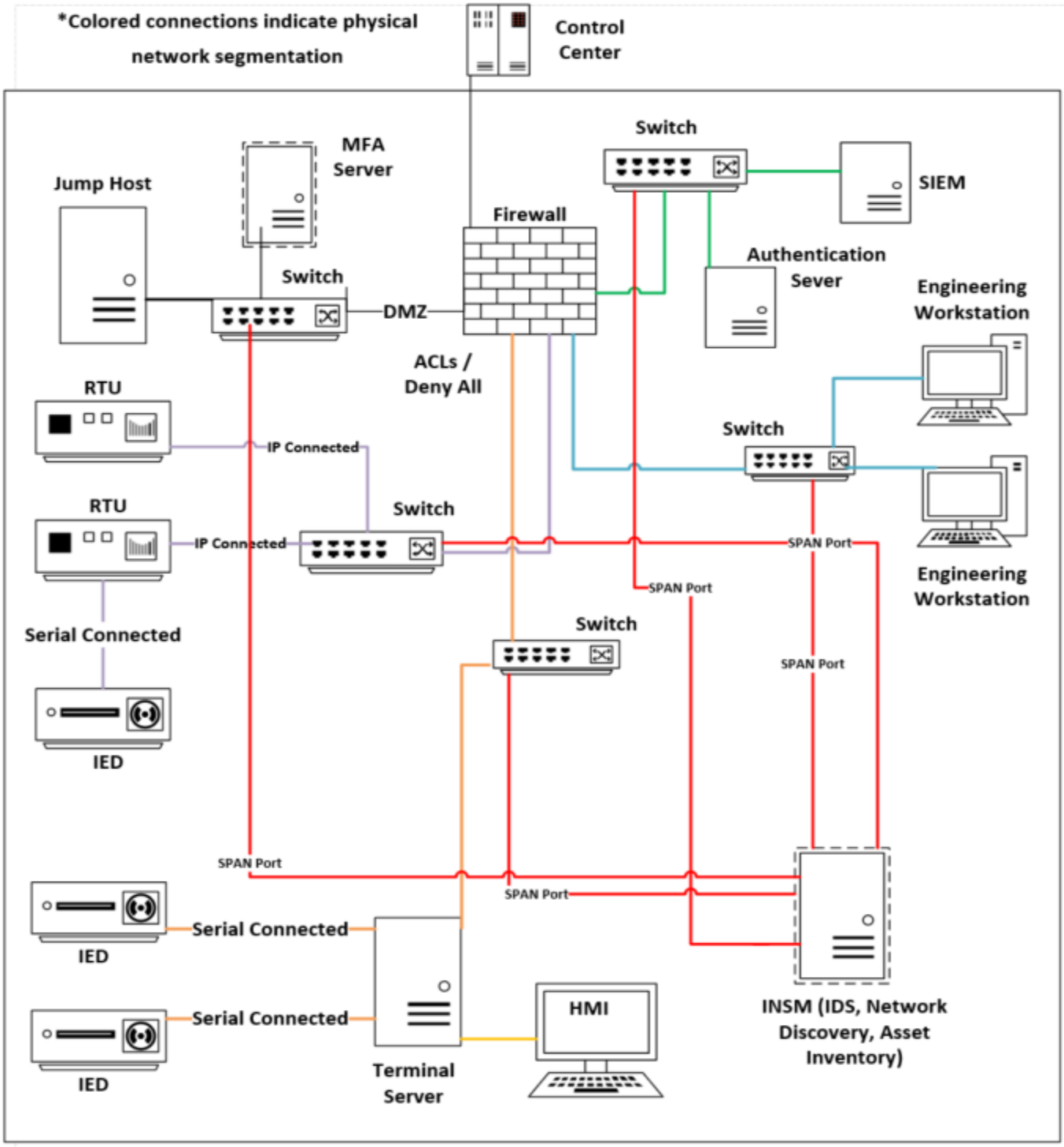


Figure E.2: Substation Defense-in-Depth

Appendix F: List of Contributors and Acknowledgments

The following individuals were involved in the development and conceptualization of the CITPF. This group included a team of ERO Enterprise engineering and security professionals working collaboratively across disciplines to identify ways in which enhanced coordination and collaboration could result in a more cyber-resilient BPS.

Name	Company
Larry Collier	North American Electric Reliability Corporation
Dan Goodlett	North American Electric Reliability Corporation
Ryan Quint	North American Electric Reliability Corporation
John "JP" Skeath	North American Electric Reliability Corporation
Dianlong Wang	Midwest Reliability Organization
Shayan Rizvi	Northeast Power Coordinating Council
Johnny Gest	ReliabilityFirst
Gregory Hardin	SERC Reliability Corporation
Stony Martin	SERC Reliability Corporation
Brad Woods	Texas RE
John Graminski	Western Electricity Coordinating Council
Doug Tucker	Western Electricity Coordinating Council

NERC would like to acknowledge the joint IEEE–NERC team that developed and published *IEEE Technical Report #105: Towards Integrating Cyber and Physical Security for a More Reliable, Resilient, and Secure Energy Sector*, which serves as a foundation for the work conducted here.

The ERO Enterprise would also like to acknowledge the following individuals for their input, feedback, and review of this white paper prior to publication.

Name	Company
Craig Preuss	Black & Veatch
Richard Alcalde	Consolidated Edison
Matt Duncan	E-ISAC
Zachary Fields	E-ISAC
Ryan Guest	E-ISAC
Elvin Ramirez	E-ISAC
Marc Child	GRE, SITES Sponsor
Mohammad Reza Khalghani	IEEE
Mark Lauby	NERC
Carter Manucy	NRECA
Paul Stockton	Paul Stockton LLC
Brian Hallett	RF
Brent Sessions	WAPA, Security Working Group Co-Chair