NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Guideline

Cyber Intrusion Guide for System Operators: Version 2

March 22, 2023

RELIABILITY | RESILIENCE | SECURITY

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

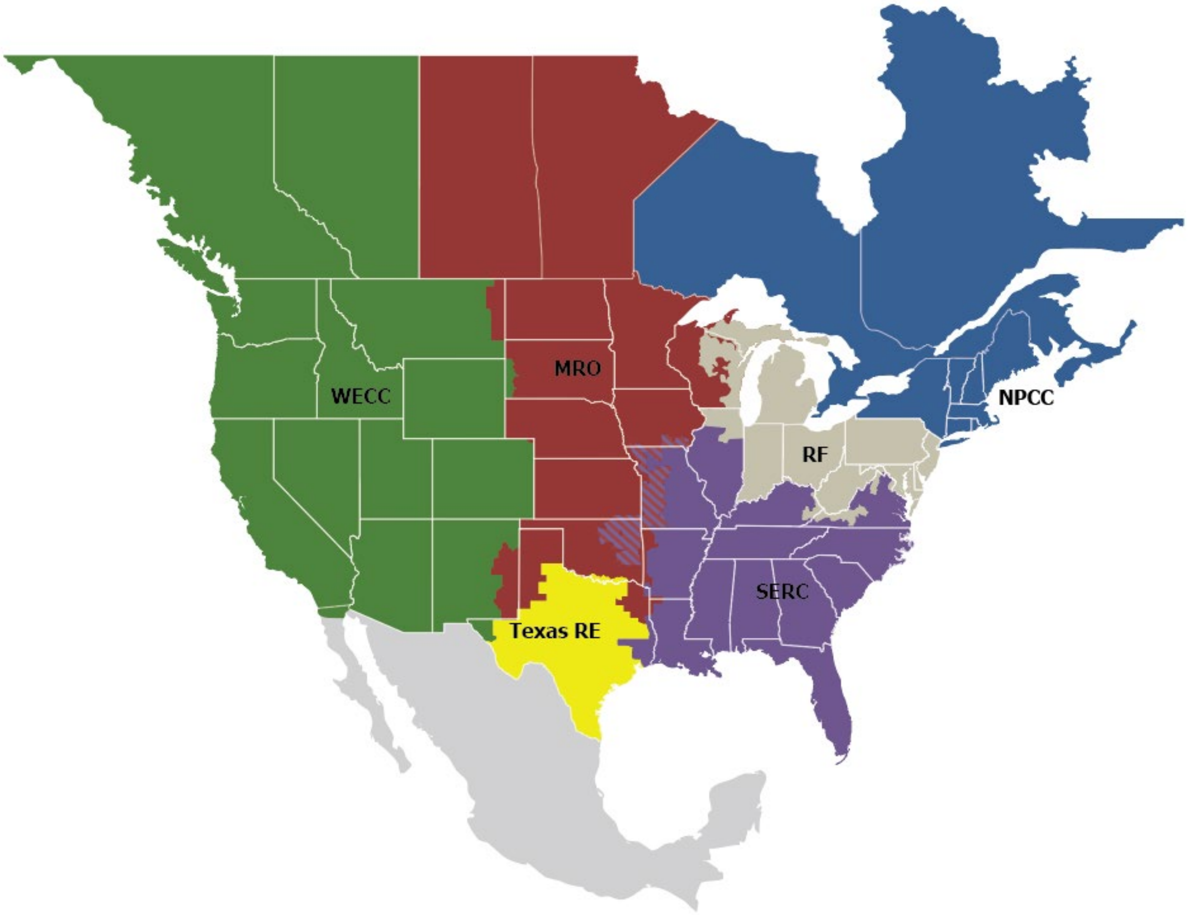
Table of Contents

Preface

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

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

The North American BPS is 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 (TOPs) participate in another.



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

Preamble

The NERC Reliability and Security Technical Committee (RSTC), through its subcommittees and working groups, develops and triennially reviews reliability guidelines in accordance with the procedures set forth in the RSTC Charter. Reliability guidelines include the collective experience, expertise, and judgment of the industry on matters that impact BPS operations, planning, and security. Reliability guidelines provide key practices, guidance, and information on specific issues critical to promote and maintain a highly reliable and secure BPS.

Each entity registered in the NERC compliance registry is responsible and accountable for maintaining reliability and compliance with applicable mandatory Reliability Standards. Reliability guidelines are not binding norms or parameters nor are they Reliability Standards; however, NERC encourages entities to review, validate, adjust, and/or develop a program with the practices set forth in this guideline. Entities should review this guideline in detail and in conjunction with evaluations of their internal processes and procedures; these reviews could highlight that appropriate changes are needed, and these changes should be done with consideration of system design, configuration, and business practices.

It is in the public interest for NERC to develop guidelines that are useful for maintaining and enhancing the reliability of the Bulk Electric System (BES). The subgroups of the Reliability and Security Technical Committee (RSTC)—in accordance with the RSTC charter[1] are authorized by the NERC Board of Trustees to develop reliability and security guidelines. These guidelines establish a voluntary code of practice on a particular topic for consideration and use by BES users, owners, and operators. These guidelines are coordinated by the technical committees and include the collective experience, expertise, and judgment of the industry. The objective of this reliability guideline is to distribute key practices and information on specific issues critical to appropriately maintaining BES reliability. Reliability guidelines are not to be used to provide binding norms or create parameters by which compliance to NERC Reliability Standards are monitored or enforced. While the incorporation of guideline practices is strictly voluntary, reviewing, revising, or developing a program using these practices is highly encouraged to promote and achieve appropriate BES reliability.

[1] https://www.nerc.com/comm/RSTC/RelatedFiles/RSTC_Charter_Board_Approved_Nov_4_2021.pdf

Executive Summary

System Operators are uniquely positioned to recognize cyber threats to the BES. Through direct access to Cyber Assets, and direct contact with field personnel, System Operators may be the first to recognize real-time threats to system security. They may also be targets of social engineering attempts.[2] System Operators are potentially the first to be able to recognize early indicators of malicious cyber activity, and the last to be able to detect such activity before impacts to operations occur. This fact notwithstanding, the System Operator organization establishes and sustains the conditions necessary for individual System Operators to successfully meet their responsibilities in real time. System Operators may be involved in recognizing indicators of potentially malicious activity, posturing facilities appropriately to maintain safe and reliable operations, and supporting certain incident response activities consistent with their organization's Cyber Security Incident Response Plan.

[2] For an overview of Social Engineering and Phishing attacks, please refer to US-CERT Security Tip ST04-14 at https://us-cert.cisa.gov/ncas/tips/ST04-014.

Introduction

Purpose

The following guideline will assist System Operators in recognizing events that may be an indicator of a cyber-attack, and how and when to share information with others. While this Cyber Intrusion Guide was created for System Operators, the principles within are applicable to any operators or support staff engaged in maintaining Reliable Operation of the BES. The intent is to increase cross-discipline familiarity and recognition of when to ask a question or raise an issue, not to make cybersecurity professionals out of System Operators or vice versa, consistent with ongoing findings from the U.S Department of Energy's CyOTE program. [3] This guideline is not intended to comprehensively cover all possible aspects of identifying a cyber-intrusion.

This document is intended to be used as a guide only. It is not intended to detract or conflict with an entity's Cyber Security Incident Response Plan required by CIP-008. Rather, the guide should highlight the plans to System Operators so that they can understand their role and what their company expects them to do. Developers of Cyber Security Incident Response Plans are encouraged to consider System Operators' perspectives when creating their organization's plans.

Applicability

Reliability Coordinators (RC), Balancing Authorities (BA), and TOPs. While not included in the NERC glossary definition of System Operator, this guideline is also relevant for Generator Operators (GOP) and Distribution Providers (DP).

Background

System Operators are uniquely positioned to recognize cyber threats to the BES. Through direct access to Cyber Assets, and direct contact with field personnel, System Operators may be the first to recognize real-time threats to system security. They may also be targets of social engineering attempts. [4] System Operators are potentially the first to be able to recognize early indicators of malicious cyber activity, and the last to be able to detect such activity before impacts to operations occur. This fact notwithstanding, the System Operator organization establishes and sustains the conditions necessary for individual System Operators to successfully meet their responsibilities in real time.

The Real Time Operating Subcommittee (RTOS) recognizes not all organizations are the same, so this guidance is general and is based on the assumption that each entity has an approved Cyber Security Incident recognition, response and reporting process in place to follow any time a Cyber Security Incident has been identified, assessed, and confirmed.

As noted above, Reliability Guidelines are not to be used to provide binding norms or create parameters by which compliance to standards is monitored or enforced.

[3] See https://inl.gov/cyote/ for more information, particularly the Methodology paper linked from there.

[4] For an overview of Social Engineering and Phishing attacks, please refer to US-CERT Security Tip ST04-14 at https://us-cert.cisa.gov/ncas/tips/ST04-014.

Chapter 1: Could this be a sign of an attack?

Recognizing indicators of potentially malicious activity

As threats to Cyber Assets are continually evolving, it is difficult to provide a comprehensive list of anomalies that may require investigation or a response. Rather, a System Operator's familiarity with their systems, awareness, and a questioning attitude likely provide the greatest value. Real-time operating staff should be vigilant in asking themselves why their Cyber Assets are responding unusually. The System Operator should be asking their Information Technology (IT) or Operational Technology (OT) support to investigate any strange, unusual behavior whenever it is detected. Similar to physical security concerns, System Operators should be encouraged to "say something when they see something." It is understood that increased vigilance may result in false positive reports, because some of the anomalies listed below can be caused by malicious activity as well as non-malicious system or equipment issues. However, it is better to "play it safe" when Cyber Assets are behaving unusually.

Examples of anomalies that may require attention:

- Observing unusual or unexplained behavior on workstations. For example:
  - Workstation unexpectedly locked out or displaying a message indicating password has been changed
  - Pointer or mouse cursor moving by itself in an intentional manner (i.e., to perform a task with the cursor, not simply random movement)
  - Files / messages flashing / suspicious pop-ups appear on the screen
  - New applications or icons appearing, or expected applications or icons disappearing from the desktop or start menu
  - System is unusually slow or unresponsive, or has unusual hard disk or network activity
- Observing unusual system activity or alarms from Cyber Assets. For example:
  - Coincident loss of multiple components of Energy Management System (EMS) or Supervisory Control and Data Acquisition (SCADA) systems supporting Real-time operations, e.g. alarming, ICCP connectivity, state estimation, or contingency analysis
  - Unexplainable power system operations such as breaker operations, transformer tap changes, or AGC set points, inconsistent with system conditions, e.g. multiple breaker operations during a non-storm event
  - Unexplainable manual operations or settings changes
  - Multiple perceived suspicious telemetry point values, inconsistent with system conditions and other apparently normal point values
  - Telephone or email requests for information about technical systems or operational procedures, or for remote access (social engineering attempts)
  - Unexpected system shutdown or reboot
  - Complete loss of SCADA capabilities that support Real-time operations.
  - Erratic EMS/SCADA system equipment behavior, messages/alarms, or degradation of performance, especially when more than one device exhibits the same behavior
  - Anti-malware application alerts on System Operator Human Machine Interface(s)
  - User account authentication requests at atypical times or systems, account lockouts, or change in user privileges

    - Calls from data partners (other entities who see your data) to verify suspicious data being received via communication associations/exchange

- Other unusual occurrences such as:
    - Coincident loss of operational support systems, e.g., Heating, Ventilation, and Air Conditioning (HVAC), Fire Suppression, phone/communications, Physical Access Control Systems (PACS) at control centers
    - Discovering unauthorized (e.g., USB sticks or wireless access points) or recognizing missing equipment from control centers

Chapter 2: Initial Actions and Internal Notifications

When unusual system behavior is investigated but not resolved, take any immediate steps outlined in your Cyber Security Incident response plan. As soon as possible, contact your cyber security team and follow their instructions; System Operators are not responders for Cyber Security Incidents. When describing the issue, include details on the observed and potential impacts of the situation. This will help responders as they work through the identification, containment, eradication, and recovery phases of incident response. Consistent with an entity’s Cyber Security Incident response plan, this may require a System Operator to:

- Contact OT or EMS Support, IT Support, and Cyber Security personnel.
- Assess impacts and risks to Reliable Operations.
- Notify the other System Operators on duty.
- Notify field personnel working in or around potentially involved facilities.

Chapter 3: Response Actions and External Notifications

Once your organization's Cyber Security Incident Response Plan has been initiated, follow the reporting instructions of the plan. Certain response actions will involve System Operators either actively or for awareness of potential risks to Reliable operations, even though System Operators are not directly responsible for these actions. These may include:

- Notifying other control centers – adjacent, distribution via Reliability Coordinator Information System (RCIS), telephone, or other existing interpersonal communications procedures
- Receiving guidance from Legal staff on allowable release of information, or Cyber Security staff assuming responsibility for confidential communications related to the incident.
- Coordination with appropriate Cyber Security, Engineering or other technical staff to effectively isolate suspect devices for containment, forensic analysis, evidence retention, eradication, and recovery.
- Law enforcement personnel requesting particular actions to preserve evidence. Reliable operations should be maintained through a coordinated response between law enforcement, operations, and an entity's physical/cyber security teams.

As the incident response progresses, System Operators should be prepared to take operational actions as documented in your organization's Operating Plan. These could include implementing specific Operating Procedures because of incident response activities (e.g., changing the status of equipment or monitoring and control systems to support investigation), or general Operating Processes as proactive steps (e.g., declaring a conservative operations status).

Chapter 4: Summary

Due to their unique role in operating the BES, System Operators may be the first to observe and report unusual behavior. To ensure that entities are able to respond effectively, it is important that System Operators maintain a questioning attitude and readiness to collaborate with other groups to assist in identifying something that requires further investigation. Further, System Operators should understand their important role in recognizing strange and unusual cyber security behavior and notifying the right people consistent with their incident response plans.

Contributors

NERC gratefully acknowledges the contributions and assistance of the following industry experts in the preparation of this guideline.

Name	Entity
Asher Steed	BC Hydro
Samuel D. Chanoski	Idaho National Laboratory
Lacy Skinner	New York ISO
Kyle Russell	IESO

Guideline Information and Revision History

Guideline Information	
Category/Topic: Operations	**Reliability Guideline/Security Guideline/Hybrid:** Reliability Guideline
Identification Number: RG-OPS-0322-2	**Subgroup:** RTOS

Revision History

Version	Comments	Approval Date
1	Approved by the NERC Operating Committee	6/25/2018
2	Approved by the Reliability and Security Technical Committee	03/22/2023

Metrics

Pursuant to the Commission's Order on January 19, 2021, *North American Electric Reliability Corporation*, 174 FERC ¶ 61,030 (2021), reliability guidelines shall now include metrics to support evaluation during triennial review consistent with the RSTC Charter.

Baseline Metrics

All NERC reliability guidelines include the following baseline metrics:

- BPS performance prior to and after a reliability guideline as reflected in NERC's State of Reliability Report and Long Term Reliability Assessments (e.g., Long Term Reliability Assessment and seasonal assessments)
- Use and effectiveness of a reliability guideline as reported by industry via survey
- Industry assessment of the extent to which a reliability guideline is addressing risk as reported via survey

Specific Metrics

The RSTC or any of its subcommittees can modify and propose metrics specific to the guideline in order to measure and evaluate its effectiveness, listed as follows:

- The effectiveness of this guideline can be assessed over time through monitoring for statistically significant changes in unauthorized electronic access resulting in disruptions in BES Facilities according to established procedures[5] developed for ERO Enterprise Metrics in previous years. The data for this metric is collected by NERC's Bulk Power System Awareness (BPSA) group and the Electricity ISAC, and is updated annually and non-publicly.

Effectiveness Survey

On January 19, 2021, FERC accepted the NERC proposed approach for evaluating Reliability Guidelines. This evaluation process takes place under the leadership of the RSTC and includes:

- industry survey on effectiveness of Reliability Guidelines;
- triennial review with a recommendation to NERC on the effectiveness of a Reliability Guideline and/or whether risks warrant additional measures; and
- NERC's determination whether additional action might be appropriate to address potential risks to reliability in light of the RSTC's recommendation and all other data within NERC's possession pertaining to the relevant issue.

NERC is asking entities who are users of Reliability and Security Guidelines to respond to the short survey provided in the link below.

Guideline Effectiveness Survey

[5] https://www.nerc.com/AboutNERC/StrategicDocuments/Metric%20Primer_BOT.pdf#page=14

Errata

Date: N/A