NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Quick Reference Guide: Security Integration

April 2024

INSIDE THIS QUICK REFERENCE GUIDE

Cyber and physical security are critical facets of the bulk power system (BPS) reliability and resilience. Grid transformation is expanding the existing attack surface due to the use of emerging technologies, additional communications, and industrial controls as well as remote control capabilities. These channels provide opportunities for adversaries to exploit latent vulnerabilities within the existing system as cyber security was not part of the design equation for legacy equipment, software, and networks. The introduction of new technologies and new types of entities entering electricity markets also present new cyber attack vectors. Beyond these challenges, addressing security risks associated with the changing resource mix continues to be a high priority for industry. Focusing on and mitigating these known and emerging risks is critical to the mission of the ERO Enterprise.[1] Modern cyber security incorporates a number of security principles and concepts, including a defense-in-depth philosophy; and historically, these concepts were not substantially integrated into the planning, design, and operation of the electric grid operational technology (OT) systems. As industry attempts to leverage improved operational performance and business efficiencies, the OT environment is increasingly connected to outside networks through the incorporation of intelligent electronic devices capable of routable internet protocol (IP) communications. This rapid change comes with greater security needs from the electricity sector OT environment and requires integration of cyber and physical security controls into these systems at deeper and earlier levels than was previously necessary. NERC is introducing the concept of security integration, which refers to the integration of cyber and physical security aspects into conventional planning, design, and operations engineering practices. This document acts as a quick reference guide for the work that the ERO Enterprise has done and plans to do in the coming years to ensure the continued reliability of the North American power grid.

[1] https://www.nerc.com/AboutNERC/StrategicDocuments/ERO%20Enterprise%20Long-Term%20Strategy%20(Approved%20December%2012,%202019).pdf

NERC Security Integration Strategy Pillars

The ERO Enterprise is dedicated to proactively identifying and addressing security challenges and continues to work with industry stakeholders to drive risk mitigation activities. Addressing these challenges requires a multifaceted strategy to identify, prioritize, and mitigate risks that face the electricity sector OT environments. The Security Integration Strategy drives security integration concept in four key areas as outlined in Figure 1. The core tenets of the NERC Security Integration Strategy incorporate near-term and long-term work items to ensure reliable and secure operation of the BPS. Components of the strategy with immediate priority are cyber-informed transmission planning, assessments of aggregate risks, cloud technology in the OT space, and DER and DER aggregator cyber security.

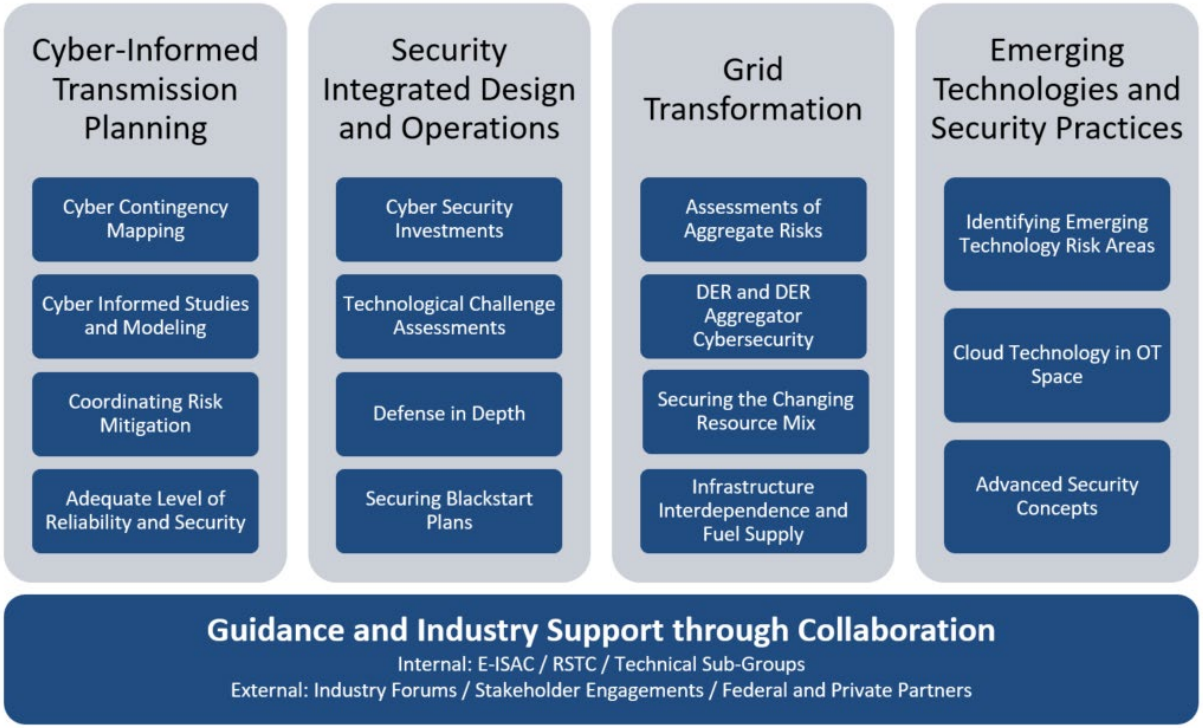

Figure 1: Security Integration Strategy Pillars

References

		References	
Published Date	**Security Integration Strategy Pillar**	**Title**	**Summary**
December 2022	**Grid Transformation**	Cyber Security for DERs and DER Aggregators	This white paper highlights equipment standards, device certification, and the possible need for NERC registration for DER aggregators to mitigate security risks.
December 2022	**Cyber-informed Transmission Planning / Security Integrated Design and Operations / Emerging Technologies and Security Practices**	Towards Integrating Cyber and Physical Security for a More Reliable, Resilient, and Secure Energy Sector (TR105)	This report provides a foundation for establishing the concept of "security integration," which attempts to begin addressing issues facing the industry through a more integrated approach incorporating cyber and physical security into the planning, design, and operational phases of the bulk power system. This report was created under the direction and guidance of a joint task force of IEEE members and the North American Electric Reliability Corporation (NERC).
May 2023	**Cyber-informed Transmission Planning**	Cyber-Informed Transmission Planning White Paper	NERC work plan priorities for 2023 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. 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.

		References	
Published Date	**Security Integration Strategy Pillar**	**Title**	**Summary**
June 2023	**Securing the Changing Resource Mix**	Recommendations for Solar Energy Cybersecurity	There is rapid and continued growth in grid-connected, large-scale solar inverter-based resources (IBR) and behind-the-meter distributed energy resources (DER). IBR/DER cybersecurity attacks may impact the energy critical infrastructure sector. Combined use of smart-grid technologies, mobile applications, and cloud-based control systems introduces risk. IBR/DER vendors, owners, operators, aggregators, grid operators, and government organizations must understand cyber threats targeting IBR/DER can create both localized and widespread impacts.
June 2023	**Emerging Technology and Security Practices**	Zero Trust Security for Electric Operations Technology	ZT is a collection of concepts intended to drive least privilege further, building upon and enhancing historical controls and perimeter-based security models. Zero trust (ZT) offers the electric industry a clear direction forward for continual improvement to securing our critical infrastructure against emerging threats to operations technology (OT)—including ransomware and industrial control system malware. Using a thoughtful implementation process will allow organizations to incorporate ZT Architectures incrementally and should be done in collaboration with OT integrators and vendors.

		References	
Published Date	**Security Integration Strategy Pillar**	**Title**	**Summary**
July 2023	**Cyber-Informed Transmission Planning**	Cyber-Informed Transmission Planning Webinar	This webinar introduces the topic of Cyber-Informed Transmission Planning and the resulting ERO Enterprise developed whitepaper. Additionally, Idaho National Laboratory presents the National Cyber-Informed Engineering strategy and the Consequence-driven Cyber-informed Engineering methodology. Lastly, the E-ISAC ties the Cyber-Informed Engineering topic to the cyber security threats facing the electric industry today.
September 2023	**Grid Transformation**	Privacy and Security Impacts of DER and DER Aggregators	This paper explores the technical facets of security controls available to DERs and DER aggregators and provides examples of potential attacks that can be mitigated through the implementation of those security controls. It also provides an overview of the security posture for the distribution landscape (particularly for DERs and DER aggregators) and correlations to relevant NERC Reliability Standards.

		References	
Published Date	**Security Integration Strategy Pillar**	**Title**	**Summary**
November 2023	**Emerging Technology in OT Space**	BES Operations in the Cloud	The Security Integration and Technology Enablement Subcommittee (SITES) recognizes industry's innovative spirit in exploring the value presented by cloud computing technology for various applications in support of the Bulk Electric System (BES). Innovative offerings from vendors within the electric sector are steadily including virtualization and cloud solutions. However, utilities should carefully assess security and reliability risks of migrating systems and applications associated with BES reliability operating services (BROS) to the cloud, especially those critical systems with high availability requirements. SITES identifies that BES operations are broad, and there are many opportunities for large data analysis and systems that are not real-time to benefit from cloud services.
January 2024	**Internal Network Security Monitoring Feasibility Study**	Internal Network Security Monitoring (INSM) Feasibility Study	On 19 January 2023, the Federal Energy Regulatory Commission (FERC) issued Order 887, which directed the North American Electric Reliability Corporation (NERC) to submit a report, within 12 months of issuance of its final rule, that studies the feasibility of implementing internal network security monitoring (INSM) at all low impact BES Cyber Systems and medium impact BES Cyber Systems without External Routable Connectivity (ERC). The public version of the report is available as of January 2024.

NERC Stakeholder Groups

Security Working Group

The 2023 ERO Reliability Risk Priorities Report highlighted "Grid Transformation" (Increased Complexity in Protection and Control Systems), "Security Risks" (Physical and Cyber Security Threats), and "Critical Infrastructure Dependencies" (Communications) as three high level risk categories for the ERO Enterprise and electric industry. At the same time, the operational and technological environment of the electrical grid is undergoing rapid transformation. The Security Working Group (SWG) serves the Reliability and Security Technical Committee (RSTC) in providing a formal input process to enhance collaboration between the ERO Enterprise and industry with an ongoing working group. The SWG also supports industry efforts to mitigate emergent risks by providing technical expertise and feedback to the ERO Enterprise Compliance Assurance group in developing and enhancing security compliance-related products, including guidelines, guidance, best practices, and lessons learned.

Security Integration and Technology Enablement Subcommittee (**SITES**):

The 2019 ERO Reliability Risk Priorities Report1 highlighted "Grid Transformation" and "Security Risks" as two of four high level risk categories for the ERO Enterprise and electric industry. At the same time, the operational and technological environment of the electrical grid is evolving significantly and rapidly. To proactively support industry efforts to mitigate risks, the NERC Security Integration and Technology Enablement Subcommittee (SITES) will identify, assess, recommend, and support the integration of technologies on the bulk power system (BPS) in a secure, reliable, and effective manner. SITES recognizes the convergence of information and operational technology cited by the RISC and will recommend practices to incorporate cyber and physical security aspects into conventional planning, operations, design, and restoration activities across North America. The goal of the subcommittee is to identify potential barriers (e.g., regulatory, technological, and complexity) and support the removal of these barriers to enable industry to adopt emerging technologies and develop cyber-informed engineering practices.