NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Security Integration Strategy

Ensuring Security of the Bulk Power System through Cyber and Physical Security Integration into Planning, Design, and Operational Engineering Practices

December, 2022

Purpose and Background

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 the 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.

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

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

Security integration encompasses all aspects of the conventional engineering part of the electric industry. NERC is primarily focused on integrating cyber and physical security concepts more holistically into transmission planning, engineering design, and system operations to ensure that mitigating security controls are considered as early in the process as possible, rather than as a "bolt-on"[2] solution. For example, security integration may entail planning a BPS that minimizes or eliminates possible risk of a widespread cyber security compromise. It also includes driving cyber security controls comprehensively into the engineering design phase. Lastly, security controls can be further integrated with system operations to enable earlier detection, more effective mitigation, and quicker recovery from security events. Addressing cyber-physical risks to the BPS through security integration in the OT environment is necessary to accomplish a complete defense-in-depth strategy for securing the grid.

The NERC Security Integration Strategy that is set forth in this document outlines the ERO priorities to enhance security integration through working collaboratively with electricity sector stakeholders. It identifies areas of focus where security integration can be enhanced to support a more secure, reliable, and resilient BPS moving forward.

Known and Emerging Risks

The ERO Reliability Risk Priorities Report has identified an increase in cyber-physical risks as a high priority for the electricity sector.[3] The process of identifying, validating, and prioritizing these risks includes gathering data and information from many sources, such as stakeholder engagements, communication with government agencies,[4] and shared public intelligence among other sources as well. Cyber and physical risks as well as the likelihood of successful attacks on devices, communication paths, and grid systems and assets increase as the reliance on digitalization grows. Vulnerabilities in the power system and related components may come in the form of incomplete contingency analysis, legacy network design, vulnerable equipment, lack of visibility to existing networks, cross sector interdependence, rapidly changing technological innovations, human factors, etc. Foreign and domestic terrorists, criminals, and nation-state adversaries—each known as advanced persistent threats— have the capability to exploit vulnerabilities and carry out sophisticated attacks given enough time, resources, and opportunities. Successful exploitation of these vulnerabilities can result in detrimental impacts to BPS reliability and resilience, which directly affects equipment integrity, public safety, the global economy, and national security.

Risk Framework

The tenets of the NERC Security Integration Strategy can be mapped to the NERC Risk Framework[5] that guides the ERO in prioritization of risks and provides guidance on the application of ERO policies, procedures, and programs to inform resource allocation and project prioritization in the mitigation of those risks. Additionally, the NERC Risk Framework includes measuring residual risk after mitigations are deployed to enable the ERO to evaluate the success of its efforts in mitigating risks. This provides a necessary

[2] Bolt-on cyber security generally refers to any security controls implemented after a system or device was designed and implemented. These security measures are likely to be expensive, less effective, or only partially implemented due to design limitations without disruptive or expensive redesign and implementation efforts.
[3] https://www.nerc.com/comm/RISC/Documents/RISC%20ERO%20Priorities%20Report_Final_RISC_Approved_July_8_2021_Board_Submitted_Copy.pdf
[4] For example, Department of Energy (DOE), the Department of Homeland Security (DHS), and the Canadian Electricity Association (CEA).
[5] https://www.nerc.com/comm/RISC/Related%20Files%20DL/Framework-Address%20Known-Emerging%20Reliabilit-Securit%20%20Risks_ERRATTA_V1.pdf

feedback for future prioritization, mitigation efforts, and program improvements. The successful reduction of risk is a collaborative process between the ERO Enterprise, industry, and the technical committees, including the Reliability and Security Technical Committee (RSTC) and Reliability Issues Steering Committee (RISC). The NERC Risk Framework provides a transparent process, with industry experts in parallel with ERO Enterprise experts, which includes risk identification, deployment of mitigation strategies, and monitoring the success of these mitigations.

Six specific steps have been identified that are consistent with risk management frameworks that are used by other organizations and industries:

1. Risk Identification and Validation
2. Risk Prioritization
3. Remediation and Mitigation Identification/Evaluation
4. Deploy Mitigation
5. Measure Success
6. Monitor Residual Risk

Each of these steps will require process development, including stakeholder engagement, validation/triage approaches, residual risk monitoring, and considerations of the ERO Enterprise's level of purview over a risk, etc. A graphical representation of the NERC Risk Framework is shown in **Figure 1**.

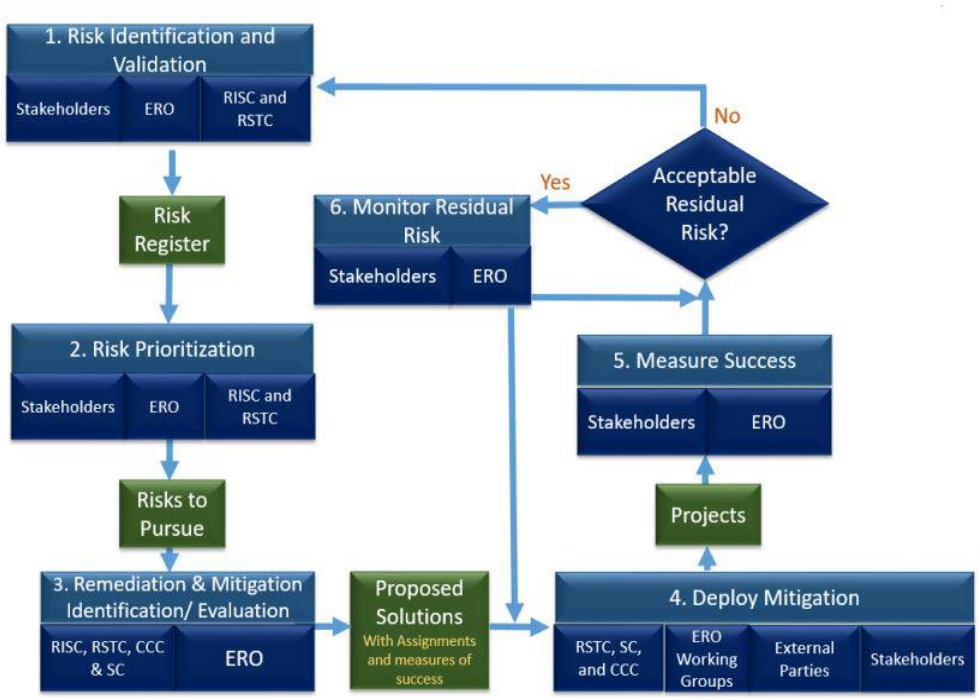

Figure 1: NERC Risk Framework

Tenets of the NERC Security Integration Strategy

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 require a multifaceted strategy to identify, prioritize, and mitigate risks that face the electricity sector OT environments. The strategy drives security integration concept in four key areas as outlined in **Figure 2**. 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.

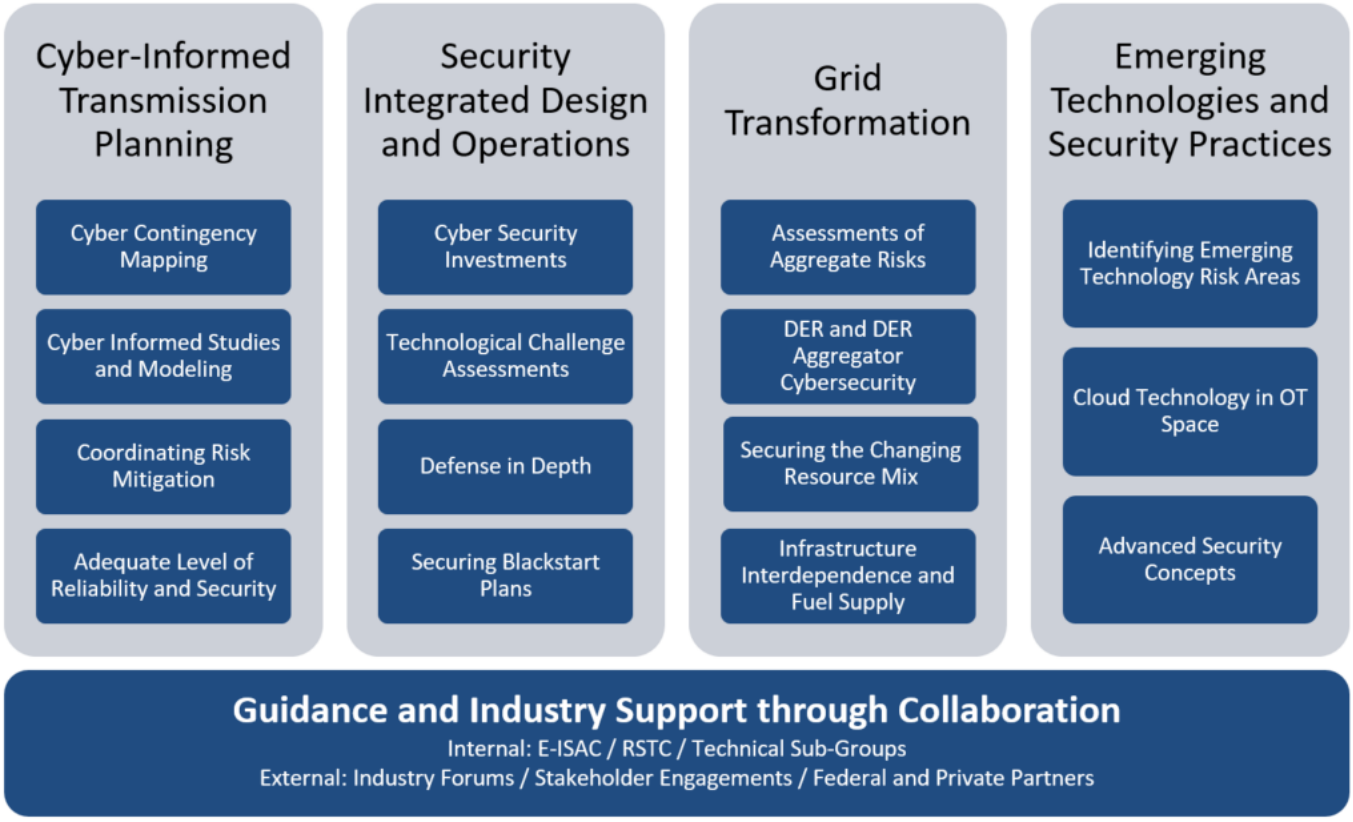

Figure 2: NERC Security Integration Strategy

The NERC Security Integration Strategy is primarily focused on risk identification and validation, prioritization, and development of possible mitigations. Future work by the ERO will explore deploying those mitigations and monitoring success collaboratively with industry.

By using anonymized data and lessons learned, NERC can explore a technical basis for incorporating cyber-informed transmission planning and additional operational controls into industry practices and possible future NERC standards enhancements. Additionally, this strategy addresses near- and long-term reliability risk issues through addressing the integration of technological advancements and emerging technologies applicable to the changing grid as well as addressing paradigm shifts, including cloud services adoption.

NERC will collaborate with industry partners to develop security guidance for aggregate "low" impacts, including development of cyber security risk scenarios in the OT space. The following sections briefly describe each tenet of the risk mitigation strategy.

Cyber-Informed Transmission Planning

Current transmission planning[6] activities focus predominantly on physical security assessment per CIP-014 and only include cyber risk as part of the extreme contingency events in TPL-001. However, the ERO Enterprise is working collaboratively with industry experts to develop a cyber-informed transmission planning framework that can be used to integrate cyber security into steady-state and dynamic simulations of BPS reliability.

This will require enhancements to traditional transmission planning processes:

- Industry will need to determine how to identify appropriate cyber security risks and map them to associated planning contingencies used in studies. How those events will be modeled and studied will need to be explored in more detail. Addressing possible reliability risks posed by cyber security events should be addressed with corrective actions that may involve either enhancing cyber security controls or other capital projects (such as those used to address environmental events studied today). The goal is to drive towards a more cyber-resilient grid by identifying gaps and implementing appropriate mitigating security controls or prioritizing appropriate investments early in the grid planning process. This will require a paradigm shift and feedback loop between transmission planning and OT cyber security groups.
- New simulation engines and models may be needed to incorporate cyber design alternatives to understand their implications on current and future systems. Transmission planning and security team coordination can address vulnerabilities identified during studies and reduce the likelihood and impact of these vulnerabilities being exploited.
- The ERO plans to consider whether any enhancements to the existing adequate level of reliability definition are needed to fully incorporate security considerations (i.e., inclusion of adequate levels of security concepts); focus in this area will hopefully enable industry to make more concerted efforts to drive necessary mitigating security controls through an objective and repeatable planning process that links the engineering and security aspects early in project development.

Security Integrated Design and Operations

The ERO considers and encourages a shift in perspective regarding cyber security and its associated costs. Rather than being thought of as an insurance policy, concerted analysis should be given to the prospect of treating these costs as a capital investment; this is a reliability enhancement that minimizes impact and risk, improving resilience. Investments in cyber security are important factors contributing to the efficacy and maturity of a registered entity's security program, including the technology controls implemented to protect its critical systems and data. It is more effective and efficient to support reliable operation of the BPS by integrating OT cyber security investments early in the design process for grid reinforcements rather

[6] Transmission planning involves studying BPS performance, and it includes modeling and simulating all elements of the BPS.

than having them "bolted on" as operations and maintenance costs. Cyber-informed transmission planning may allow these and other benefits to be realized more effectively as well.

Equipment manufacturers may have networking access to large amounts of generation for maintenance, monitoring, or control that is not subject to minimum cyber-physical security standards. Analysis of the technical limitations of existing electric OT equipment must be performed in order to understand how to improve guidance and support industry when selecting and implementing next generation OT equipment capable of integrated security. In order to connect equipment to information networks, that equipment must be robust and capable of addressing security risks. The ways in which one thinks about and expect the equipment and systems to perform need to include cyber security best practices. Working with industry, NERC will provide needed guidance on how to assess technology solutions to meet rapid technological advancements in a secure way.

Segmented networks with appropriately grouped assets, designed-in security controls, hardened security-capable equipment, and other factors should be incorporated into system design and operations phases. As increasing levels of distributed energy resources (DER) come on-line, the need to add essential reliability services to the resources drives the need to ensure proper security assessments and planning as well.

Grid Transformation

The transformation of the electricity sector is primarily driven by the shift towards clean energy resources, and requires a deliberate and sustained focus from both an engineering and security perspective. Newly interconnecting inverter-based resources, such as wind, solar photovoltaic, battery energy storage, and hybrid plants, are changing how the grid is planned, operated, and designed. Furthermore, the growth of DERs and the introduction of the DER aggregator with FERC Order 2222[7] changes the attack surface of the electricity sector. Many of these entities and the resources that they control are not subject to regulatory cyber security standards, such as the NERC Critical Infrastructure Protection (CIP) standards, and will require a collaborative and holistic approach to securing the overall electricity ecosystem. NERC is focused on identifying areas in which additional effort is needed to support entities in developing, procuring, and operating a high renewables grid of the future in a secure manner. This includes guidance around enhanced security postures, equipment standards and certification, integrated security practices, and risk assessments. Possible assessments may include exploring the concepts of aggregate risks by assessing the amount of generation any one entity or manufacturer controls, how their systems are deployed and secured, and identifying reliability risks. Regulatory visibility and oversight into these areas is key for assessing, implementing, and enforcing adequate levels of security across the BPS.

The energy transition requires a phased approach; however, the ERO must be agile and effective in driving meaningful security enhancements in this area as new resources connect to the system rapidly. Critical infrastructure interdependence continues to be of the utmost importance as the existing BPS still relies heavily on synchronous balancing resources for essential reliability services; understanding possible security vulnerabilities in the natural gas, hydro, and other critical infrastructure areas will be key to identifying possible BPS reliability issues. Analysis in this area is required to implement effective cyber

[7] https://www.ferc.gov/media/ferc-order-no-2222-fact-sheet

security programs that encompass the networks and infrastructure that ensure fuel and resource availability.

Emerging Technologies

The electricity sector is experiencing a rapid change in the technologies being connected, used, and leveraged to plan and operate the BPS. Some of these technologies are still evolving or are relatively new for the adoption in the electric OT space, which may have an impact on BPS reliability moving forward. Examples include cloud technology, artificial intelligence, blockchain, DERs and DER aggregators, grid edge technologies, and others. NERC supports the adoption of emerging technologies and seeks to assist in fully realizing the potential that these technologies could have to enhance reliability and resilience of the BPS; however, leveraging and implementing these technologies in a reliable and secure manner is paramount. Key focus areas of this pillar (see **Figure 2**) include cloud adoption in the OT space, monitoring of emerging technologies and their deployment within the BPS, and promoting security enhancements through borderless architectures, such as zero trust, internal network security monitoring, and software-defined networking. NERC will work collaboratively with industry stakeholders to develop guidance material regarding the adoption of emerging technologies as well as conduct assessments on any necessary enhancements to the NERC CIP standards to adequately secure and leverage these technologies moving forward.

Guidance and Industry Support through Collaboration

Delivering on all aspects of this strategy requires outreach and collaboration with industry stakeholders, regulatory bodies, policy organizations, and equipment standards bodies. NERC is focused on identifying areas in which additional guidance related to enhanced security postures and integrating security with the planning, design, and operations that can be efficiently targeted. NERC is working with industry stakeholders to conduct assessments of possible risk areas and to develop guidance to support improved security practices in this area of the BPS. This includes coordinating with industry partners, such as the U.S. Department of Energy, Idaho National Laboratory (INL), the Electric Power Research Institute (EPRI), and others to drive adoption of security best practices, identify and address gaps in standards and requirements as well as to foster a security culture through focused collaboration between engineers, security professionals, and industry leadership. NERC and its Electricity-Information Sharing and Analysis Center continue to work collaboratively with a broad set of stakeholders to support these efforts.

NERC is relying on engagement and support from industry members through its Reliability and Security Technical Committee, particularly with the Security Integration and Technology Enablement Subcommittee (SITES), the Security Working Group and others. These groups can support the development and execution of components of this strategy with specific work items. This includes industry guidance materials, whitepapers, technical assessments and reports, and possibly future standard authorization requests (if needed) to move the needle towards more wholly integrated cyber and physical security within the BPS.

Milestone Plan

In support of NERC's Security Integration Strategy, the following deliverables are planned for 2023. These include items being developed by the ERO Enterprise, in coordination with industry stakeholders as well as materials being developed by NERC SITES and planned to be submitted to the NERC RSTC:

- **Technical Report—IEEE-NERC Security Integration Report (IEEE):** It outlines the need to integrate cyber and physical security for a more reliable, resilient, and secure energy sector. Expected completion: Q4 2022
- **White Paper—Cyber Security for DERs and DER Aggregators (SITES):** It highlights equipment standards, device certification, and the possible need for NERC registration for DER aggregators to mitigate security risks. Expected completion: Q4 2022
- **White Paper—Cyber-Informed Transmission Planning (ERO Enterprise):** This cyber-informed transmission planning framework providing a roadmap for integrating cyber security aspects into transmission planning activities. Expected completion: Q1 2023
- **White Paper—Zero Trust (SITES):** It outlines important considerations for adoption of zero trust in OT environments. Expected completion: Q1 2023
- **White Paper—BES Operations in the Cloud (SITES):** It outlines important considerations for adoption of cloud technology in the electric utility environment. Expected completion: Q2 2023
- **White Paper—Cyber Security Maturity Models and NERC CIP Standards (ERO Enterprise):** It maps cyber security maturity model concepts to NERC CIP cyber security controls. Expected completion: Q3 2023
- **Assessment—Inverter-Based Resource Vendor Cyber Security:** It explores possible cyber security risks pertaining to vendor remote access for BPS inverter-based resources. Expected completion: Q3 2023
- **White Paper—Controls for DERs and DER Aggregator Cyber Security (SITES/NERC SPIDERWG[8]):** It provides technical details and guidance regarding cyber security for DERs and DER aggregators. Expected completion: Q4 2023
- **White Paper—Cyber Security for the Changing Resource Mix (SITES):** It describes recommended cyber security controls and practices for BPS-connected inverter-based resources. Expected completion: Q4 2023

[8] NERC System Planning Impacts from Distributed Energy Resources Working Group