Security Integration and Technology Enablement Subcommittee Scope

December 2020

Purpose

The *2019 ERO Reliability Risk Priorities Report*[1] 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 possible 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.

Activities

SITES activities are intended to help industry adopt emerging technologies in a secure, reliable, and resilient manner to ensure reliability, security, and resilience of the BPS. This includes a focus on work products that assist in integrating emerging technologies in a manner that complements grid planning, design, operations, and restoration practices. Key activities and work products of the SITES include, but are not limited to, the following:

Technology Enablement:

1. Provide guidance to industry with recommendations for cyber and physical security practices, emerging technology solutions (e.g., cloud computing, virtualization), and approaches to appropriately secure operational technology systems.
    a. Enhance the effective use of emerging technologies and support the convergence of operational and information technology solutions. Examples include, but are not limited to, inverter-based resources, new digital communications strategies, and advanced BPS hardware and software systems.
    b. Identify solutions that remediate or mitigate potential risks to BPS reliability, security, and resilience resulting from increased threat vectors[2] (i.e., cyber attacks) or improperly implemented or configured technologies.

[1] https://www.nerc.com/comm/RISC/Related%20Files%20DL/RISC%20ERO%20Priorities%20Report_Board_Accpeted_November_5_2019.pdf
[2] A threat vector is a path or a means by which a cybercriminal gains access into a computer system by exploiting a vulnerability

2. Develop and promote industry education through materials that address emerging technologies and how they can the impact BPS reliability and resilience and encourage an industry culture of cybersecurity awareness when adopting new technologies and when planning, designing, and operating the BPS.

Security Integration:

1. Develop recommendations in coordination with other NERC stakeholder groups (as appropriate) to ensure that cyber and physical security are an integral component of BPS planning, design, operations, and restoration:
    a. To effectively *plan* a future BPS by considering existing and emerging security vulnerabilities, equipping planners with knowledge necessary to remediate or mitigate vulnerabilities. This includes the need to consider balancing economies of scale against the risk of a centralized attack surface, developing methods, models, and tools that simulate BPS threat vector scenarios, and establish industry best practices for cyber resilience.[3]

    b. To effectively *operate* the existing and future BPS by using new technologies in an effective way that does not introduce unforeseen cybersecurity vulnerabilities. Empower grid operators by identifying solutions that integrate cyber and physical security intelligence into the real-time operating environment.

    c. To effectively *design* a BPS infrastructure to minimize potential cybersecurity threats while leveraging state-of-the-art capabilities and equipment.

    d. To effectively *restore* the BPS if a cyber or physical attack were to affect a geographically diverse area and comprise various types of operating entities. This addresses system restoration coordination activities under severe cyber attack, or coordinated physical attack conditions.

2. Provide an assessment of the transformation of the BPS operational and technological environments across North America; define recommended practices that support secure, reliable operation of the BPS with the convergence of information and operational technology (IT/OT); the growing reliance on emerging technologies, and; assess current and future potential risks that these changes present to the BPS.

3. Develop a cybersecurity framework[4] to determine baseline cybersecurity maturity metrics for BPS cyber systems. Identify ways to further protect the BPS during its rapid transformation. Key areas of focus for security consideration include, but are not limited to: BPS-connected inverter-based resource physical and cyber security, distributed energy resources (as well as aggregators and management systems), microgrid communications, and cloud computing.

4. Identify potential security threats across all applicable entities and areas of the BPS and define the potential impacts (i.e. BPS planning, operations, design, restoration activities) from an overall BPS system perspective, as well as individual elements.

[3] Cyber resilience is the ability of an organization to prepare, respond, and recover when cyber attacks happen.
[4] Leveraging the NIST Cybersecurity Framework: https://www.nist.gov/cyberframework

a. Identify and assess potential risks to the BPS arising from adoption of emerging technologies. Examples include, but are not limited to, the following: cybersecurity vulnerabilities within distributed energy resource management systems, diverse data locations in cloud environments, supply chain risk management, contingency events from high-altitude EMP, and other geographically diverse threats.

b. Identify potential security threats and determine the impacts to critical energy infrastructure from possible electrically and geographically diverse threats.

c. Coordinate with the NERC Electricity Information Sharing and Analysis Center (E-ISAC) to support the cyber-informed engineering practices in planning, designing, and operating the BPS.

d. Deliver recommended risk mitigation strategies to industry in an appropriate fashion for implementation.

5. Develop planning, operating, design, or restoration metrics that could be used to measure adequate levels of reliability of the BPS in the context of cyber and physical security.

6. Develop collaborative partnerships with industry, governmental partners, national laboratories, research and development institutes, academia, and other organization to determine the current state-of-the-art in cyber and physical security designs, cutting-edge tools, and expertise.

   a. Provide a forum for open discussion about new research, tools, and initiatives across North America.

   b. Encourage the development of partnerships between NERC, research partners, and asset owners that help streamline the piloting and eventual adoption of new solutions.

Coordination with NERC and Other Industry Technical Groups:

1. Collaborate with other NERC stakeholder groups within the Reliability and Security Technical Committee (RSTC) on applicable topics to eliminate potential overlaps, avoid duplicative efforts, and ensure alignment of assignments and responsibilities. The goal of these activities will be to coordinate and effectively leverage expertise across groups to the extent possible.

   a. This includes close coordination with the NERC Security Working Group to advise them of planning and operational issues, trends, and other factors that should inform their discussions about security matters.

   b. This includes coordination with other NERC technical groups focused in these areas to provide them with useful perspectives on security-related issues that may affect them.

2. Provide requested support to the development of the NERC Long Term Reliability Assessment and State of Reliability Report, as well as other assessments pertaining to emerging technologies and grid transformation.

3. Take input from the Electricity Subsector Coordinating Council (ESCC), and consult with the Institute of Electrical and Electronics Engineers (IEEE), and other industry technical groups, as needed.

4. Any other activities or assignments defined by the RSTC.

Deliverables

The SITES will develop work products in the following areas to support industry efforts relating to integrating emerging technologies and security enhancements into conventional planning, operations, and design practices:

- Technical reference documents, technical reports, white papers, and tools
- Reliability Guidelines and Security Guidelines as assigned by the RSTC or through periodic review
- Compliance Implementation Guidance
- Standard Authorization Requests
- Supporting materials to other NERC work products (e.g., NERC Long Term Reliability Assessment)
- Other educational materials (webinars, workshops, conferences, etc.)

Membership

The SITES will include members with expertise in the following areas:

- Design and implementation of cybersecurity infrastructure, systems and networks in BPS control centers, transmission systems, generation facilities, systems critical to BPS restoration, special protection systems, and other systems impacting users, owners, and operators of the BPS
- Understanding state-of-the-art and emerging technologies (e.g., software-as-a-service (SaaS), cloud computing) and how these technologies can be put into practice to improve BPS reliability, security, and resilience
- Cybersecurity threat vectors and risks posed by changing technologies for owners, operators, and end-users of the BPS as well as new operating paradigms for the BPS (e.g., distributed energy management systems)
- Identifying and defining physical and cyber security risks with respect to BPS reliability and resilience
- Relevant information security standards and NERC Reliability Standards
- BPS planning practices and how security concepts could be integrated into these practices more effectively and efficiently
- BPS operating processes and procedures and how cybersecurity concepts could be integrated into these practices
- BPS design practices (e.g., field operations, substation design) and how cybersecurity concepts could be integrated into these practices

SITES will consist of a Chair and Vice Chair with a two-year term limit, nominated by SITES and approved by the RSTC leadership. The working group officers may be reappointed, provided that no officer may serve longer than two consecutive terms. NERC staff will be assigned as Coordinator(s). SITES operates under the direction and coordination of the RSTC. Decisions made by the membership will be consensus-based, led by the chair and staff coordinators. Any minority views will be documented, as necessary. The RSTC will assign a Sponsor to help advocate SITES activities and to coordinate with RSTC and its other sub-groups.

Reporting and Duration

The SITES will report to the NERC RSTC. The group will submit a work plan to the RSTC following its inception and maintain its work plan throughout its existence. The duration of the SITES is expected to be indefinite so long as the group is deemed by the RSTC to be effectively accomplishing its purpose.

Meetings

SITES will have two to three meetings (in-person or remote) per year, supplemented with regular conference calls to continue workload as needed.