NIST Technical Note 2182

Distributed Energy Resource Security: Potential Guidelines and Research Topics

Avi Gopstein
Nelson Hastings
Larry Feldman
Ravi Agarwal
Nadya Bartol

This publication is available free of charge from:
https://doi.org/10.6028/NIST.TN.2182

National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Technical Note 2182

Distributed Energy Resource Security: Potential Guidelines and Research Topics

Avi Gopstein
Smart Grid Program
Communications Technology Laboratory

Nelson Hastings
Applied Security Division
Information Technology Laboratory

Larry Feldman,[α] Ravi Agarwal,[β] Nadya Bartol[β]
[α]*Huntington Ingalls Industries*
[β]*BCG Platinion*

This publication is available free of charge from:
https://doi.org/10.6028/NIST.TN.2182

October 2021

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

National Institute of Standards and Technology Technical Note 2182
Natl. Inst. Stand. Technol. Tech. Note 2182, 18 pages (October 2021)
CODEN: NTNOEF

This publication is available free of charge from:
https://doi.org/10.6028/NIST.TN.2182

Abstract

This paper describes an effort to validate the applicability of cybersecurity controls from the 2014 National Institute of Standards and Technology (NIST) Interagency Report 7628 Revision 1 (NISTIR 7628 r1) *Guidelines for Smart Grid Cybersecurity* to High Distributed Energy Resources (High-DER) environments [1]. The paper summarizes insights gained through stakeholder interviews and workshops, and provides updates to current cybersecurity guidance and recommendations for future research.

Key words

Cybersecurity; Smart Grid; Logical Interface Categories.

Table of Contents

List of Tables

List of Figures

1. Introduction

Smart grids are examples of a Cyber-Physical Systems that consist of both Information Technology (IT)[1] and Operational Technology (OT)[2] systems. Thus, cybersecurity requirements of a smart grid should reflect both IT and OT concerns, including prevention of traditional IT attacks as well as recognition and mitigation of cyber-physical attacks.

Modernized smart grids with large numbers of distributed energy resources (DERs), called High-DER environments, introduce additional complexity through the implementation of novel technologies and new communications interfaces. Described extensively in NIST Special Publication 1108r4 [2], *NIST Framework and Roadmap for Smart Grid Interoperability Standards* (Smart Grid Interoperability Framework), grid domains[3] are conceptual tools that aid understanding of organizational and device function and responsibility. The existence of domain-specific regulations, along with a growing need for different stakeholders to access devices for a variety of purposes, complicates the security issue.

As described in the Smart Grid Interoperability Framework, power system communications increasingly transit several domain and organizational boundaries. This obfuscates the community's understanding of which domain or administrative body is responsible for providing security of communication interfaces. It is possible that if one organization in a domain is compromised, an organization in another domain could become compromised through cross-domain communication.

NIST Interagency Report 7628r1 [1], *Guidelines for Smart Grid Cybersecurity* (NISTIR 7628), provided a comprehensive set of cybersecurity controls for smart grid when it was published in 2014. This paper describes an effort to validate applicability of NISTIR 7628 cybersecurity controls to High DER environments and provides recommendations for future guidance to be developed and potential research.

2. Approach and Initial Findings

The Smart Grid Interoperability Framework identifies seven domains within the smart grid, as shown in **Figure 1**. These include Transmission, Distribution, Operations, Generation including DER, Markets, Customer, and Service Provider domains. A smart grid domain is a high-level grouping of organizations, buildings, individuals, systems, devices, or other actors.[4] Numerous actors participate in transmitting, storing, generating, and processing the data needed within a smart grid. To enable smart grid functionality, the actors in a particular domain often interact with actors in other domains. Communications among actors in the same domain or between the domains have unique characteristics and security requirements.

[1] Including connection to the Internet.
[2] Including connections to physical equipment.
[3] NIST SP1108r4 identifies seven grid domains that conceptually organize grid participants and roles by physical and operational context and are described in more detail in Section 2.
[4] An actor is a device, computer system, software program, or the individual or organization that participates in the smart grid. Actors have the capability to make decisions and to exchange information with other actors. Organizations may have actors in more than one domain.

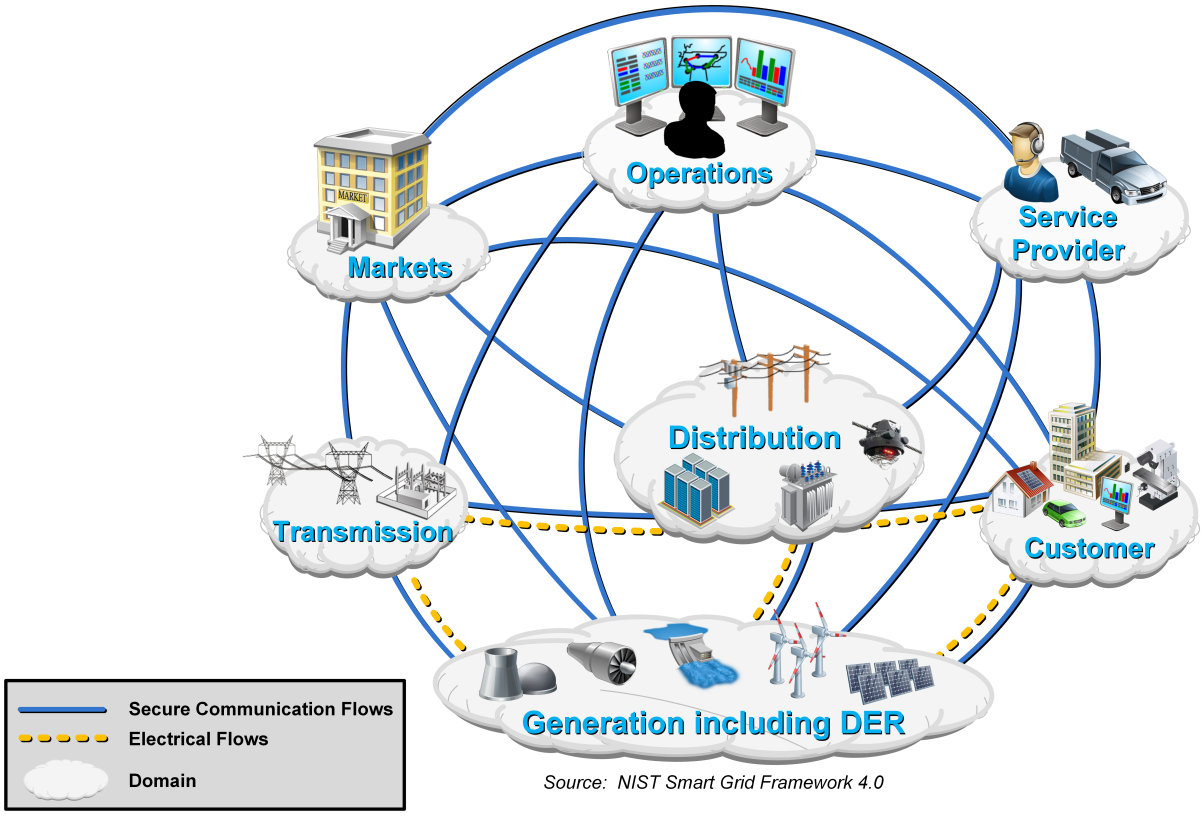

Figure 1 - NIST smart grid conceptual model domains [2]

Information exchanges within the grid environment happen through logical interfaces. These interfaces are grouped into logical interface categories (LICs) by similar functions or type of communication. The attributes that define LICs also drive similarities in security requirements for the interfaces grouped within a particular LIC. Based on such similarities, the LICs can be used to guide:

- Organizations in identifying risk-based security requirements for High-DER environments
- Vendors and integrators as they design, develop, implement, and maintain the security requirements

The Smart Grid Interoperability Framework includes discussion of how new electrical system architectures affect information exchanges in the grid, to include how new information exchanges occur in High-DER versus traditional grid environments.

While a typical High-DER environment includes several new interfaces, the types of interfaces are not fundamentally new. Rather, these interfaces are being established between new actors or those who have until now not interacted with the grid. Since the types of interfaces are not new, it is reasonable to apply existing knowledge on how to secure LICs to

the process of securing those new interfaces. For example, LIC 6 is a control signal communication that crosses domain and organizational boundaries. That type of communication has previously existed between operations centers in the Transmission and Distribution domains, but in a High-DER environment that type of communication is now moving into the Customer domain as well.

Cybersecurity guidance for existing LICs contained in NISTIR 7628 was not specifically designed for a High-DER environment. To determine which of NISTIR 7628 guidance for existing LICs applies to High-DER environments, the cybersecurity protections for existing LICs in traditional utility environments were compared with cybersecurity protections for new interfaces within the same LICs identified in the Smart Grid Interoperability Framework.

An analysis was conducted that concentrated on the cybersecurity of three specific LICs – numbers 6, 9, and 16. These LICs were selected because they cover a broad spectrum of cross-domain communications, have different security requirements, and provide a good example of communications in traditional grids as well as modernized grids with High-DER environments.

New High-DER interfaces identified in the Smart Grid Interoperability Framework were compared to the LIC descriptions contained in NISTIR 7628 and evaluated for similarities and differences in communication interface characteristics between the two conventional and High-DER scenarios presented in these reports. Results of this analysis showed that, in general terms, characteristics of the new interfaces could be mapped to existing LICs.

The diagram in Error! Reference source not found. shows an example of Logical Interfaces by Category that may be used in cross domain communications within power systems. The example includes traditional smart grid interfaces from NISTIR 7628, and new High-DER interfaces from the Smart Grid Interoperability Framework.

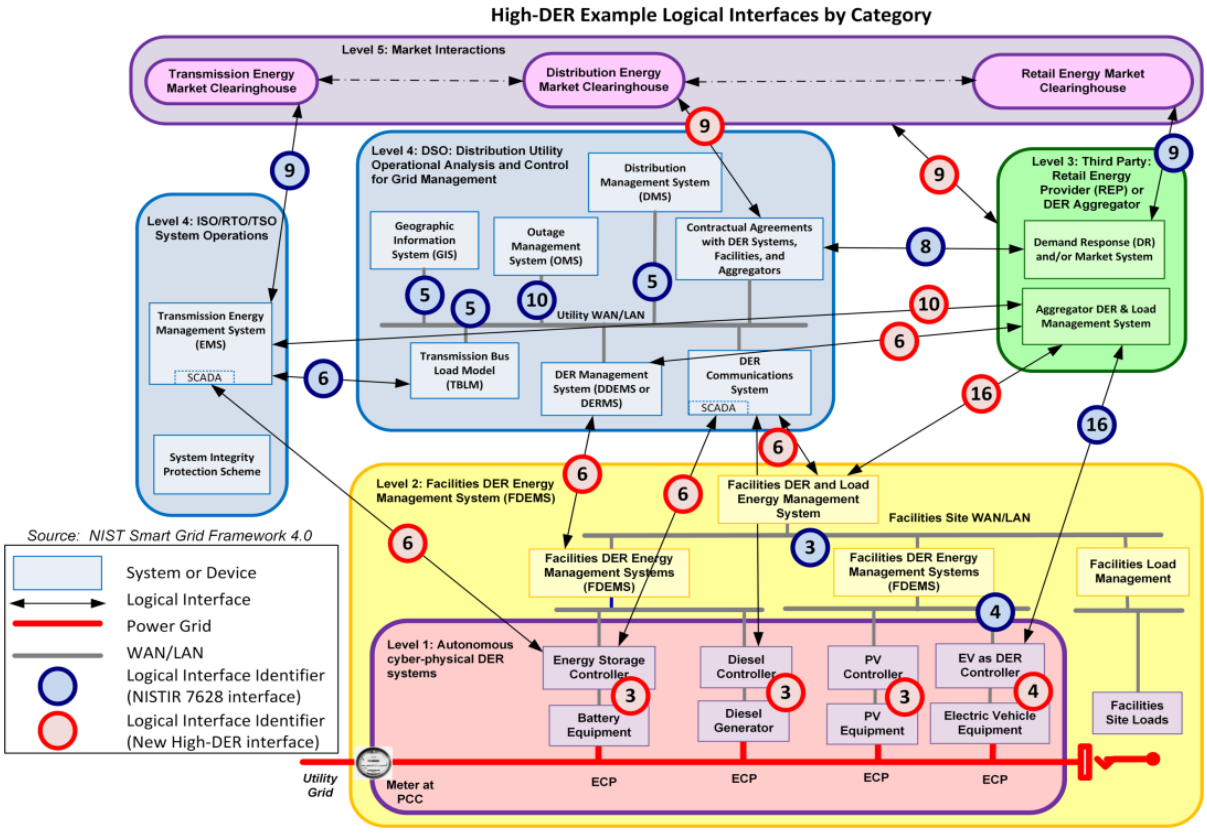

Figure 2 - High-DER Example Logical Interfaces by Category from Smart Grid Interoperability Framework [2]

LIC 6 covers the interfaces between control systems in different organizations, for example between a Regional Transmission Operator/Independent System Operator (RTO/ISO) energy management system (EMS) and a utility EMS. The security-related characteristics of interfaces between such control systems include:

- High data accuracy and availability requirements, with the most stringent requirements of either system determining the requirements for all connected systems
- The control systems are usually located in secure physical environments, although this may no longer apply to customer-sited or other distributed assets
- Data exchanges can be between organizations, requiring establishment and maintenance of the chain of trust

LIC 9 covers interfaces for business-to-business (B2B)[5] connections typically involving financial or market transactions, for example between a Retail Aggregator and a Retail Energy Market Clearinghouse. The security-related characteristics of B2B systems with interfaces between them include:

- Confidentiality requirements due to the potential financial impacts as well as confidential organizational and market information;
- Privacy requirements to maintain legal market operations and prevent market manipulation;
- Timing latency, critical time availability, and data integrity are important to avoid missed market opportunities and prevent market manipulation; and
- Market operations are between organizations, posing trust issues.

LIC 16 covers interfaces between external systems and the customer site, for example between a third party and the home area network (HAN) gateway. The security-related characteristics of the interfaces between external systems and the customer include:

- Information exchanged is confidential and needs to be protected against unauthorized third party access;
- Data integrity requirements must be specific to an application, as interaction types vary according to function and role;
- Availability is not critical and communications do not need to be real-time; and
- Devices may be in a physically unsecure location.

Based on data gathered for this work, which included feedback from utility professionals obtained during a workshop, cybersecurity protections applied within utilities seem to be of high quality and maturity. It was evident that utilities are implementing and improving cybersecurity controls and procedures on a regular basis for both traditional and High DER environments. Specific findings include the following:

- Stakeholders agree that the following NISTIR 7628 security controls recommended for LICs 6, 9, and 16 are applicable to High-DER environments:
    - Using firewalls to protect the perimeter of the system, sub-systems, and particular segments of a system;
    - Implementing cybersecurity hygiene for each device used within Smart Grid;

[5] NISTIR 7628 and NIST SP 1108r4 refer to LIC9 as covering B2B connections.

  - Protecting data (at-rest and in-transit) against unauthorized access and change by using data encryption (e.g., Virtual Private Network – VPN, or Public Key Infrastructure - PKI); and
  - Protecting against service interruptions as a result of Denial-of-Service attacks.

- NISTIR 7628 also includes securing Voice over IP (VoIP) as one of the security controls applicable to the LICs that were examined. However, that control was withdrawn from a subsequent revision of NIST SP 800-53 [3]. Stakeholders agree that securing voice over IP (VoIP) is not applicable to LICs 6, 9, and 16.
- NISTIR 7628 security controls for LICs 6 and 9 that were required for the transmission domain by NERC Critical Infrastructure Protection (CIP) standards [4] were well understood and applied in appropriate contexts. For example, **Table 1** maps NISTIR 7628 security controls for LIC 6 to the relevant NERC CIP requirements, and **Table 2** provides a similar mapping for LIC 9. LIC 16 functions in the distribution domain only and therefore is not subject to NERC CIP requirements.
- When assets are owned and operated by a single organization, stakeholders within that organization are able to determine which controls are relevant to their specific environment and implement them as needed.
- While the drivers for cybersecurity protections may vary,[6] the actual protection strategies and controls are similar.

Table 1 - NIST 7628 Controls for LIC 6 Mapped to Relevant NERC CIP Requirements

Applicable NISTIR 7628 Control	Relevant NERC CIP Requirement
SG.SC-8 – Communications Integrity	CIP-012-1 (R1) - Communications between Control Centers
SG.IA-4 – User Identification and Authentication	CIP-007-6 (R5) - System Security Management CIP-005-6 (R1, R2) - Electronic Security Perimeter
SG.IA-6 – Authenticator Feedback	CIP-007-6 (R5) - System Security Management
SG.SC-5 – Denial-of-Service Protection	CIP-007-6 (R5) - System Security Management

[6] For example, risk management, a desire to innovate, regulatory compliance with current federal or state regulations, or proactive compliance with emerging regulations and standards.

SG.SC-7 – Boundary Protection	CIP-005-6 (R1, R2) - Electronic Security Perimeter
SG.SC-29 – Application Partitioning	CIP-007-6 (R5) - System Security Management
SG.SI-7 – Software and Information Integrity	CIP-010-3 (R1) - Configuration Change Management and Vulnerability

Table 2 - NIST 7628 Controls for LIC 9 Mapped to Relevant NERC CIP Requirements

Applicable NISTIR 7628 Control	**Relevant NERC CIP Requirement**
SG.SC-8 – Information Input Validation	CIP-012-1 (R1) - Communications between Control Centers
SG.SC-9 – Error Handling	CIP-012-1 (R1) - Communications between Control Centers
SG.IA-4 – User Identification and Authentication	CIP-007-6 (R5) - System Security Management CIP-005-6 (R1, R2) - Electronic Security Perimeter
SG.SC-5 – Denial-of-Service Protection	CIP 007-6 (R5) - System Security Management
SG.SC-7 – Boundary Protection	CIP-005-6 (R1, R2) - Electronic Security Perimeter
SG.SC-26 – Confidentiality of Information at Rest	CIP-011-2 (R1) - Information Protection
SG.SI-7 – Software and Information Integrity	CIP-010-3 (R1) - Configuration Change Management and Vulnerability
SG.AC-12 – Session Lock	CIP-005-6 (R2) - Electronic Security Perimeter
SG.AC-15 – Remote Access	CIP-005-6 (R1, R2) - Electronic Security Perimeter CIP-007-6 (R5) - System Security Management
SG.AU-16 – Wireless Access Restrictions	CIP-007-6 (R4) - System Security Management

3. Challenges

Adapting current approaches to cybersecurity to the type of complex, multi-stakeholder ecosystem inherent to a High-DER modernized grid environment is challenging. Current cybersecurity controls for specific LICs tend to address the technical aspects, but not the people and process aspects, of securing High-DER environments. A summary of people and process challenges that require consideration and attention, most likely from the broader community beyond NIST, include:

Multi-stakeholder environment: High-DER environment stakeholders include, but are not limited to: DER device owners, utilities, equipment manufacturers, aggregators and retail energy providers, and regulators. Driving alignment and consensus across these stakeholders is a challenge, especially given their disparate objectives and physical or informational constraints.

Heterogeneity in regulatory and business environments: Regulators are a substantial stakeholder that can influence the outcome of the cybersecurity process and are working to address the problem as they see it in their jurisdiction. High-DER environments are subject to state-level regulations which drive both how the grid is engineered and the specific security requirements for the grid and individual devices.

Stewardship of devices is varied: In a complex High DER environment, individual devices can be owned, managed, and maintained by a variety of stakeholders, each of whom believe they should have access to either manage or monitor the device. Numerous physical and informational interdependencies are not uniformly understood across all stakeholders, especially as device and system functionality continuously evolve to incorporate new technologies and business models. This leads to:

- Difficulty in ensuring that consistent security practices are implemented for devices that are not under direct control of the utilities;
- Difficulty in defining security-related roles and responsibilities, including which organization should implement, manage, and monitor security controls on individual devices; and
- Increased vulnerability of devices due to multiple stakeholders wanting to access them for multiple purposes.

Stakeholder security expectations: Interoperable devices can engage many different markets or services that include, but are not limited to, direct interactions with utilities, aggregators, and wholesale markets. This creates uncertainty over which stakeholders are responsible for specifying and managing cybersecurity controls. Access to many markets and services may also lead active stakeholders to desire complete visibility into the devices, a requirement that is not practicable over the full range of devices and interactions inherent to a High-DER electric grid.

Stovepiped structures within utilities and in industry: Multiple groups within individual utilities own pieces of the security challenge, including telecom, IT, engineering (OT), physical and cyber security, regulatory compliance (e.g., NERC CIP), grid modernization, and possibly others. Each group has insight to only some of the security controls implemented for each of the LICs. Furthermore, it appears that these groups do not necessarily interact in a way that would provide full visibility within a utility into how High DER resources are secured.

This complexity and lack of full visibility is mirrored in numerous working groups and standards organizations that are trying to solve pieces of the grid cybersecurity problem while potentially lacking a holistic view. Individual utilities do not have adequate resources to participate everywhere, and so cybersecurity engagement is often focused on affinity and attachment to a constrained set of professional groups which limits the organization's exposure to the latest strategies and best practices for grid cybersecurity controls. It should be noted that this particular challenge applies to both traditional and High-DER environments.

4. Recommendations

The stakeholder engagement and research activities completed for this work highlighted a range of opportunities to improve cybersecurity in power systems. These include the use of secure design principles that could be applied immediately, potential changes to existing NIST cybersecurity guidance, and possible ideas for future research topics.

Overall, there is a rich body of work addressing smart grid and High-DER security practices. While this body of work may not address all cybersecurity challenges, it provides a significant amount of useful information which—if applied—will substantially improve cybersecurity of modern grid operations. Examples of sources that can be consulted are:

- Electricity Subsector Cybersecurity Capability Maturity Model (C2M2) [5],
- NIST SP 800-53 Rev5 – Security and Privacy Controls for Information Systems and Organizations [3],
- NIST SP 1800-32B - Securing the Industrial Internet of Things: Cybersecurity for Distributed Energy Resources [6], and
- NIST Technical Note 2051 - Cybersecurity Framework Smart Grid Profile [7].

4.1. Secure Design Principles to Adopt Now

Several design principles were identified that could be adopted immediately. These are known design principles that could be applied to modernized power systems and High-DER environments, including:

1. **Defense in Depth –** implement layered security mechanisms to increase the security of the systems as a whole and apply multiple security controls that can address the same concern from different security perspectives.
2. **Principle of Least Privilege –** provides users, programs, and processes only with necessary privileges to complete their tasks. The system should offer only the minimum required access for each authorized user to resources they absolutely need, and access should be granted only for as long as necessary to complete that work. When properly implemented, this will substantially reduce the risk of potential cascading failure of utility operations caused by multiple devices being compromised through a single device compromise. Such cascading failures scenarios are well known and well described elsewhere [8].
3. **Principle of Least Functionality –** restricts the functions that users and devices are allowed to access only to those required to perform a task or for a device to function to reduce potential vulnerabilities and remove potential points of attack. This applies to both access to the device itself and to the functions running on the device. Examples include enforcing use of specific protocols, removal of default settings, disabling services and functionalities that are not required for specific allowed applications, and thus removing potential points of attack.
4. **Zero Trust –** assume there is no implicit trust granted to devices or user accounts based solely on their physical or network location or ownership. In other words, the overall system needs to be designed to trust devices based on authenticating their identity and confirming the functions they are authorized to perform rather than assume that the devices are trusted at all times [9].
5. **Continuity of operations –** operate under the assumption that a breach is inevitable, so the ability to anticipate, withstand, and recover from a breach is key. If a breach occurs, operations should continue—even at a diminished capacity—until the breach is resolved.
6. **Data minimization –** by default, limit collected and processed data to only what is required to fulfill a specific purpose which will result in using the least amount of data necessary. Implement appropriate technical and organizational protection measures to limit data collection.
7. **Configuration management –** do not rely on default security settings. Instead, change them to specific settings based on what is required for utility operations.
8. **Fail Secure –** when a failure occurs, the system should not be in a compromised or vulnerable state. For example, if a power failure occurs, a locked door should not become unlocked, unless there are safety or regulatory rules that require it to be

unlocked. In general, technical failures should result in actions being disallowed rather than allowed.

9. **Comprehensive monitoring and auditing –** Significant security events must generate forensic evidence that is traceable to support auditing of security events within the device. Audit trails should follow a consistent format and be available for export or direct exposure to third party applications and monitoring tools.

4.2. Changes to NIST Guidance

Based on the conducted research, the following guidelines could be updated or further developed to enhance cybersecurity in High DER environments:

1. **Update NISTIR 7628 r1 to align with NIST SP 800-53 Rev5 –** to keep up with advancements in cybersecurity, privacy, and cyber supply chain risk management, as well as advances in grid modernization including High-DER environments. NISTIR 7628 was released in 2014 and was, at that time, aligned with NIST Special Publication (SP) 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*. Since 2014, NIST SP 800-53 has been revised twice, with the most recent version (revision 5) published in 2020. The difference between NIST SP 800-53 Rev3 and Rev5 is substantial with several controls withdrawn or revised, and other new controls introduced. Most prominently, NIST SP 800-53 Rev5 includes standalone and integrated privacy and cyber supply chain risk management controls. Two examples of potential updates include:
    a. Withdrawing SG.SC-17 (Voice-Over Internet Protocol) from NISTIR 7628 r1 to align with NIST SP 800-53 Rev5 and stakeholder feedback that VOIP is not applicable to LICs 6, 9, and 16.
    b. Include malware detection and malicious command detection control (SI-3) as applicable to LICs 6, 9, and 16, as these controls are a mechanism to improve security of cross-domain communications inherent to High DER environments.
2. **Develop simplified technical guidance for customers on how to secure High-DER assets** – Consider producing simple technical guidance to end-customers, such as putting smart grid devices on a separate (guest) network segment to limit the potential for compromise of other assets at the customer site. Such guidelines will help customers become cognizant of security practices that they should adopt to protect High-DER devices and their network environments.

Additionally, stakeholders can work through numerous existing information sharing forums to enable community members to share observations, challenges, and best practices.

4.3. Future Research

Cybersecurity challenges are complex. The information and associated guidance necessary to understand and mitigate evolving security risks must be regularly updated to address changing technology, operations, and threats. The following research topics identified through this work may provide ongoing opportunities for improving the understanding of—and updating guidance for managing—emerging cybersecurity concerns for High-DER grid environments:

1. **Research how other industries solve similar problems -** Other industries may have similar security challenges in different contexts that could provide useful lessons learned for managing security of High-DER power systems. Potentially, these solutions may hold valuable insights for monitoring and managing security of High-DER grids across multiple ecosystem stakeholders. One such example to explore is an emerging solution by United States Space Command to track space debris.[7] This is a software-based solution that tracks objects belonging to multiple entities including state governments. Some of the design principles used for this solution may be useful in creating an approach where information about the status of High-DER devices can be collected and shared with those who need this information without granting every entity complete access to the device. Additional industry solutions can be identified, and lessons learned distilled, that might help drive security requirements for High-DER environments.

2. **Research security mechanisms in current commercial solutions** - Once NISTIR 7628 security control recommendations are updated to align with NIST SP 800-53 Rev5, identify whether and how the updated set of security controls are typically implemented in commercial equipment considered for the High DER scenarios.

3. **Explore Security Service Business Model** - Research potential business models for introducing independent service providers whose sole purpose would be to provide security of DER devices (e.g., cybersecurity service provider for High-DER system architectures). Examples of types of services include:

    a. Commissioning assets to ensure proper initial installation and configuration;

    b. Maintaining assets to ensure appropriate cybersecurity hygiene and flag misconfigurations; and

    c. Data aggregator and communication focal points to ensure that only relevant data is sent to appropriate stakeholders for analysis and processing.

4. **Regulatory Harmonization** – Examine the potential for creating a strawman framework that consistently satisfies 80 % of applicable cybersecurity regulatory requirements with the expectation that 20 % of requirements will always be customized based on the jurisdiction or business model. The Financial Services Profile[8] can serve as an example of such a framework.

[7] https://spacenews.com/u-s-space-command-announces-improvements-in-space-debris-tracking/
[8] https://cyberriskinstitute.org/the-profile/

5. **Updating existing NIST standards and guidelines** – Harmonization of NIST documents that are applicable to cybersecurity for smart grids could ensure applicability in the current technology environment (e.g., reconsidering VoIP protection controls in NIST IR 7628 since that has been dropped from NIST 800-53 Rev.5).

References

[1] Pillitteri VY , Brewer TL (2014) Guidelines for Smart Grid Cybersecurity. (National Institute of Standards and Technology, Gaithersburg, MD), NISTIR 7628r1. https://doi.org/10.6028/NIST.IR.7628r1

[2] Gopstein AM, Nguyen CT, O'Fallon CM, Hastings NE, Wollman DA (2021) NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 1108r4. https://doi.org/10.6028/NIST.SP.1108r4

[3] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53 Rev. 5, Includes updates as of Dec. 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[4] NERC (2021) *CIP Standards* (North American Electric Reliability Corporation, Atlanta, GA). Available at https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

[5] U.S. Department of Energy (2014) *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)*. Available at https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf.

[6] McCarthy J, Division E, Faatz D, Urlaub N, Wiltberger J, Yimer T (2021) Securing the Industrial Internet of Things: Cybersecurity for Distributed Energy Resources. (NIST NCCoE, Gaithersburg, MD), NIST SP 1800-32, Vol. B.

[7] Marron J, Gopstein A, Bartol N, Feldman V (2019) Cybersecurity Framework Smart Grid Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST TN 2051. https://doi.org/10.6028/NIST.TN.2051

[8] Lee A (2015) Electric Sector Failure Scenarios and Impact Analyses - Version 3.0. (Electric Power Research Institute, Palo Alto, CA).

[9] Rose S, Borchert O, Mitchell S, Connelly S (2020) Zero Trust Architecture. (NIST, Gaithersburg, MD), NIST SP 800-207. https://doi.org/10.6028/NIST.SP.800-207