NARUC
National Association of Regulatory Utility Commissioners

Understanding Cybersecurity for the Smart Grid: Questions for Utilities

Lynn P. Costantini

December 2020

Acknowledgments

This document was prepared by the National Association of Regulatory Utility Commissioners (NARUC) using federal funds under Award Number 70NANB18H285 from the National Institute for Standards and Technology (NIST), U.S. Department of Commerce. The statements, findings, conclusions, and recommendations are those of the author and do not necessarily reflect the views of NIST.

During the preparation process, subject matter experts provided editorial comments and suggestions. Special thanks to:

Andy Bochman, Idaho National Labs

Avi Gopstein, NIST

Danjel Bout, California Public Utility Commission

Dominic Saebeler, University of Illinois

Ashton Raffety and **Danielle Sass Byrnett**, NARUC

Please direct questions regarding this paper to **Lynn P. Costantini**, Deputy Director, NARUC Center for Partnerships and Innovation at lcostantini@naruc.org.

Cover illustration by metamorworks — shutterstock.com

NARUC
National Association of Regulatory Utility Commissioners

Introduction

Public utility commissions (PUCs) are responsible for ensuring adequate, safe, and reliable utility services at reasonable rates. As such, they need to know that utilities have effective cybersecurity risk management programs in place to mitigate cybersecurity vulnerabilities, counter malicious cyber threats, and rapidly respond to and recover from successful attacks. The evolution of the "smart" electric grid, which embraces advanced sensing and controls technologies and supports the integration of distributed energy resources, has opened new avenues for attackers to exploit and brings a new dimension to what PUCs' need to know. Understanding these risks and their impact on grid reliability and resilience[1] and to consumers is paramount.

This paper introduces cybersecurity topics relevant to the smart grid. It also suggests questions PUCs might ask utilities to better understand how they are assessing and mitigating these new risks. Concepts in this paper draw from seminal works by the National Institute of Standards and Technology (NIST) as well as topics introduced in National Association of Regulatory Utility Commissioners (NARUC)'s Cybersecurity Manual.[2] The questions presented herein complement those posed in *Understanding Cybersecurity Preparedness: Questions for Utilities*, one component of the manual.[3]

Smart Grid Defined

Leveraging advancements in digital technologies and modern communications networks, the push for a more reliable, resilient, and greener grid is only accelerating. Modernizing the grid to make it "smarter" enhances the efficiency of transmission and distribution systems, reduces the frequency and duration of power outages, and promotes the integration of distributed energy resources, such as solar, wind, and batteries. It also provides new opportunities for consumers to manage their electricity consumption and lower costs.[4]

Key enablers of the smart grid are cutting edge technologies, both hardware and software, that enable bidirectional flows of energy and offer enhanced monitoring and control capabilities. Examples include intelligent sensors, relays, switches, and new distributed technologies such as advanced metering infrastructure and automated distribution management systems. The underpinning is robust private and public communications networks capable of secure two-way information flow. *See Figure 1.*

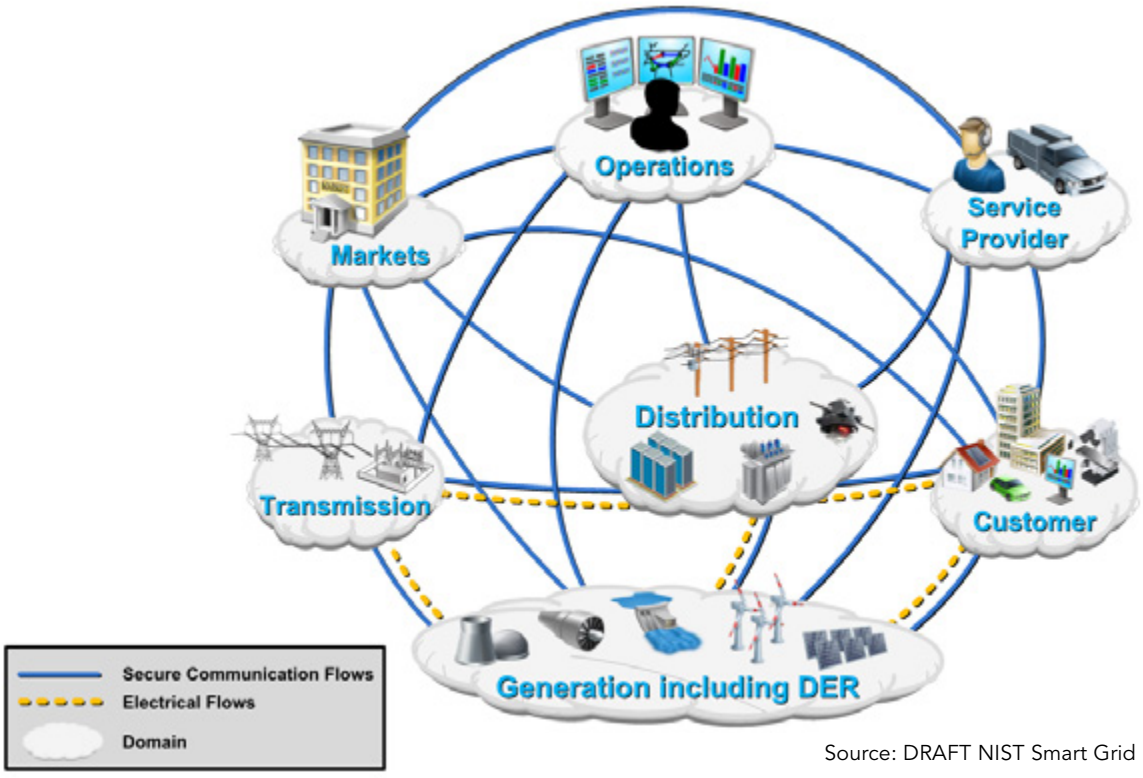
1 Resilience refers to the ability of a system to continue to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities. See https://csrc.nist.gov/glossary/term/resilience

2 "Cybersecurity Manual." NARUC, www.naruc.org/cpi-1/critical-infrastructure-cybersecurity-and-resilience/cybersecurity/cybersecurity-manual/. Accessed December 15, 2020

3 Costantini, Lynn, and Matthew Acho. 2019. "Understanding Cybersecurity Preparedness: Questions for Utilities," https://pubs.naruc.org/pub/3BACB84B-AA8A-0191-61FB-E9546E77F220

4 Office of Electricity. "Grid Modernization and the Smart Grid." Energy.Gov, 2019, www.energy.gov/oe/activities/technology-development/grid-modernization-and-smart-grid

Figure 1. Smart Grid Conceptual Model



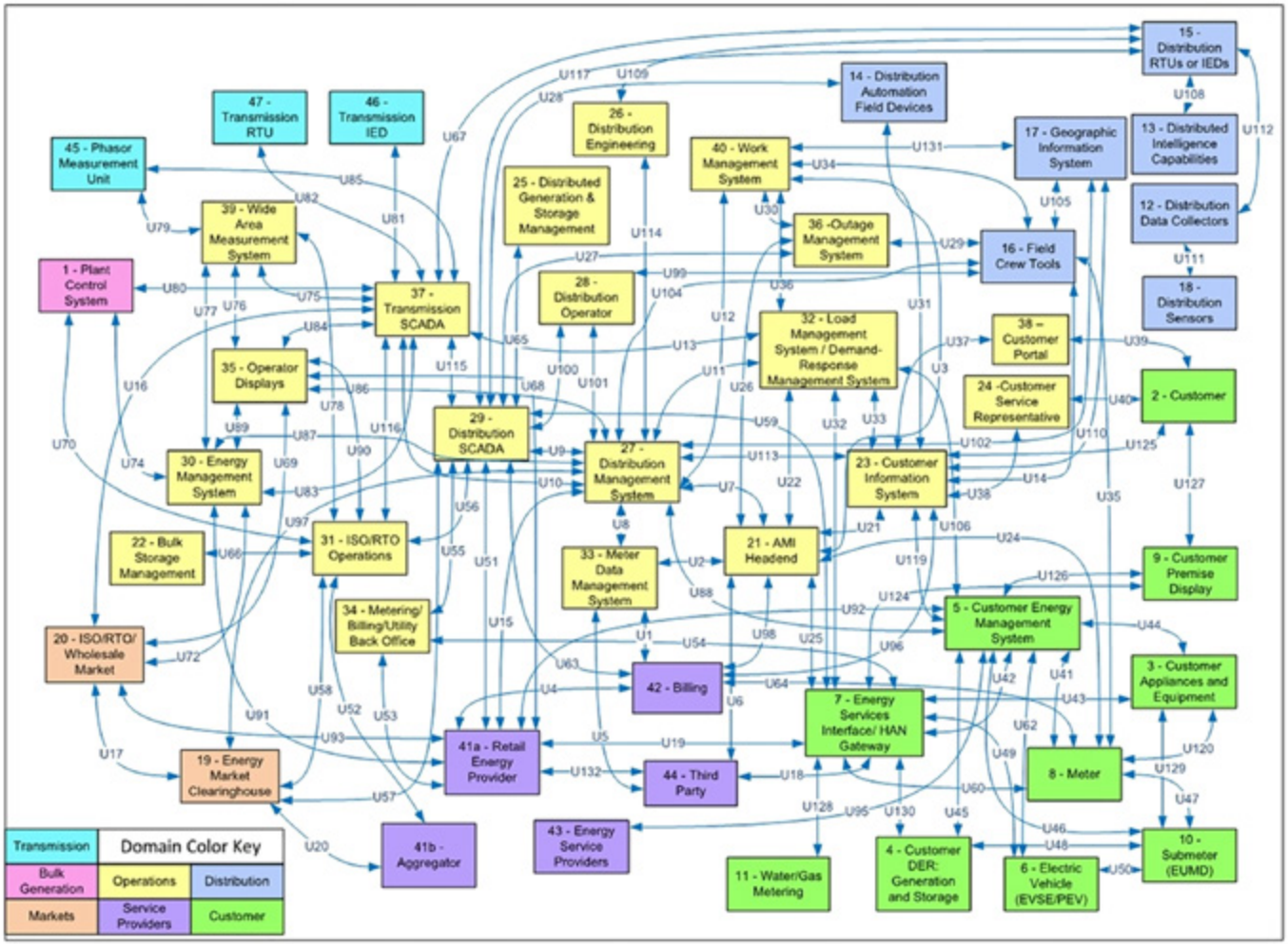
Source: DRAFT NIST Smart Grid Framework 4.0

Ultimately, the smart grid is a system of cyber-physical systems that must work together seamlessly and securely to exchange data reliably and perform predictably. In other words, delivering the intended benefits of the smart grid for utilities and consumers alike, hinges on interoperability.

Much work has focused on the architecture, functionality, and implementation of both physical and data exchange networks for interoperability purposes.[5] The rapid growth of the smart grid is due in part to the success of this work. However, the proliferation of smart technologies and the explosion of participants in the smart grid value chain has added layers of complexity to the grid. *Figure 2*, a composite diagram of entities that exchange information within and across the seven smart grid domains represented in the conceptual model, demonstrates this complexity. As connectivity, operational interdependencies, and reliance on digital infrastructures grow, so do the cybersecurity concerns. These concerns range from the availability of critical infrastructure to reliability and resilience, to data privacy.

5 See, for example, Department of Energy and EPRI.

Figure 2. Logical Reference Model



Source: DRAFT NIST Smart Grid Framework 4.0

Cybersecurity and the Smart Grid

Cyber attacks targeting the energy sector are on the rise and pose an ever-growing risk to reliability and safety. The successful attacks on the electric grid in Ukraine in 2015 and 2016 exemplify this risk. During these events, attackers took control of distribution grid operator consoles and remotely closed breakers causing local blackouts.[6,7] Potentially, attackers could penetrate communications pathways and manipulate data, or flood the highly interconnected network with data traffic limiting operators' ability to monitor and control the grid.[8] Other cybersecurity risks stem from supply chain vulnerabilities as well as the digital exchange of growing amounts of customer-specific data. Thus, securing the devices, systems, networks, and data that comprise the smart grid, even as it continues to evolve, remains a critical challenge. Effective cyber risk management and mitigation are key to meeting this challenge.

6 "Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case." 2016, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

7 Slowik, Joe. CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack. Dragos, Inc., August 19, 2019, www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf. Accessed December 15, 2020

8 "SECURITY: First-of-a-Kind U.S. Grid Cyberattack Hit Wind, Solar." 2019. Eenews.net. E&E News. October 31, 2019, https://www.eenews.net/stories/1061421301

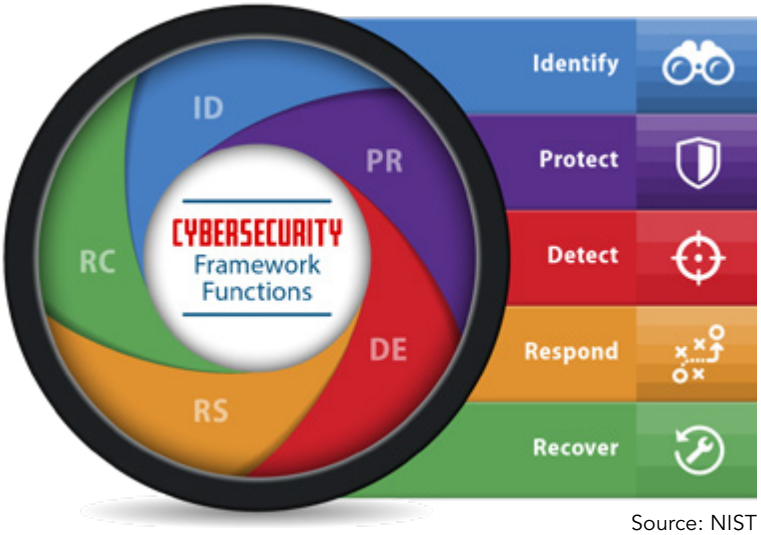
Cybersecurity Risk Management for the Smart Grid

Cybersecurity of the electric grid is not a new concern. The growing dependence on the grid for the health and wealth of the United States has prompted the federal government to focus resources on reducing cyber risks[9,10] and enforce mandatory cybersecurity standards on owners and operators of the bulk-power system.[11]

In 2014, NIST released its Framework for Improving Critical Infrastructure Cybersecurity, which provides a consistent, comprehensive, and iterative approach to identifying, assessing, and managing cybersecurity risk. The framework divides the risk management process into five discrete functions (*see Figure 3*) and categorizes specific sets of cybersecurity activities and related risk-reducing outcomes within each.

A strength of the framework is the included profile. A score card of sorts, profiles help organizations align cybersecurity functions, activities, and outcomes from the framework to their unique business goals and available resources. Once created, a profile serves as a road map between the as-is cybersecurity posture of an organization and a well-articulated desired end state.

Figure 3. Cybersecurity Risk Management Core Functions



Source: NIST

Owing to common business objectives across stakeholders, NIST has built framework profiles for specific industry sectors, such as manufacturing, maritime, and financial services. Similarly, in 2019, NIST released a Smart Grid Profile for utilities that operate electric infrastructure with high penetrations of distributed energy resources. The Smart Grid Profile prioritizes cybersecurity risk management activities and outcomes from the framework to common, high-level objectives for the smart grid: safety, reliability, resilience, and grid modernization.[12] The Smart Grid Profile also maps to the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Standards,[13] which further strengthens the alignment and prioritization of cybersecurity risk management activities in the electric sector.

Resources such as the framework and Smart Grid Profile are valuable to utilities as they work to identify, prioritize, and mitigate emerging threats to the grid.[14] They are also instructive for PUCs seeking to understand the efficacy of utilities' efforts and the relationship of those efforts to the NERC cybersecurity requirements.

---

9 Executive Order 13636: *Improving Critical Infrastructure Cybersecurity*

10 Executive Order 13800: *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*

11 "CIP Standards," NERC, accessed December 15, 2020, https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

12 Marron, Jeffrey, Avi Gopstein, Nadya Bartol, and Valery Feldman. 2019. "Cybersecurity Framework Smart Grid Profile," https://doi.org/10.6028/nist.tn.2051

13 "One-Stop Shop (Compliance Monitoring & Enforcement Program)." n.d. Accessed December 15, 2020, https://www.nerc.com/pa/comp/Pages/CAOneStopShop.aspx

14 Other tools exist, such as the Department of Energy's Cybersecurity Capability Maturity Model (C2M2), but may not specifically address smart grid assets. See https://www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf

Cybersecurity Considerations for PUCs

Changes in the design and operation of the electric grid are causing utilities and regulators alike to re-examine the potential for, and impact of, coordinated cyberattacks on geographically distributed resources. Correspondingly, utilities' cybersecurity programs must evolve to manage the increasingly complex, technologically advanced landscape. For PUCs, engaging utilities in topical discussions about their cybersecurity practices and priorities in general,[15] and for the smart grid specifically, is appropriate. PUC decisions regarding the provisioning of safe, reliable utility services benefit from knowing how utilities are identifying emerging threats, mitigating vulnerabilities, and training staff to effectively detect and respond to incidents when they occur.

The following high-level issues and related questions serve as discussion prompts for PUCs wishing to explore aspects of utilities' cybersecurity risk management program that target smart grid devices, systems, and networks, collectively referred to as assets. Thus, they are not exhaustive. For convenience, they are organized according to NIST's Cybersecurity Framework and are reflective of NIST's Smart Grid Profile.

1. **Identify**

- Mitigating potential cascading effects of an attack on the grid requires knowing what assets are deployed, where they are on the network, and their purpose. Maintaining up-to-date inventories of all operational assets, inclusive of smart grid assets, and the relationships between them are critical for grid reliability and resilience and for fostering grid modernization efforts. Keep in mind that assets typically include both hardware and software components, which should be inventoried and managed accordingly.
  - Does a current asset inventory exist, inclusive of smart grid assets?
  - Have criticality levels been assigned to smart grid assets consistent with predefined business objectives?
  - Do diagrams exist that map the integration points of distributed assets?
  - Have communications and data flows between and among devices and systems, both legacy and smart grid, been documented?
    - Do cybersecurity risk assessments include threats, vulnerabilities, and impacts specific to smart grid assets? How are threats and vulnerabilities identified? What is the periodicity of threat and vulnerability assessments?
- Utilities rely on and interact with numerous third parties, such as vendors and suppliers. The smart grid has introduced new parties, including distributed resource owners and operators. Each third-party participant introduces its own cybersecurity risks, which have the potential to impact grid operations. Interoperability expands these risks.
  - How are smart grid supply chain cybersecurity risk management processes identified, established, assessed, and managed?
  - Are cybersecurity risk management requirements included in procurement contracts with suppliers and third-party partners? If so, how is conformance with these requirements evaluated?

15 See NARUC's Cybersecurity Manual for more information.

2. **Protect**
   - Mitigating cybersecurity risks requires utilities to develop and implement appropriate safeguards that protect critical assets and ensure service delivery. Approving and controlling access to devices are key safeguards, but the highly distributed nature of the smart grid complicates these tasks. Nonetheless, cyber and physical protections support grid reliability and safety, and ensure the trustworthiness of data to and from smart grid devices.
     - Are personnel surety/background checking performed before granting personnel, including third parties, access to smart grid assets? If so, what criteria are used?
     - How are access credentials authorized, issued, managed, verified, revoked, and audited?
     - How are users, devices, and assets that connect to the grid authenticated to ensure only authorized access is allowed?
     - How is remote access to smart grid devices, including third-party access, managed? How is remote access managed for distributed energy resources owned by a third party?
   - The dependence on bidirectional, real-time data flows inherent in the smart grid increases the importance of data integrity. Control information that is tampered with may cause a safety or reliability issue. Protecting data, at rest and in transit, is an important activity to help protect the integrity of operational control information.
     - What protections are in place to ensure the integrity of device control settings?
     - How are changes to baseline configurations approved and implemented? How do configuration change control processes address devices owned by third parties?
     - Is all data residing on devices and flowing over the network encrypted? If not, what protections are in place to ensure the integrity of this data?
   - The distributed and multi-owner nature of the smart grid extends responsibilities for cybersecurity beyond utilities. Ensuring all personnel, including third parties, receive training commensurate with their roles is imperative to grid safety, reliability, resilience, and grid modernization efforts.
     - Are cybersecurity roles and responsibilities defined? If so, are third parties included?
     - Is training for security personnel tailored to understanding the unique risks of the smart grid? Are third parties participating in training?

3. **Detect**
   - Discovering cybersecurity events in a timely fashion is essential to ensuring safety, reliability, and resilience. Smart grid assets by nature rely on hardware, firmware, and software, and as such, must be continuously monitored for signs of intrusion.
     - Do policies and procedures regarding cybersecurity event detection address smart grid assets? Do they include threat detection and monitoring? Are suspicious activity thresholds assessed and updated in accordance with policies? Are automated log analytic tools employed?
     - Are regular vulnerability tests conducted? Are third-party assets included in these detection activities? How are findings prioritized and corrected? What interim procedures are in place to mitigate risks before corrections can be accomplished?
     - Is threat and vulnerability information shared with relevant third parties?

4. **Respond**
   - Despite protection efforts, cybersecurity incidents will occur. Rapid and effective response to contain the impact of such incidents is essential for grid reliability. However, care must be taken to ensure that response actions do not adversely affect grid operations. Because of the distributed nature of the smart grid, response plans must reflect an understanding of the operational impacts of the failure of a single asset as well as assets in the aggregate.
     - Are cyber incident response policies and plans in place for minimizing the effects of a cyber incident involving smart grid assets? Are the operational impacts well understood?
     - Do response plans include interactions with third parties?
     - Are third-party roles and responsibilities for recovery defined?
     - Are third-party incident notification requirements documented?
   - Effective response to cyber incidents requires routinely testing plans and capabilities. In smart grid environments, the inclusion of third parties enhances effectiveness.
     - How frequently are cyber incident response plans tested? Are third-party service providers and asset owners involved?
     - How are lessons learned addressed? Are response plans updated to incorporate lessons learned?
5. **Recover**
   - The speed with which utilities can restore assets to acceptable levels of functionality following cybersecurity incidents is the ultimate bellwether for grid reliability and resilience. As with other aspects of cybersecurity, the distributed nature of the smart grid and numerous third parties involved complicate restoration efforts. Overcoming these challenges require attention to detail and inclusiveness.
     - Are minimum functionality thresholds documented for smart grid assets?
     - Do restoration plans reflect smart grid assets based on their priority designation?
     - Are restoration plans communicated to and coordinated with third parties including owners of distributed resources?

Conclusion

As the smart grid continues to grow and evolve, cybersecurity concerns loom large. Utilities must be diligent and broaden their cybersecurity risk management policies and practices to address their new operational environment. As PUCs consider issues around smart grid deployments, engaging utilities in discussions relating to their emerging cybersecurity challenges and mitigation efforts is invaluable. The issues explored in this paper are intended to facilitate those discussions.

NARUC
National Association of Regulatory Utility Commissioners

1101 Vermont Ave, NW • Suite 200 • Washington, DC 20005
www.naruc.org • (202) 898-2200