NRRI Insights *Practical perspectives on critical policy issues.*

APRIL 2021

Understanding Cyber Attacks and Available Cybersecurity Technologies

Peter Fischer; Karen Wayland, Ph.D.; and Chuck Louisell

Introduction

The electric grid is undergoing rapid transformation as a result of new technologies being deployed on utility networks and behind-the-meter by consumers. Many of these technologies produce and transmit massive amounts of data and are increasingly connected to grid operations centers through network-based communications. The growing connectivity between the grid and customer devices increases cybersecurity vulnerabilities and broadens the threat landscape by expanding the number of potential entry points through which malicious cyberattacks can be launched. A 2019 survey of utility security professionals revealed that the frequency and potency of attacks on utility systems is increasing, with 56 percent experiencing at least one attack in the past year that resulted in either the loss of data or an outage.[1]

This paper reviews the potential threats that utilities are facing to operations technologies (OT) and the new equipment that utilities may use to stop or minimize problems associated with these cyber events. An understanding of these threats and how to minimize them will help regulators and utility staff assess requests for rate increases for implementing these mitigation strategies.

Although in recent years U.S. energy companies have spent only a small percentage (0.2 percent) of their revenues on cybersecurity,[2] more than two thirds of executives surveyed for *Utility Dive*'s 2020 State of the Utility report said their utility had increased its spending on cyber protections.[3] Since the 2015 cyberattack on a Ukrainian distribution company, utilities have focused increasingly on cybersecurity investments,[4] either as part of overall grid modernization plans or as stand-alone expenditures. A recent Guidehouse report projected that global smart grid security expenditures will nearly double to $3.2 billion annually between 2017 and 2026.[5]

Despite these increased security expenditures, the cybersecurity threat landscape is expanding. In many cases, these new threats are asymmetric, perpetrated using low-cost, widely available, and difficult-to-detect tools that bypass utility system

1 Ponemon Institute and Siemens Gas and Power, "Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?," https://assets.new.siemens.com/siemens/assets/api/uuid:35089d45-e1c2-4b8b-b4e9-7ce8cae81eaa/version:1572434569/siemens-cyber-security.pdf, accessed March 16, 2021.

2 Steve Morgan, "Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021," *Cybercrime Magazine,* June 10, 2019, https://cybersecurityventures.com/cybersecurity-market-report/.

3 "State of the Electric Utility: 2020 Survey Report," *Utility Dive,* https://resources.industrydive.com/state-of-the-electric-utility-survey-report-2020, accessed March 16, 2021.

4 Robert Walton, "Utilities say they are prepared to meet cyber threats. Are they?," *Utility Dive,* February 14, 2020, https://www.utilitydive.com/news/utilities-say-they-are-prepared-to-meet-cyber-threats-are-they/572080/.

5 Richelle Elberg and Mackinnon Lawrence, "From Smart Grid to Neural Grid: Industry Transformation and the Top Five Technologies Poised to Bring the Grid into the Cloud," January 2, 2018, https://guidehouse.com/-/media/www/site/insights/energy/2018/from-smart-to-neural-grid--industry-transformation.pdf.

cyber-protections by taking advantage of vulnerabilities, such as those described later, to cause maximum damage or disruption. Distribution utilities are grappling with the implications of projections that millions of consumer digital devices will connect to the grid in the coming decade, creating new pathways for cyber-attacks. More importantly, cyber attackers are increasingly targeting not just data theft through information technologies (IT), but also causing disruption through targeting operational technologies (OT)—the equipment and systems that generate and transmit electricity. These attackers target OT systems with the intent of causing equipment damage and power outages.[6] At the same time, the coronavirus pandemic has introduced new challenges that must be addressed in utility cyber plans, including managing risks generated in the expanded connected constellation, as workers and vendors access critical data and systems remotely from a wide variety of origination networks and devices, including home computers.[7]

The good news is that catastrophic cyber risks for utilities, such as an attack that significantly interrupts system operations, causing blackouts or reducing energy availability, can be mitigated through a combination of technology and software hygiene practices, including ensuring that security updates are regularly installed. Following these practices can lead to a more resilient electric grid.

One challenge for regulators and utilities is that the useful product lifecycle of most cyber technologies is much shorter than that of conventional utility assets (3-7 years vs. 30-40 years).[8] Furthermore, new cyber technologies can protect against emerging threats and mitigate catastrophic risks, but may also render cyber protections currently in place obsolete long before the end of the expected lifecycle of those assets. When these new technologies become commercially available, utilities and regulators must consider the possibility that an entire class of utility assets or cyber equipment could become obsolete, what Dr. Carl Pechman of NRRI refers to as "catastrophic cyber obsolescence."[9] An example of catastrophic cyber obsolescence would occur if, as in some telecommunications networks, a utility needs to replace all potentially cyber compromised Huawei equipment before it is fully depreciated, creating a significant regulatory asset. [10]

There are several approaches to reducing the risk and impact of catastrophic cyber obsolescence. One is to develop new cost recovery measures for replacing existing equipment before it is fully depreciated; another is to ensure that any new cyber technologies deployed by the utility provide maximum flexibility and security to respond to known and unknown cyber-attack signatures.

As state public utility commissions evaluate utility strategies underlying utility cybersecurity investment plans, they may need to consider the deployment of flexible cybersecurity technologies that can protect against catastrophic threats. The rapidly changing threat landscape and the technologies available in the market to mitigate those threats complicate the prudent investment test that regulators typically apply to proposed investments. These tests evaluate whether the decisions made were reasonable based on what is "known and knowable." Given the rapid evolution of both the threats and technological

6 Ponemon Institute and Siemans Gas and Power, "Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?," https://assets.new.siemens.com/siemens/assets/api/uuid:35089d45-e1c2-4b8b-b4e9-7ce8cae81eaa/version:1572434569/siemens-cybersecurity.pdf, accessed March 16, 2021.

7 West Monroe, "2020 Energy & Utilities Outlook: Mid-Year Update," https://www.westmonroepartners.com/perspectives/report/2020-energy-and-utilities-outlook, accessed March 16, 2021.

8 Institute for Energy and the Environment, *Improving the Cyber Security of the Electric Distribution Grid: Phase 2 Report,* Vermont Law School, November 2019, https://www.vermontlaw.edu/sites/default/files/2019-11/VLS%20IEE%20-%20Cybersecurity%20Report%20-%20Phase%202.pdf.

9 Personal communication between authors and Dr. Carl Pechman, February 2020.

10 The U.S. government has determined that Huawei equipment manufactured in China constitutes a potential cyber threat to communications and other networks, Federal Communications Commission, "FCC Designates Huawei and ZTE as National Security Threats," Press Release, June 30, 2020, https://docs.fcc.gov/public/attachments/DOC-365255A1.pdf.

protections, it would be useful for regulators to have an understanding of how cyber-attacks can be mounted against utility assets and the ability of alternative types of commercially available technologies to provide flexible protection.

This paper provides regulators with background information about the current technologies available to detect and prevent cyber attacks, from basic firewalls to emerging cybersecurity technologies. The impact of a cyber attack on any asset will vary, depending on its location in the network and the service it provides. Therefore, it important to understand not only attack vectors, but the potential impact associated with a successful attack. For this reason, not every asset on the grid requires the same level of protection. As a consequence, we also discuss attack vectors and methods for evaluating cybersecurity investment requests. The paper seeks to inform discussions between regulators and utilities about cybersecurity investments and strategies centered on cyber-technologies and the prevention of catastrophic failure. We also provide some security approaches that may help protect both modern and legacy supervisory control and data acquisition (SCADA) systems from unknown vulnerabilities as part of a reasonable and prudent cybersecurity strategy.

Grid Integration Brings Benefits and New Threats

Electrical grid networks, including computers, data networks and operator interfaces, are often referred to as OT or SCADA networks. Electrical grid OT networks are increasingly being integrated with enterprise and IT networks for clear operational and business advantages. Among the integration benefits are:

- Improved data collection from OT systems into IT Systems to provide a better understanding of OT network performance, allowing system operators and business leaders to make decisions based on readily available data insights.

- Real-time warnings of system degradation and failure, which enable faster repairs, resulting in less down-time.

- Easier equipment updates, because software can be pushed to OT devices from a remote location rather than requiring on-site visits.

Integrating electrical grid OT networks with IT networks has clear advantages, but it also introduces new cyber risks. IT cybersecurity focuses on the information security triad of "CIA" — data confidentiality (C), data integrity (I), and data availability (A). The CIA triad drives IT cybersecurity professionals to focus on protecting data above all else. OT cybersecurity is less concerned with protecting data and focuses instead on cybersecurity practices that enhance the availability (A), reliability (R), and safety (S) of OT networks and systems. For this reason, regulators evaluating utility requests for recovery of cybersecurity investment, may want to ask not only about the way in which these investments provide data security, but also how the investment preserves or improves the availability, reliability, and safety (ARS) of OT networks and systems.

Integrating IT and OT systems has also increased the vulnerability of OT systems to cyber-attack. The recent National Academies of Science report, *The Future of Electric Power in the United States*[11] notes that "The current grid is monitored by connected sensors recording physical changes, and the sensor data is telemetered using ICT for analytics and subsequent control decisions, and decisions are telemetered to end points that take physical actions to protect or operate the system. Every component and communication step in this process, and any combination thereof, is potentially subject to cyberattack; the availability of data to the intended recipient can be compromised, the integrity of the data can be altered through malicious intervention, or the confidentiality of the data can be breached."

We review different types of "malicious interventions," or cyberattacks, against grid infrastructure in the following section, and then examine why

11 National Academies of Sciences, Engineering, and Medicine, *The Future of Electric Power in the United States,* 2021, https://doi.org/10.17226/25968.

boundary protection between IT and OT systems requires a new paradigm.

Types of Cyber-attacks

Cyber-attacks against the electric grid can be initiated via malware, advanced persistent threats, insider threats, human error, hardware Trojans,[12] and other threat vectors. The most well-known method, the one used against the Ukrainian grid, is a successful phishing attack through the IT network that plants malware in the company's systems.[13] The malware gains access to protected resources or applications, at the command or administrator level and allows hackers to make their way to the OT network, where they launch an attack. Advanced Persistent Threats (APTs) are a more nefarious type of malware that penetrate an OT network and lie dormant,[14] like a bomb that does not detonate unless and until it is triggered by an event or command. Insider threats are employees or other trusted personnel who can act as a vector for malware introduction or use other methods to threaten or violate the ARS protection model of OT networks and systems. Human error is an unintentional method of cyber-attack, where hazardous commands or other unintentional actions threaten a network. An emerging cybersecurity threat is the hardware Trojan, characterized by altered integrated circuit (IC) chips inserted into equipment during the manufacturing process before delivery and installation. When triggered, hardware Trojans cause operational technology devices to misbehave in unpredictable ways.

All of these threat types can either corrupt network data or initiate activities that can damage equipment or disrupt electricity delivery. Utilities must invest in and use robust cybersecurity to protect against these threat types.

Advanced Persistent Threats (APTs) and Hardware Trojans may pose the most critical threats to the grid, because they remain hidden despite surveillance. APTs include "zero-day" threats, which the cybersecurity firm FireEye™ defines as "an undiscovered software flaw . . . that exposes a vulnerability in software or hardware and can create complicated problems well before anyone realizes something is wrong. In fact, a zero-day exploit leaves NO opportunity for detection."[15]

Widespread zero-day vulnerabilities are real. In July 2019, cybersecurity firm Armis® announced that it had discovered 11 zero-day vulnerabilities in VxWorks,® the operating system used in more than 2 billion devices, including critical industrial, medical, and enterprise applications. Armis described the potential impact of the VxWorks zero-day vulnerabilities as "an attacker who has already managed to infiltrate a network [and] can use [this vulnerability to]. . . broadcast an attack capable of taking over all impacted VxWorks devices in the network simultaneously."[16] A widespread zero-day vulnerability exploited by a hostile nation state or other bad actor is a likely path for initiating a potentially catastrophic event.

Optimizing Cybersecurity for OT

Cybersecurity technologies offer different levels of protection for utility OT networks **(Table 1),** so it is important to understand the capabilities of different classes of commercially available technologies that can be deployed on the grid, from current,

12 According to IEEE, a hardware Trojan is the "Malicious modification of hardware during design or fabrication … Such tampering … causes an integrated circuit (IC) to have altered functional behavior, potentially with disastrous consequences in safety-critical applications. Conventional design-time verification and post-manufacturing testing cannot be readily extended to detect hardware Trojans due to their stealthy nature, inordinately large number of possible instances and large variety in structure and operating mode," https://ieeexplore.ieee.org/document/5340158.

13 The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. Oxford Languages, https://www.google.com/search?q=phishing+definition&rlz=1C1CHBF_enUS781US781&oq=phisi&aqs=chrome.2.69i57j0i10i433i457j0i10i433l3j46i10j0i10i433j0i10.4537j0j7&sourceid=chrome&ie=UTF-8.

14 National Institute of Standards and Technology, "Glossary: Advanced Persistent Threat," https://csrc.nist.gov/glossary/term/advanced_persistent_threat, accessed March 25, 2021.

15 FireEye, "What is a Zero-Day Exploit?," https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html, accessed March 16, 2021.

16 Ben Seri, "Urgent/11: Affects Additional RTOSs: Highlights Risk to Medical Devices," Armis blog post, https://www.armis.com/resources/iot-security-blog/urgent-11-update/, accessed March 16, 2021.

Table 1 — Comparison of OT Cybersecurity Technologies

Capability Required to Protect Grid Network	In-Line Edge Devices	IDS/IPS	Next Generation Firewall	Unidirectional Gateway
Protection against insider and advanced persistent threats	☑			
Processing & validating the entire content of every message	☑			
Security that accounts for operational conditions and system state	☑			
Adaptive operating modes to support workflow and ensure system reliability	☑			
Secure one-way data flow	☑			☑
FIPS 140-2* for data confidentiality and node validation	☑		☑	
Anomaly detection with custom protocol specific logging	☑	☑	☑	
Deep content inspection of industrial protocol message headers and payloads	☑			
Block unauthorized network ports, addresses, and protocols	☑	☑	☑	☑
*The Federal Information Processing Standard 140-2 (FIPS 140-2) is a NIST accreditation program for validating that cybersecurity technologies meet federal security standards.				

well-understood technologies, to new and disruptive technologies designed to optimize OT security. The typical elements of a well-designed converged IT-OT architecture are described below in the order in which they would be encountered in a multi-layered defense.

Firewalls

Firewalls are the first line of defense employed in IT networks. Gartner defines a firewall as "an application or an entire computer (e.g., an Internet gateway server) that controls access to the network and monitors the flow of network traffic. A firewall can screen and keep out unwanted network traffic and ward off outside intrusion into a private network. This is particularly important when a local network connects to the Internet. Firewalls have become critical applications as use of the Internet has increased."[17] In the past, firewalls prevented cyber intrusions by blocking outside access by a specific entry port and/or by Internet address. These early devices executed access control rules based on an access control list maintained by the system administrator.

Over the past five years, with the advent of cloud computing, the firewall has increased in importance and functional scope. Not only does it need to protect port access and block specified fixed internet address outside traffic, but it now also needs to be able to evaluate the risk associated with dynamic cloud-hosted applications that may change version and points of origin even through the course of a single day. To this end, the most advanced next generation firewalls incorporate multi-layer signature recognition algorithms that screen for threats based on real-time global threat intelligence. This global threat intelligence is primarily directed to IT network threats but also can identify and block the persistent outsider threats that enter utility enterprises through IT systems.

17 Gartner, "Gartner Glossary: Firewall," https://www.gartner.com/en/information-technology/glossary/firewall, accessed March 16, 2021.

Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS)

Like firewalls, modern Intrusion Detection Systems and Prevention Systems (IDS/IPS) monitor incoming traffic and look for signatures of known malicious cyber behavior. These systems include malware and port scanning agents that probe the network to find open pathways to get to target systems, such as critical machine control systems. Like next generation firewalls, modern IDS/IPS technologies use real-time global threat intelligence and artificial intelligence to monitor data at the packet level to identify threats, trigger isolation strategies at machine speed, and alert administrators so that they may plan and execute remediation and recovery strategies. Although the combination of next generation firewalls and modern IDS/IPS technologies is aimed at establishing the highest potential level of cyber hygiene possible to detect and isolate threats rapidly, they are not capable of protecting machine operations integrity and availability alone. Additional hardware protection is required to ensure protection from cyber threats.

Unidirectional Gateways

Unidirectional Gateways have played an important role in the converged IT-OT architecture over the past decade. They have been used to establish a buffer between the IT and the OT environment, called the DMZ. The DMZ device or application acts as the traffic director to ensure that only authenticated users on compliant devices originating from authorized networks can access data generated at the machine control layer. They provided a secure data export from the OT network into the IT network by replicating or emulating database copies from the OT side onto the IT side to provide monitoring and control data to authenticated users and applications while enforcing one-way, outbound data flow.

Although unidirectional gateways are useful, commissions and utilities should be aware of their drawbacks. First, they introduce system complexity due to the requirement for data replication and static access publication in the IT network. Second, as connected machine technology advances, the machines increasingly require real-time feedback and control loop interaction via cloud-hosted applications to gain the degree of precision management associated with smart grid and micro-grid operations. This means that the usefulness of unidirectional gateways will diminish over time, leaving a machine integrity and availability protection gap that must be filled by new, disruptive technologies such as dedicated in-line, edge protection.

In-Line Edge Cybersecurity Devices

The newest and most protective technologies against cyberattacks are in-line cybersecurity devices that can be deployed within a network boundary. These devices offer unique capabilities to ensure that malicious commands cannot reach equipment, such as deep content packet inspection of all messages or commands and the comparison of incoming commands to operational conditions and system state. The devices are programmed with all possible operational commands for a particular piece of equipment and will prevent the execution of any command outside the safe operational parameters of the equipment, a process referred to as "whitelisting." In-line cybersecurity devices protect operational systems not only from incoming cyberattacks, but also from dormant APTs. In addition, these devices can isolate and repair systems suspected of sabotage or subversion by a foreign adversary or other bad actor. By allowing only commands within a defined range set by the grid operator to process, in-line edge cybersecurity devices also protect against insider threats and human error, because they prevent all commands that would cause catastrophic equipment disruption/destruction, regardless of the source.

Not every piece of equipment on a utility network merits the highest level of protection; utility planners and state commission reviewers must consider both the risk to an individual system and the risk of service disruption. Some systems or devices (such as a sub-station transformer) may be so expensive to replace or provide such a critical function that they merit the most comprehensive (and potentially most expensive) cyber protections. Other devices may be easily replaced and so would only merit the highest level of protection if they were located in a particularly critical node of the network.

Assessment frameworks to evaluate the objective risk to an individual device and to the larger system have been developed by the U.S. Department of

Energy (DOE)[18] and the North American Electricity Reliability Corporation (NERC). These frameworks assign consequence classes based on multiple risk dimensions to inform cybersecurity investments. The Federal Energy Regulatory Commission (FERC) is responsible for the security of the bulk electric power system and has designated NERC as the authority to issue and enforce cybersecurity standards.

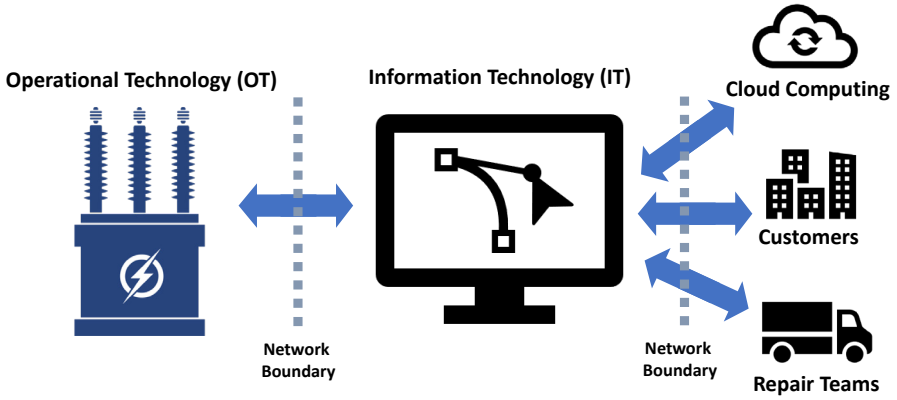
A New OT Cybersecurity Paradigm

The capabilities of the rapidly evolving cyber technologies now available on the market call for a new OT cybersecurity paradigm that goes beyond NERC CIP compliance to a risk-based approach similar to the NIST 800-53 risk management framework. The National Association of Regulatory Utility Commissioners (NARUC) recently published guidance for the international regulatory community for evaluating utility proposals for cyber investments.[19] The guidance articulates two approaches to implementing cybersecurity on a networked grid – the compliance-based approach and the risk-based approach. An important tool in this guidance is the Zero Trust Model, in which no single cybersecurity solution is trusted by default or expected to be a single point of enforcement. This model assumes that because unauthorized network access will happen and zero-day vulnerabilities will be discovered, many levels of dynamic network segmentation and protection are required.

Implementing the Zero Trust Model requires that the electric industry embrace a new, layered protection paradigm, such as the approach recommended by the National Institute of Standards and Technology (NIST 18-207).[20] NIST's guidance states that "a single security product, technology or solution cannot adequately protect an ICS by itself. A multi-layer strategy involving two (or more) different overlapping security mechanisms, a technique also known as defense-in-depth, is required. A defense-in-depth architecture strategy includes the use of firewalls, the creation of demilitarized zones, intrusion detection capabilities along with effective security policies, training programs, incident response mechanisms and physical security."[21] State commissions may be able to enhance the utilities' implementation of these practices by reviewing and enforcing the implementation of NIST guidance and potentially incenting utilities to ensure that it is implemented.

NIST's approach to OT network security focuses to a large extent on layers of network boundary security, as shown in **Figure 1.** This approach is defined as "monitoring and control of communications at the **external boundary** (emphasis added) of an information system to prevent and detect malicious and

Figure 1. Network Boundaries in a Utility System



18 See U.S. Department of Energy Cybersecurity Capability Maturity Model (C2M2) Program, https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0, accessed March 16, 2021.

19 Elena Ragazzi et al., *Evaluating the Prudency of Cybersecurity Investments: Guidelines for Energy Regulators,* National Association of Regulatory Utility Commissioners, May 2020, https://pubs.naruc.org/pub.cfm?id=9865ECB8-155D-0A36-311A-9FEFE6DBD077.

20 Keith Stouffer et al., *Guide to Industrial Control System (ICS) Security,* National Institute of Standards and Technology, SP 800-82 Rev.2., May 2015, https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final.

21 Keith Stouffer et al., *Guide to Industrial Control Systems (ICS) Security,* National Institute of Standards and Technology, SP 800-82 Rev.2, May 2015, https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final.

other unauthorized communication, through the use of boundary protection devices."[22] The boundary protection approach relies primarily on firewalls, and, to a lesser degree, to unidirectional gateways. It is therefore important to recognize the advantages provided by an (operational) zero trust model that evaluates the reasonableness of internal signals.

As we pointed out, not all cybersecurity processes protect against all threats. A weakness in NIST's boundary-focused approach is exemplified by two 2020 cyberattacks against oil and gas and water Industrial Control Systems (ICS). In each case, boundary protections were bypassed to reach and harm Intelligent Electronic Devices (IEDs) inside the boundary. In one instance, malware traveled through an IT network into the OT system of an oil pipeline compressor station, where it triggered ransomware that encrypted the memory modules of several IEDs, leading to their failure. The net effect was a two-day shutdown of the pipeline, and the replacement of all the IEDs made inoperable by the malware.[23]

In a second instance, in April 2020, an Israeli cyber research organization reported that a water treatment system's Programmable Logic Controllers (PLCs, or computers hardened for industrial processes) had their software modified by malware, causing the PLCs to issue control orders causing water valves to behave erratically.[24] A more recent example occurred at a Florida water treatment plant, where remote access allowed a hacker to gain access to the system and adjust sodium hydroxide to dangerous levels. This attack was unsuccessful, because the change was noticed, but a more sophisticated attack that masked the change could have led to catastrophe. These types of attacks are exactly what in-line edge cyber security is designed to protect against by whitelisting only "safe" operations.

These recent, real-world cyber-attacks help us to understand the nature of threats to the electric grid. The same cyber-attack methods can (and will) be used to bypass grid boundary protection to reach IEDs that control the operation of substations and other critical infrastructure.

The advent of new cyber technologies that can be deployed within the network boundary has expanded the concept of layered security to include innovative in-line edge devices that will provide key defenses against advanced persistent threats (APT) that have breached boundary cybersecurity protections. Cybersecurity professionals and control system engineers have begun to develop new standards that embed cybersecurity protections in grid Intelligent Electronic Devices (IEDs).

A recent standard adopted by the International Electrotechnical Commission (IEC) for industrial automation and control systems, IEC 62443, addresses "embedded devices, network components, host components, and software applications."[25] Another standard, IEEE Std. C37.240™-2014,[26] establishes cybersecurity standards for IEDs deployed in the electric grid to protect substation automation and control systems.

Although these standards are positive steps toward creating densely layered grid cybersecurity protections, they are not mandatory, so there is no regulatory regime to ensure compliance. Original Equipment Manufacturers (OEMs) may choose to implement either standard — or neither. Indeed, even assuming some OEMs begin designing cybersecurity features into their IEDs, widespread grid

22 Ibid.

23 Christian Vasquez, "Cyberattack Shut Down Gas Pipeline for Days — DHS," *E&E Energy Wire,* February 19, 2020, https://www.eenews.net/stories/1062388455.

24 Edward Kovacs, "Hackers Knew How to Target PLCs in Israel Water Facility Attack: Sources," *SecurityWeek,* April 30, 2020, https://www.securityweek.com/hackers-knew-how-target-plcs-israel-water-facility-attacks-sources.

25 International Society of Automation, "New ISA/IEC 62443 Standard Specifies Security Capabilities for Control System Components," https://www.isa.org/intech/201810standards/, accessed March 17, 2021.

26 IEEE, –"IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems," *IEEE Std C37.240-2014,* January 30 2015, doi: 10.1109/IEEESTD.2015.7024885.

deployment will take years, if not decades.

While companies are designing these protections into their systems, encryption and two-factor authentication may be insufficient to protect the electric grid. The immediately available solution is deploying in-line devices to protect one or more IEDs. These devices can inspect every command and message to an IED and deny those that are outside the operating parameters of the IED. This equipment could be used in substations and other vulnerable grid locations to protect against the various cyber-attack methods described previously in order to provide the missing grid defense-in-depth element.

The in-line cybersecurity devices available on the market today supplement NIST's reliance on boundary protection with capabilities beyond many boundary defense devices as shown in **Table 1** and provide a flexible and, therefore, lower risk approach to securing utility networks, SCADA, and OT systems. These technologies build upon current security best practices to respond to the rapidly evolving cyber threat landscape and provide protection against catastrophic cyber risks, such as insider threats, zero-day vulnerabilities, and advanced persistent attacks from nation states. Importantly, this technology provides flexibility against by repelling attacks regardless of the source or type. Other technologies could be rendered obsolete if the attackers can skirt protections. In line cyber-devices are just emerging into the market. These inline devices incorporate operational contingencies and emergency protocols that provide a rapidly integrated minimally intrusive for the utility operational systems.

New in-line devices that provide additional advantages over other cyber protections are being tested at EPRI and the DOE national labs. The design of these devices streamlines the way this technology can be inserted into existing networks to provide in-depth cyber defense by diversifying the technologies currently used. Adapting cybersecurity architecture and regulations to accommodate these new in-line tools may provide a valuable tool for mitigating catastrophic cyber risks, increasing the inherent security and resiliency of the utility grid's networks and systems.

Guarding Against Obsolescence

Grid modernization and the convergence of IT with SCADA and OT systems is a trend that will only grow as the benefits of connected control systems are realized. However, this trend creates increased cyber-physical risks for utility power systems. As outlined in this paper, these cyber risks may cause potentially significant failures, with financial impacts to both utilities and the customers they serve. The risk of cyberattacks can be mitigated in an operationally effective manner through deployment of cyber technologies and security practices, leading to a more resilient electric grid.

The rapid evolution of both the threat landscape and cyber technologies to respond to these threats complicates the traditional cost recovery process for utilities and regulators, who must now contend with two related obsolescence issues. The first is the possibility that the onboard cyber protection capabilities built into high-cost, long-lived components in major electrical equipment are eclipsed by emerging threats, creating pockets of vulnerability. The second is that new technologies with superior capabilities over currently installed cyber-technologies will become commercially available before the older equipment is fully depreciated. Both situations could potentially create regulatory assets to account for obsolete equipment that is retired early, resulting from replacement of grid assets before the anticipated end-of-life considered in utility investment plans.

The in-line cyber technologies described in this paper **(see Table 1)** are a cost-effective solution to provide flexibility against an ever changing threat environment, thereby potentially avoiding the early retirement of high-cost, long-lived equipment. The cost of deploying these new protections is relatively low in comparison to the cost of replacing damaged equipment and, although difficult to calculate, provides significant avoided costs of economic loss in the event of disruption.

The problem of evaluating cost recovery requests for new cyber technologies that make existing cyber protections obsolete is a difficult subject that is beginning to garner the attention of regulators and academics alike. This paper attempts to resolve that problem by providing an overview of currently avail-

able cyber protection technologies. This information may be helpful in guiding discussions among utilities, regulators, and consumer advocates as they evaluate cyber investment plans. The test for financial recovery investments made to mitigate against disruptive cyber technologies is "reasonable and prudent." This test is complicated by the unknown nature of these risks. Given the severity of the cyber threats, regulators may wish to consider the importance of these investments in rate making cases to encourage utilities to adopt these technologies as part of their annual security reviews. Doing so will help to ensure timely improvements to the utilities' cybersecurity posture by ensuring that cyber technologies that can identify and reduce threats are introduced proactively.

About the Authors

Peter Fischer is the senior director of Cyber Programs at Sierra Nevada Corporation (SNC), a high-tech electronics, engineering, and manufacturing corporation. He is responsible for product strategy, new product development and market launch of SNC's portfolio of cyber security products.

Dr. Karen Wayland is CEO of GridWise Alliance and Principal at kW Energy Strategies, where she provides strategic consulting on grid modernization and clean energy policy. She is a recognized expert in national energy and environmental policy and served in leadership positions at the highest levels of government and nonprofits, including as policy advisor at the U.S. Department of Energy and to the Speaker of the House.

Chuck Louisell, PhD, PE, M.ASCE is a senior strategic program manager at Cisco Systems, Inc., where he specializes in systems engineering.

About NRRI

The National Regulatory Research Institute (NRRI) was established in 1976 as the research arm of the National Association of Regulatory Utility Commissioners (NARUC). NRRI provides research, training, and technical support to State Public Utility Commissions. NRRI and NARUC are co-located in Washington, DC.

The purpose of *NRRI Insights* is to provide a forum that gives readers information about and insights into new ideas, questions, and policy positions affecting the regulatory community. To that end, these articles represent differing points of view, policy considerations, program evaluations, etc. and may be authored by those with an economic or policy interest in the subject. We hope that sharing diverse ideas will foster conversation that will support innovation in the industries we study. Each of the papers is reviewed both internally and externally for factual accuracy and their contribution to the body of regulatory knowledge. NRRI encourages readers to respond to these articles, either via "letters to the editor" or by joining the conversation with critiques/articles of their own.

NRRI provides these diverse views as part of our role fostering communication in the regulatory community, and we do not accept compensation for publication. We welcome submissions from all members of the regulatory community and look forward to presenting diverse and competing points of view.

Please provide your comments and questions concerning Insights papers to slichtenberg@nrri.org.

* * *

The views expressed in these papers are the authors' and do not necessarily reflect those of NRRI or NARUC.