EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Cyber Security Industry Updates

2018 Edition

3002014707

Cyber Security Industry Updates

2018 Edition

3002014707

Technical Update, November 2018

EPRI Project Manager

E. Loveday

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

THE FOLLOWING ORGANIZATION, UNDER CONTRACT TO EPRI, PREPARED THIS REPORT:

OPUS Consulting Group

This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

Copyright © 2018 Electric Power Research Institute, Inc. All rights reserved.

ACKNOWLEDGMENTS

The following organization, under contract to the Electric Power Research Institute (EPRI), prepared this report:

OPUS Consulting Group
628 Island View Drive
Seal Beach, CA 90740

Principal Investigator
D. Holstein

This report describes research sponsored by EPRI.

This publication is a corporate document that should be cited in the literature in the following manner:

Cyber Security Industry Updates: 2018 Edition. EPRI, Palo Alto, CA: 2018. 3002014707.

ABSTRACT

The EPRI Cyber Security Program provides monthly updates to utilities on cyber security activities and events that are impacting the electric sector. The goal is to cover the activities of industry groups, government organizations, regulatory bodies, and research groups from around the world. This document provides highlights from these monthly updates.

Keywords
Cyber security
Industry updates
Newsletter

CONTENTS

LIST OF FIGURES

1
INTRODUCTION

With increased attention focused on securing the electric sector, numerous industry groups and public-private partnerships have been created to develop new security requirements and technologies. Additionally, working groups of organizations such as the North American Electric Reliability Corporation (NERC) and the Smart Grid Interoperability Panel (SGIP) will continue to have a direct impact on utility operations.

These groups are addressing specific needs in the industry; however, utility personnel are often unavailable to support all of these efforts. This lack of availability can lead to two key issues: First, utilities are less aware of changes that might impact the industry. Second, manufacturers of security products may lack the perspective of the electric sector.

EPRI's Industry Collaboration project support active participation in and contribution to collaborative efforts and interest groups such as the following:

- Smart Grid Interoperability Panel (SGIP) Smart Grid Security Committee (SGCC)
- CIGRE, the Council on Large Electric Systems
- European Network and Information Security Agency (ENISA)
- Department of Homeland Security Industrial Control Systems Joint Working Group (ICSJWG)
- European Commission
- International Electrotechnical Commission (IEC)

The EPRI Industry Collaboration project provided monthly email updates to the members to summarize industry cyber security activities and the status of EPRI's research projects. This report highlights articles from the monthly updates.

2
INDUSTRY UPDATE HIGHLIGHTS

Key Principles of the SDN Architecture (January Update)

Two colloquiums in 2017 highlighted the possibility of migrating operational applications to leverage cloud computing services in a software defined networking (SDN) environment. Hosted by CIGRE-Russia, SC D2 held their conference in August and CIGRE-Brazil hosted a joint group of study committees in December in Rio de Janeiro BR. Both conferences included papers and presentations describing prototype projects that leveraged cloud-based telecom services. The cost effectiveness of a secure migration strategy is very attractive to the power utility. The momentum is building to perform more prototype deployments to measure the benefits and identify the security issues that must be addressed.

Multiple IEEE projects are currently underway to address the security issues. IEEE Computer Society and the Communication Society sponsored most of these projects in early in 2017 and they have reached a critical mass of participation by highly-qualified subject matter experts (SMEs). These two societies have a broad charter that includes multiple critical infrastructure sectors. To tailor the requirements for the electric power sector, PSCC (Power System Communications and Cybersecurity) has formed a task force (P11) and both CIGRE SCs B5 and D2 have working groups (WGs) to develop technical brochures (TBs). CIGRE WG B5.66 will start in January 2018 to focus on protection and control systems (PACS). As soon as CIGRE technical committee approves the terms of reference (TOR), CIGRE WG D2.xx will also start in early 2018 to focus on governance requirements for the power utility to use cloud services – the issue is protection of sensitive data, including personal data. In addition to the IEEE work, both CIGRE WGs will build their recommendations using the newly published TB #698.

Early work in WG B5.66 has identified the key principles of the SDN architecture that must be addressed. With SDN, the applications can be network aware, as opposed to traditional networks where the network is application aware (or rather, application ambivalent):

- Traditional (i.e. non-SDN) applications only implicitly and indirectly describe their network requirements, typically involving several human processing steps, e.g., to negotiate if there are sufficient resources and policy controls to support the application.
- Traditional networks (e.g. the current Internet and its services like web browsing, media streaming) do not offer a (dynamic) way to express the full range of user requirements, for example throughput, delay, delay variation or availability. Packet headers can encode priority requests, but network providers typically do not trust user traffic markings. Therefore, some networks try to infer the user's requirements on their own (e.g. through traffic analysis), which may incur additional cost and sometimes leads to misclassification. SDN offers the ability for a user to fully specify its needs in the context of a trusted relationship that can be monetized.
- Traditional (i.e. non-SDN) networks do not expose information and network state to the applications using them. Using an SDN approach, SDN Applications can monitor network state and adapt accordingly. [1]

In an SDN architecture (see basic architecture in the Open Network Foundation (ONF) specification – TR 521)[1], the control plane is (1) logically centralized and (2) decoupled from the data plane. The SDN Controller summarizes the network state for applications and translates application requirements to low-level rules.

- This does not imply that the controller is physically centralized. For performance, scalability, and/or reliability reasons, the logically centralized SDN Controller can be distributed so that several physical controller instances cooperate to control the network and serve the applications.
- Control decisions are made on an up-to-date global view of the network state, rather than distributed in isolated behavior at each network hop. With SDN, the control plane acts as a single, logically centralized network operating system in terms of both scheduling and resolving resource conflicts, as well as abstracting away low-level device details, e.g., electrical vs. optical transmission.

The SDN Controller has complete control of the SDN data paths, subject to the limit of their capabilities, and thus does not have to compete/contend with other control plane elements, which simplifies scheduling and resource allocation. This allows networks to run with complex and precise policies with greater network resource utilization and quality of service guarantees. This occurs through a well-understood common information model (e.g. as the one defined by OpenFlow). [1]

Security for EPU Data Handling Subsystem (February Update)

Today's Electric Power Utilities (EPUs) realize the necessity of protecting their valuable and sensitive information to mitigate attempts to steal the information and use it to harm the reputation of the EPU, or to interfere with, disrupt, or disable mission critical functions. Given the volatile threat landscape and rapidly evolving protective solutions, EPU risk assessment teams are challenged to find the best security solution to protect these data. One approach is to provide a cryptography-based protection mechanism as close to the data creation source as possible. Protection enabled by role-based access control (RBAC) and attribute-based access control (ABAC) at the data object level is the key. The logical location for this protection mechanism is the data handling subsystem, which might be a separate component or an embedded component in any intelligent electronic device (IED) or intelligent network device (IND).

Consider a protection and control (P&C) IED, such as a modern multi-function protective relay. The data handling subsystem includes two parts: at least one P&C data management subsystem, and possibly none or multiple crypto content management subsystems. An instance of the crypto content management subsystem is responsible for managing the cryptographic keys containing access and use privileges and for performing the encryption and decryption functions at the object level. The crypto management subsystem uses the data management objects for this task. Any solutions offered to determine if the IEDs and INDs provide the capability to process RBAC and ABAC control parameters should be thoroughly evaluated. If the solutions provide the

[1] www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/SDN-architecture-overview-1.0.pdf

capability, the implementation should also provide the interoperability that conforms to IEC 62351.

CrashOverride Attack Demonstration Video (February Update)

This year's Winter Advisory was kicked off with a looped video that was created as part of an internal team exercise. The video was meant to highlight some part of EPRI's work in 2017. The video created by Ben Sooter highlighted some of the reverse engineering work that was performed on the CrashOverride / Industroyer malware that was uncovered during the 2016 attack on the Ukraine power grid. A copy of the video can be found on the EPRI Member Center.[2] The video moves fast, as they were supposed to be under three minutes long.

The video starts off zipping through several of the initial reports by Dragos[3] and ESET[4] reviewing the attack and the malware discovered from it. The identified hashes and what they were reported to be used for were highlighted. Many of the samples were available on VirusTotal[5] if the user had an enterprise account. That wasn't available, so additional digging was done before samples were discovered on a Chinese malware repository a few days after the reports were published.

From there the video starts to move through some static analysis of the launcher in IDA Pro.[6] The launcher was used to kick off several of the OT focused payloads and also executed a wiper module to further frustrate recovery efforts. It was reported that the function calls were all called 'Crash' in the malware. Crash was searched for, and the first function discovered is the function that calls one of the two wiper modules that are designed to brick the computer after the malware has executed. The second function identified with the 'Crash' string is the main function that runs the OT payloads that attacks relays using IEC 60870-5-101 or IEC 60870-5-104. Of interest in this part are several variables defined for a specific System Time. This was because the malware was only designed to run the payload on 17 December 2016 22:27 (UTC). The times shown are in epoch time, or time since 1 January 1970 at 00:00 UTC.

```
19  SystemTime = 0i64;
20  SystemTime.wMilliseconds = 0;
21  *(_DWORD *)&SystemTime.wYear = 788448;
22  *(_DWORD *)&SystemTime.wDay = 1441809;
23  *(_DWORD *)&SystemTime.wMinute = 27;
```

Figure 2-1
Variables defined for a specific System Time

---

[2] https://membercenter.epri.com/Programs/072143/pages/eventdetails.aspx?eventID=8654494D-6D8C-4E38-9ABC-6F2B083F2979&perror=4

[3] https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

[4] https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

[5] https://www.virustotal.com/#/home/upload

[6] https://www.hex-rays.com/products/ida/

Next the 104 attack payload was analyzed. The insertion point into the DLL file was the 'Crash' function so that is identified initially. Next part of the 'range' function is shown, which is one of four different attack modes that the 104 payload has. The 'range' function was created to enumerate active 104 information object addresses (IOA). Not highlighted in this video, but discovered during dynamic analysis of the malware the range function only correctly enumerates IOAs on ABB relays. A GE relay that was targeted did not behave as the authors had intended.

At this point the video moves to dynamic analysis and sees if the launcher will run and execute the 104 payload. A configuration file is visible in this shot that while not covered by the video, is well documented in the ESET[7] report. The file is attempted to be run, but does nothing. Which makes sense because it's not December 17th, 2016. Also highlighted in the video there is some service stomping that the malware attempts to do, it was not successful either because of the patch level of that particular VM. The video now launches into a whirlwind of activity as the debugger is used to better understand program execution and memory hooks.

Ultimately, after dynamic analysis, it was decided the easiest way to successfully launch the payloads would be to attempt to execute the payload function when the time check function fails and attempts to execute an exit function. The launcher module was unpacked into assembly with Hiew.[8] The binary was edited to change the memory address that is executed after the time check fails to be the address of the beginning of the payload function. The binary was repacked and the execution of the launcher module is now attempted again and we can see evidence of its success.

The video cheekily closes with the question of whether or not the modified code really works, as a target is identified on Shodan[9] that appears to have internet facing IEC 104. The payload pretends to be executed against the target and dramatically shows the power being shut off.

The Impact of Explicit Consent on Protection of Personal Data (March Update)

The new EU General Data Protection Regulation (GDPR)[10] aims to protect all European Union citizens from privacy and data breaches, and will apply to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location. The conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it. [2] However, the inclusion of the word "explicit" has much greater ramifications.

"Explicit" in the data protection world generally means "specific". In other words, the consent must specify the types of data, the specific purposes for which they may be used and/or the countries to which they may be disclosed. If it's going to be harder to rely on consent, what about the alternative avenues enabling utilities to avoid having to collect consent? As Nick

---

[7] https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

[8] http://www.hiew.ru/

[9] https://www.shodan.io/

[10] https://eugdpr.org/the-regulation/

Graham notes, "...the alternative avenues are being narrowed or closed off under the new regulation." [3]

Because utilities use personal data for access control and use privileges, and collection of smart metering data, explicit consent from the person affected is required. For example, the current practice is for the utility to avoid collecting consent where processing is necessary for their (or the relevant recipients') "legitimate interests". Under the regulation, however, the "legitimate interests" avenue is being substantially narrowed. Within the utility, the responsible organization will only be able to rely on this in connection with its own "legitimate interests" (not those of third parties). Furthermore, the new transparency rules will require responsible organizations to notify individuals of any legitimate interests on which it is relying.

To comply with this regulation, the utility will have to be specific in its relevant policies, procedures, and organizational directives and of the requirements to collect and maintain "explicit consent" to use personal data. If the operating organizations rely on "legitimate interest" they will have to specifically disclose those interests in their enabling procedures. These enabling procedures will have to be totally transparent to the individuals affected. [2]

DERS Face Increasing Cybersecurity Challenges (March Update)

In an excerpt from their T&D World online magazine article, Candace Suh-Lee and Galen Rasche reported on the rapid, disruptive changes happening in electric grids around the world. In many states and countries, initiatives are underway to integrate small renewable generation into the distribution grid to meet local demand for electricity while reducing the dependency on large central generation facilities and long-distance transmission.

This integration requires new technologies, connectivity and intelligence — all of which increase cybersecurity risks. Through its collaborative, independent research and development, the Electric Power Research Institute (EPRI) is examining the risks and exploring solutions. Connectivity and security standards, device authentication, protection of data in transit, and a basic modeling and benchmarking of risk can help utilities to plot the way to a cyber secure, integrated grid.

General awareness of these risks is the first step to mitigation. The following list suggests some study areas where the industry could benefit from further research and development:

- Multiparty grid risk model in which loosely associated multiple parties are participating in the electricity market
- Framework for collaborative security management, which enables loosely associated multiple parties to work collaboratively to secure common resources
- Cybersecurity guidelines for integration for electric utilities, DER manufacturers, DER integrators and DER managers
- Lightweight encryption schemes for embedded systems with limited system resources
- Simple certificate or cryptographic key management schemes for digital certificate or key management
- Cloud security for cyber-physical systems guidelines as well as for cloud-based services in cyber-physical systems

- Grid impact studies and simulation with cyberattack scenarios, collaborative studies among electric engineers, communications specialists and cybersecurity professionals.

EPRI is working on many of these areas through collaborative research with utilities, industry, government entities and the U.S. Department of Energy, and national laboratories. EPRI's new research and development project, ICT and Security Architecture for DER Integration[11], addresses some of the most pressing cybersecurity concerns related to DER integration from the utility's perspective. [4]

The Future of ENISA (April Update)

"The distinction between internal security and defense becomes increasingly blurred. From a defense perspective cyberspace has become a fifth domain of warfare equally as critical as military operations occupying land, sea, air, and space." --Elżbieta Bieńkowska, European Union Commissioner[12]

The European Union's efforts to increase cyber resilience efforts have been made through these concrete actions:

- A proposal to transform the European Union Agency for Network and Information Security (ENISA) into a EU cybersecurity agency able to prevent and respond to cyber-attacks in a more coordinated way. The agency will be able to conduct pan-European cybersecurity exercises and will ensure a better sharing of intelligence.
- Promoting the creation of a true single cybersecurity market with an EU-wide framework for cybersecurity certification.
- Proposing a blueprint for faster response in a more coordinated way at the EU level during large scale cybersecurity incidents.
- Proposing to develop a network of cybersecurity competence centers with a European Cybersecurity research and competence center. Its role will be to roll out the technologies and cyber-capacities needed to detect and counter cyber-attacks.
- Establishing mainstream cybersecurity principles in all the key strategic sectors. Cybersecurity is a cross sectoral issue. And a weakness in one sector can have an important impact on others and the rest of the economy. [5]

A Cyber Security Metrics Tool for Utilities (April Update)

In an excerpt from his article in CIO Review[13] online magazine, Mark McGranaghan explained the security metrics methodology and framework for security metrics created in collaboration between EPRI and several industry associations and councils, including the Edison Electric Institute, the American Public Power Association, the National Rural Electric Cooperative Association, and the SANS Institute.

---

[11] https://www.epri.com/#/pages/product/3002009694/

[12] https://www.automation.com/automation-news/article/industrial-cybersecurity-international-defense-inside-siemens-cybersecurity-charter-of-trust

[13] https://utilities.cioreview.com/cxoinsight/a-cyber-security-metrics-tool-for-utilities-nid-23603-cid-41.html

In 2015 the collaboration created a security metrics methodology and a framework for creating security metrics. In 2016 the group revised the methodology and developed specific metrics[14] for utilities to use as a starting point in evaluating their own posture and path forward. [5]

A Practical Methodology for Cyber Security Metrics Development

EPRI's research approach incorporated five common-sense rules to our metrics development:

1. Utility cyber security metrics must be based on quantitative and repeatable data,
2. Metrics must be independent of compliance to mandatory standards,
3. Metrics must allow for tailoring across the utility's business units, functions, and ownership structures,
4. Metrics must take into account difference between IT and OT architectures,
5. Metrics must be able to clearly communicate the utility's state of cyber security to different stakeholders.

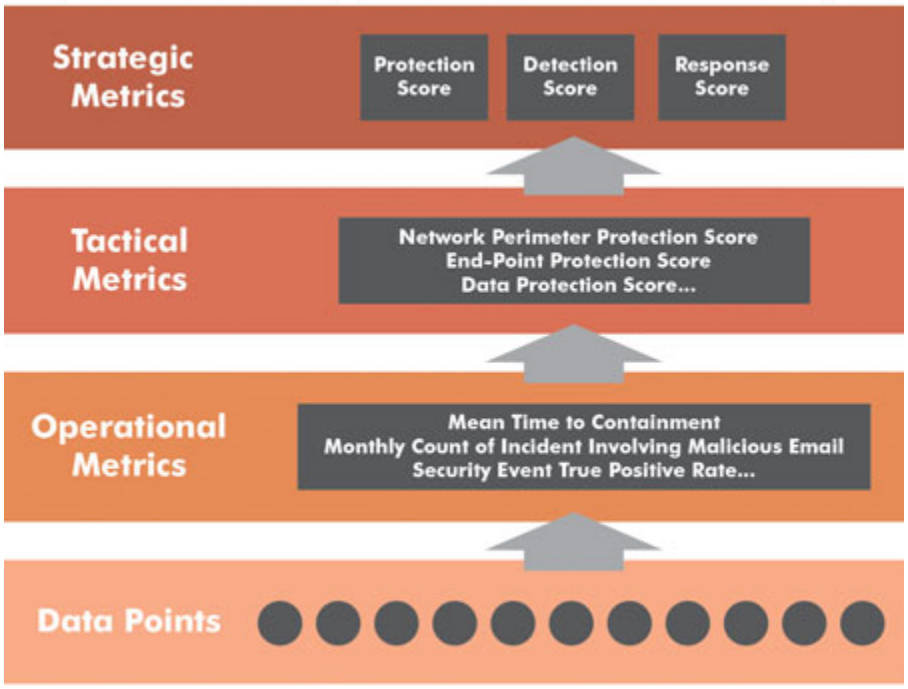

Figure 2-2
Metrics pyramid

EPRI's approach, shown in the metrics "pyramid" organizes data points, then rolls them up and assigns a weight of importance to either an operational, tactical, or strategic metric. The resulting tiers of data will help a broad range of utility stakeholders gain improved knowledge about cyber security postures and thus inform decision-making about policies, investments, and action plans...Operational metrics measure real-time, day-to-day operations such as logs, rule sets, and signatures. Tactical metrics address programmatic health and progress in the organization.

[14] https://www.epri.com/#/pages/product/3002010426/

Strategic metrics measure corporate risk and alignment of the metrics to the direction of the business.

As a relatively new field, security metrics is not as mature or robust as metrics in finance, reliability operations, or safety. However, EPRI's collaborative research and practical methodology offers an optimal, standardized and complementary approach utilities can use to evaluate their own postures and resulting action plans. [6]

Metrics and Key Performance Indicators for Strategic Planning (May Update)

CIGRE WG D2.46 is a new working group with the charter to develop a methodology to include cybersecurity in electric power utilities 10 and 20-year strategic plans. WG D2.46 is using Debra Herrmann's "Complete Guide to Security and Privacy Metrics" as the primary resource for this clause [7]. Collection, analysis, and actionable decisions derived from metrics and key performance indicators (KPIs) is recognized as a continuous process. When properly executed, executive decision makers can make informed decisions to improve security processes, operating procedures, and resource allocations to improve their cybersecurity posture. Aggregation of metrics to provide a coherent picture of the cybersecurity situation is critical for a well-informed decision making.

To develop a coherent picture of the security situation, organizational directives should require all responsible organizational units to execute the following steps:

1. Define what information is going to be collected.
2. Define why this information is being collected and how it will be used.
3. Define how the information will be collected, the constraints and controls on the collection process.
4. Define the time interval and frequency with which the information is to be collected.
5. Identify the sources(s) from which the information will be collected.
6. Define how the information collected will be preserved to prevent accidental or intentional alteration, deletion, addition, other tampering, or loss.
7. Define how the information will be analyzed and interpreted. [7]

Aggregating the collection information for the decision maker requires a clear understanding of the limitation for using individual or aggregate measurements. The most effective way to communicate the security posture is a KPI color-coded description: GREEN – situation is well within the bounds of acceptable risk, YELLOW – situation is marginal and requires more frequent monitoring to determine impact on mission-critical operations, and RED – situation exceeds the bounds of acceptable risk and requires immediate attention. YELLOW and RED assessments should include a recommendation for a resourced action plan.

Framework for an Electric Power Utility Software Defined Network Data Operations Center (June Update)

The proliferation of software defined networks (SDN) and network function virtualization (NFV) solutions provide the means for an electric power utility (EPU) to reinvent their data center. To future-proof themselves, EPUs should benchmark the degree to which different vendor products are open as well as evaluate the performance, security, and resilience advantages associated with

SDN/NFV solutions. Enabling their SDN data center networks to interface with non-SDN systems and to comply with local laws and regulations is critical. The basic concept is shown in the figure below, where XaaS is the requested service; e.g., software as a service (SaaS).

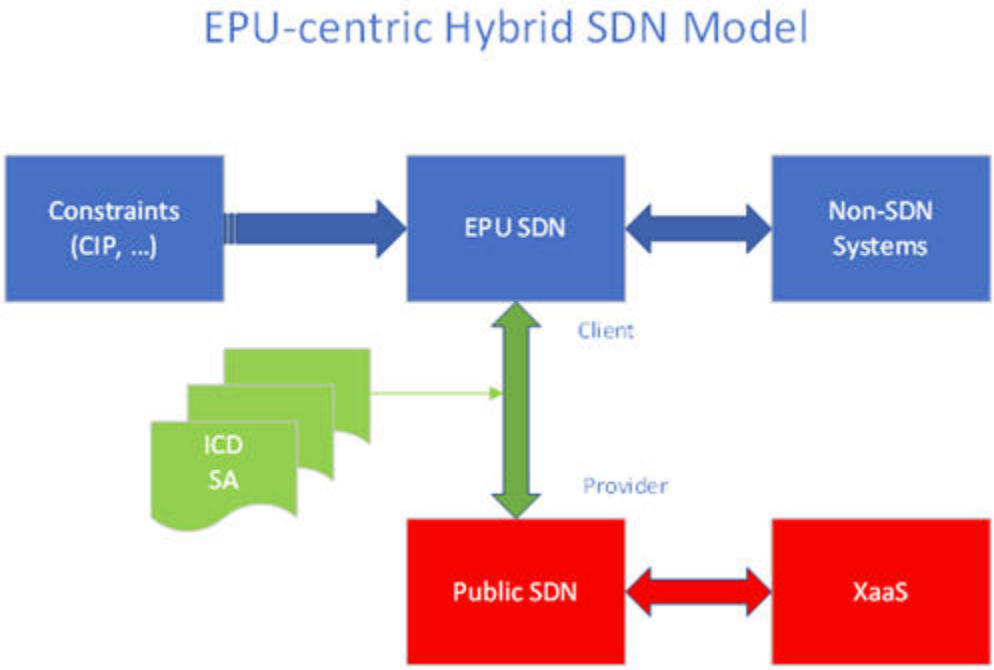

Figure 2-3
EPU-centric Hybrid SDN Model

Open Network Foundation (ONF) defined in TR 521[15] is the basic architecture for the SDN/NFV data center. This architecture can be tailored to satisfy the requirements for an EPU SDN data operations center.

IEEE P1915.1[16] (Security in Virtualized Environments) is addressing the security required, P1916.1[17] (Performance for Virtualized Environments) is addressing the performance required, and P1917.1[18] (Reliability for Virtualized Environments) is addressing the reliability required. IEEE P1930.1[19] (SDN-based Middleware for Control and Management of Networks) defines the middleware needed to support the SDN controller. These IEEE projects and the findings of CIGRE WG D2.43[20] (Enabling Software-defined Networking for EPU Telecom Applications) provide the information needed to tailor the requirements for an EPU SDN data operations center.

---

[15] https://3vf60mmveq1g8vzn48q2o71a-wpengine.netdna-ssl.com/wp-content/uploads/2014/10/TR-521_SDN_Architecture_issue_1.1.pdf

[16] https://standards.ieee.org/project/1915_1.html

[17] https://standards.ieee.org/project/1916_1.html

[18] https://standards.ieee.org/project/1917_1.html

[19] https://standards.ieee.org/project/1930_1.html

[20] http://d2.cigre.org/WG-Area/D2.43-Enabling-software-defined-networking-for-EPU-telecom-applications

A new working group has been proposed to CIGRE Study Committee D2 "Information Technology and Security." If approved by SC D2 in August 2018, and approved by the Technical Committee, the work will start in the second quarter of 2019 and be completed by December 2022. The tasks are:

1. Survey the EPU to identify their requirements and concerns for the development of an EPU SDN data operations center. The results of the survey should help the working group prioritize the requirements and identify the challenges of interest to their target audience.
2. Describe the capabilities required for an EPU to design, develop, and operate a SDN data operations center. The EPU SDN data operations center must provide the capability to interface with non-SDN systems and comply with local laws and regulations. As a private cloud solution it should have the capability to act as a client using public cloud services. The EPU's SDN should include components with full SDN capabilities and network components with reduced capabilities. It is the responsibility of the EPU SDN controller and middleware to recognize the difference in these capabilities.

Describe the benefits and challenges that must be addressed to design, develop, test, and operate a SDN operations center, including identifying the major cost drivers and relate those costs to people skills, processes, and technology and offer recommended best practices to address these challenges.

IEEE Global Initiative for Ethical Considerations (July Update)

The IEEE Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems (AI/AS) was launched in April 2016 to move beyond the paranoia and the uncritical admiration regarding autonomous and intelligent technologies and to illustrate that aligning technology development and use with ethical values would help advance innovation while diminishing fear in the process. The goal of the IEEE Global Initiative is to incorporate ethical aspects of human well-being that may not automatically be considered in the current design and manufacture of AI/AS technologies, and to reframe the notion of success so human progress can include the intentional prioritization of individual, community, and societal ethical values.

Below are titles and descriptions for each of these approved IEEE Standards Projects:

- **IEEE P7000: Model Process for Addressing Ethical Concerns During System Design** outlines an approach for identifying and analyzing potential ethical issues in a system or software program from the onset of the effort. The values-based system design methods address ethical considerations at each stage of development to help avoid negative unintended consequences while increasing innovation.
- **IEEE P7001: Transparency of Autonomous Systems** provides a standard for developing autonomous technologies that can assess their own actions and help users understand why a technology makes certain decisions in different situations. The project also offers ways to provide transparency and accountability for a system to help guide and improve it, such as incorporating an event data recorder in a self-driving car or accessing data from a device's sensors.
- **IEEE P7002: Data Privacy Process** specifies how to manage privacy issues for systems or software that collect personal data. It will do so by defining requirements that cover corporate data collection policies and quality assurance. It also includes a use case and data

model for organizations developing applications involving personal information. The standard will help designers by providing ways to identify and measure privacy controls in their systems utilizing privacy impact assessments.

- **IEEE P7003: Algorithmic Bias Considerations** provides developers of algorithms for autonomous or intelligent systems with protocols to avoid negative bias in their code. Bias could include the use of subjective or incorrect interpretations of data like mistaking correlation with causation. The project offers specific steps to take for eliminating issues of negative bias in the creation of algorithms. The standard will also include benchmarking procedures and criteria for selecting validation data sets, establishing and communicating the application boundaries for which the algorithm has been designed, and guarding against unintended consequences.
- **IEEE P7004: Standard on Child and Student Data Governance** provides processes and certifications for transparency and accountability for educational institutions that handle data meant to ensure the safety of students. The standard defines how to access, collect, share, and remove data related to children and students in any educational or institutional setting where their information will be access, stored, or shared.
- **IEEE P7005: Standard on Employer Data Governance** provides guidelines and certifications on storing, protecting, and using employee data in an ethical and transparent way. The project recommends tools and services that help employees make informed decisions with their personal information. The standard will help provide clarity and recommendations both for how employees can share their information in a safe and trusted environment as well as how employers can align with employees in this process while still utilizing information needed for regular work flows.
- **IEEE P7006: Standard on Personal Data AI Agent Working Group** addresses concerns raised about machines making decisions without human input. This standard hopes to educate government and industry on why it is best to put mechanisms into place to enable the design of systems that will mitigate the ethical concerns when AI systems can organize and share personal information on their own. Designed as a tool to allow any individual to essentially create their own personal "terms and conditions" for their data, the AI Agent will provide a technological tool for individuals to manage and control their identity in the digital and virtual world.
- **IEEE P7007: Ontological Standard for Ethically Driven Robotics and Automation Systems** establishes a set of ontologies with different abstraction levels that contain concepts, definitions and axioms that are necessary to establish ethically driven methodologies for the design of robots and automation systems.
- **IEEE P7008: Standard for Ethically Driven Nudging for Robotic, Intelligent and Autonomous Systems** establishes a delineation of typical nudges (currently in use or that could be created) that contains concepts, functions and benefits necessary to establish and ensure ethically driven methodologies for the design of the robotic, intelligent and autonomous systems that incorporate them. "Nudges" as exhibited by robotic, intelligent or autonomous systems are defined as overt or hidden suggestions or manipulations designed to influence the behavior or emotions of a user.
- **IEEE P7009: Standard for Fail-Safe Design of Autonomous and Semi-Autonomous Systems** establishes a practical, technical baseline of specific methodologies and tools for the development, implementation, and use of effective fail-safe mechanisms in autonomous and

semi-autonomous systems. The standard includes (but is not limited to): clear procedures for measuring, testing, and certifying a system's ability to fail safely on a scale from weak to strong, and instructions for improvement in the case of unsatisfactory performance. The standard serves as the basis for developers, as well as users and regulators, to design fail-safe mechanisms in a robust, transparent, and accountable manner.

- **IEEE P7010: Wellbeing Metrics Standard for Ethical Artificial Intelligence and Autonomous Systems** will establish well-being metrics relating to human factors directly affected by intelligent and autonomous systems and establish a baseline for the types of objective and subjective data these systems should analyze and include (in their programming and functioning) to proactively increase human well-being. [8]

Network Function Virtualization in the European Telecommunications Standard Institute (August Update)

Founded in November 2012 by seven of the world's leading telecoms network operators, the Industry Specification Group for Network Function Virtualization (ISG NFV) became the home of the Industry Specification Group for NFV.

Five years and over 100 publications later, the ISG NFV community has evolved through several phases; its publications have moved from pre-standardization studies to detailed specifications (see Release 2[21] and Release 3[22]) and the early Proof of Concepts (PoCs) efforts have evolved and led to interoperability events (Plug tests). This large community (300+ companies including 38 of the world's major service providers) is still working intensely to develop the required standards for NFV as well as sharing their experiences of NFV implementation and testing.

Building the Software-Defined Network

Modern telecoms networks contain an ever-increasing variety of proprietary hardware. The launch of new services often demands network reconfiguration and on-site installation of new equipment which in turn requires additional floor space, power, and trained maintenance staff.

The innovation cycles accelerate and require greater flexibility and dynamism than hardware-based appliances allow. Hard-wired networks with single functions boxes are tedious to maintain, slow to evolve, and prevent service providers from offering dynamic services.

In the same way that applications are supported by dynamically configurable and fully automated cloud environments, virtualized network functions allow networks to be agile and capable to respond automatically to the needs of the traffic and services running over it.

Key enabling technologies for this vision include Software Defined Networking (SDN) and NFV. SDN and NFV are complementary but increasingly co-dependent for the benefits of software-defined networking to be fully realized. [9]

---

[21] https://docbox.etsi.org/ISG/NFV/Open/Other/NFV(18)000241_NFV_Release_2_Description_v17.pdf

[22] https://docbox.etsi.org/ISG/NFV/Open/Other/NFV(18)000240_NFV_Release_3_Definition_v0_11_0.pdf

Cyber Intrusion Detection and Prevention for Power Delivery Systems – Research and Testing of Binary Armor from Sierra Nevada Corporation (August Update)

In an excerpt from his publicly available abstract[23], Ralph King discussed testing the configuration, placement, usage, and gaps involved with deploying cyber intrusion detection/prevention (IDS/IPS) solutions for power delivery systems.

Thirty solutions were considered for testing based upon criteria such as technical capabilities, compatibility in an industrial control environment, and EPRI member utility specific requests. Of the thirty solutions, six solutions were tested over a two-year period in the Cyber Security Research Lab (CSRL).

The testing process included the following phases:

Technical Design

- Deployment of the IDS/IPS solutions in the CSRL
- Development of use case scenarios for cyber-attacks
- Design of substation testbed design
- Determination of the most effective configuration and placement for the IDS/IPS solutions
- Testing
- Implementation of the substation testbed based upon the approved design
- Use case testing for cyber attacks
- Additional use cases were identified during testing that exercised the solutions against sophisticated cyber attacks
- Technology transfer and reporting
- Delivered the design recommendations and testing results to EPRI utility members through the research report, various meetings, web conferences, and workshops.
- Report deliverable reference: Implementing Intrusion Detection / Prevention Systems for Power Delivery Systems: Phase 2. EPRI, Palo Alto, CA: 2017. (Product ID: 3002010595).[24]
- EPRI Power Delivery and Utilization Advisory Meeting for the cyber security program
- EPRI Cyber Security Technology Transfer Workshop

Binary Armor Results

A solution tested in the CSRL in 2017 was Binary Armor from the Sierra Nevada Corporation. The testing results indicate the Binary Armor solution is an effective IDS/IPS solution for utility substations and may be implemented as part of the cyber security defense infrastructure for power delivery systems. The detection rate and block rate of attacks for Binary Armor was 100% during the 2017 testing period and an updated Binary Armor solution has been deployed in the EPRI CSRL and will be utilized in new testing activities during 2018-2020 as part of the "Intrusion Detection Systems/Intrusion Prevention Systems Solutions Analysis and Testing for

[23] https://www.epri.com/#/pages/product/3002014248/

[24] https://www.epri.com/#/pages/product/3002010595/

ICS Environments" project (Product ID: 3002012235).[25] The updated version of Binary Armor is in the process of undergoing US Department of Defense testing and evaluation as a cyber security tool for use on operation technology networks. The evaluation will conclude with placement on the Defense Information Systems Agency (DISA) Approved Products List (APL) and National Information Assurance Partnership (NIAP) Product Compliant List (PCL). [10]

Federated Security Operations Center for Smaller Utilities (September Update)

The cybersecurity threat landscape is rapidly evolving. As discussed in several CIGRE technical brochures including the emerging work in WG D2.46 (Cybersecurity: Future Threats and Impact on Electric Power Utility Organizations and Operations), electric power utilities need an Integrated Security Operations Center (ISOC) to provide a center of excellence for cybersecurity management.

Standing up and operating an ISOC requires significant resources for training, process management, and technical controls. Such a resource commitment is not affordable for smaller utilities. Thus, a Federated Security Operations Center (FSOC) using cloud-based services may be economically feasible. The basic FSOC concept is to provide a cloud-based arrangement for multiple smaller utilities to use federated management schemas that let subscribers use the same information for access control, use control, timely reporting of events, etc. For an FSOC to be effective, protection of sensitive data and data sharing are trust issues that need to be addressed.

A new working group has been proposed to CIGRE Study Committee D2: "Information Technology and Security." If approved by SC D2 in August 2018, and approved by the Technical Committee, the work will start in the second quarter of 2019 and be completed by December 2022. The tasks involved are:

1. To review existing standards, CIGRE technical brochures and open source documentation to define the FSOC architecture and applicable cloud-based services (xx-as-a-service). Federated architecture is expected to deliver high flexibility and agility among independently cooperating electric power utilities, and at the same time reduce complexity significantly.
2. Estimate the impact on small utility cybersecurity policies, procedures, and organizational directives needed for effective oversight management of FSOC operations.

Associated with each impact, recommend solutions to improve the security posture of small utility operations. Solutions need to protect sensitive data and data sharing.

Israel's New Cybersecurity Law (October Update)

Israel's government wants to forge a new type of relationship with the private sector to combat cyber threats. In the opinion of Cyber Week in Review author Deborah Housen-Couriel, how it will do so might prove controversial. The draft represents years of consultation and debate on Israel's approach to cybersecurity. It combines elements of existing cybersecurity legislation and policy with several significant innovations, including some controversial broadening of powers of the lead organization, the National Cyber Directorate (NCD).[26]

---

[25] https://www.epri.com/#/pages/product/3002012235/

[26] https://www.gov.il/en/Departments/israel_national_cyber_directorate

Under the proposed law, the NCD's position will be strengthened by a bolstering of its leadership role in assessing national cyber risks, planning for national preparedness and resilience, and providing guidance to government agencies and the Israeli private sector. Under the proposed law, the NCD is specifically charged with enhanced authority to issue national guidance on cybersecurity matters, even within the scope of other regulators in such areas as finance, health, transport, energy, and communications.

Two fundamental principles are specified: (a) the need to develop an innovative approach to cybersecurity by initiating an unprecedented type of cooperation between government and the private sector; and (b) the need to devote national efforts to improve cyber preparedness and mitigate the fallout from incidents. [11] The NCD is only responsible for assessments, the response to attack is the responsibility of the military or security agencies.

NCD is established as the primary national cybersecurity regulator and maintains its direct accountability to the prime minister. Among its core responsibilities, the NCD will deploy two operative bodies: (1) a center for countering cyber threats on an ongoing basis (the national computer emergency response team, CERT-IL, will continue to serve this function) and (2) a detection and verification hub for early warning and attack mitigation. The hub will facilitate information sharing among specified governmental and private sector actors, essentially creating a national database of threat indicators and other data. The proposed database has already sparked controversy in the Israeli media because of its inevitable collection and processing of large amounts of private and corporate data.

The proposed law introduces a new data classification and protection regime that applies to the information gathered by the NCD itself or shared with it, categorized by risks entailed by its exposure. Data of techno-security value (i.e., indicators of a hostile cyber event; unidentifiable data (that does not reasonably allow for the identification of an individual or an organization); and protected data (which draws it status from Israel's data privacy and other domestic laws) are subject to different processing safeguards by the NCD and those sharing such information. The sufficiency of these safeguards is an additional point of public critique of the bill. [11]

ISA99's View of Common Roles (November Update)

The International Society for Automation (ISA) has entrusted the ISA99 committee to work closely with IEC TC57 WG10 (Power System IED Communication and Associated Data Models) on the development of IEC 62443, a multi-part cybersecurity certificate program and standard. Publications of 62443 under the ISA label sometimes contain minor differences with the publication of 62443 under the IEC label. However, the objective of the two publications is the same.

ISA99 has long been concerned with the use of security levels (SLs) and maturity levels (MLs). Currently they have developed a concept called protection level (PL) that conflates SL and ML in a two-dimensional table. They have also addressed the application of PLs to the roles played by various stakeholders. One aspect of the human element of a cybersecurity management system is addressed through the definition and consistent application of a set of common role descriptions. These descriptions define the specific accountability and responsibilities of each role, as well as the relationships and dependencies between roles. [12] The organizational responsibilities associated with these stakeholders is shown in the following figure.

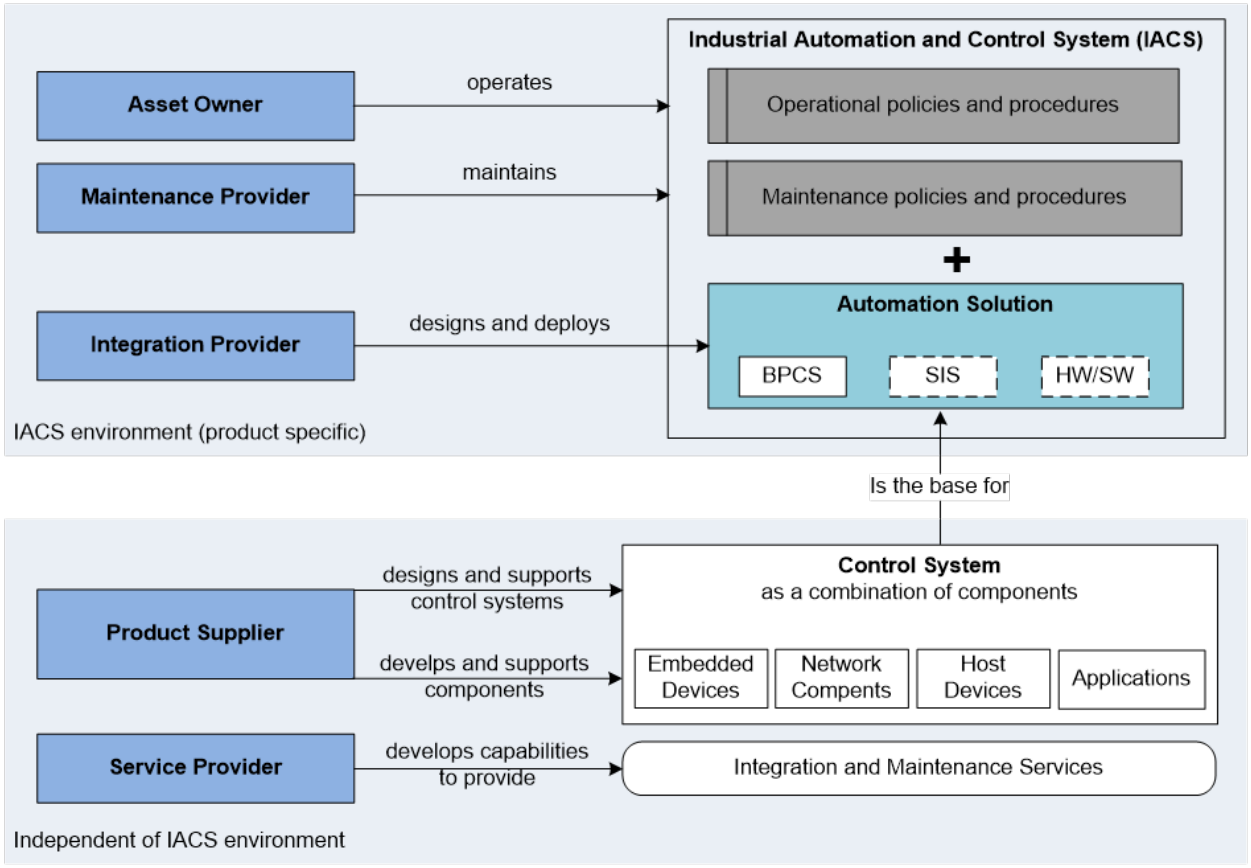

Figure 2-4
IACS Stakeholders

ISA99 defines these roles as follows:

Product Supplier – The principal responsibility of the product supplier is to design and provide the components that are used to assemble the industrial automation control system (IACS) within their scope of supply.

Integration Provider – It is common for an automation solution to be designed and configured by an independent or external system integrator, according to specifications and requirements provided by the asset owner and meeting product supplier requirements

Asset Owner – This is the person or organization that has primary accountability for the IACS performance including safety and security. Responsibilities include assessment of risk and to ensure a commensurate design, operation, and maintenance of the IACS within all requirements.

Maintenance Provider – This is the person or organization that is responsible for the health of the system under consideration. This may or may not be the same entity as the asset owner. For example, the asset owner may be different in situations involving some types of joint ventures or similar business structures. In addition, there are several situations where aspect(s) of maintenance are performed as part of maintenance contracts.

System Operator – This is the person or organization that is responsible for the operation of the system under consideration. This may or may not be the same entity as the asset owner. For example, the asset owner may be different in situations involving some types of joint ventures or similar business structures. However, in this standard, except if otherwise specified, the asset owner is expected to be also the asset operator.

Service Provider – Ensuring the security of an IACS also requires services throughout the life cycle, including design, consulting, operation, maintenance and system updates. [12]

Mapping these definitions onto electric power utility operations is relatively straight forward. There are only some differences in how the basic process control system (BPCS) and safety instrumented system (SIS) are described.

3
REFERENCES

1. Bailey, Stuart. "SDN Architecture Overview Version 1.0." *Open Networking Foundation*, 12 Dec. 2013, www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/SDN-architecture-overview-1.0.pdf
2. *"GDPR Key Changes."* www.eugdpr.org/the-regulation/
3. Graham, Nick. *"Explicit Consent Under the New Data Protection Regulation."* Lexology, 16 May 2012, www.lexology.com/library/detail.aspx?g=444da6e8-8649-4579-8fe4-9b3a637015b4
4. Suh-Lee, Candace and Galen Rasche. *"DERS Face Increasing Cybersecurity Challenges."* T&D World, 2 Jan 2018, www.tdworld.com/distribution/ders-face-increasing-cybersecurity-challenges
5. Lydon, Bill. *"Industrial Cybersecurity & International Defense – Inside Siemens' Cybersecurity Charter of Trust."* Automation, 17 Apr. 2018, www.automation.com/automation-news/article/industrial-cybersecurity-international-defense-inside-siemens-cybersecurity-charter-of-trust
6. McGranaghan, Mark. *"A Cyber Security Metrics Tool for Utilities."* CIO Review, 2018, www.utilities.cioreview.com/cxoinsight/a-cyber-security-metrics-tool-for-utilities-nid-23603-cid-41.html
7. Herrmann, Debra S. *Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI*. 1st ed., Auerbach Publications, 2007.
8. *"Ethically Aligned Design,"* Version 2 (EADv2). IEEE Standards Association. www.ethicsinaction.ieee.org/
9. *"Network Functions Virtualisation."* www.etsi.org/technologies-clusters/technologies/nfv
10. King, Ralph. "Cyber Intrusion Detection and Prevention for Power Delivery Systems." EPRI Product Abstract, 14 Aug 2018, www.epri.com/#/pages/product/3002014248/
11. Housen-Couriel, Deborah. *"A Look at Israel's New Draft Cybersecurity Law."* Cyber Week in Review, 2 July, 2018, www.cfr.org/blog/look-israels-new-draft-cybersecurity-law
12. *"ISA99, Industrial Automation and Control Systems Security."* www.isa.org/isa99/

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI members represent 90% of the electric utility revenue in the United States with international participation in 35 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together…Shaping the Future of Electricity

3002014707

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com