Cybersecurity Based on IEC 62351 and IEC 62443 for IEC 61850 Systems

David Dolezilek, Dennis Gammel, and William Fernandes
Schweitzer Engineering Laboratories, Inc.

Presented at the
15th International Conference on Developments in Power System Protection
Liverpool, United Kingdom
March 9–12, 2020

CYBERSECURITY BASED ON IEC 62351 AND IEC 62443 FOR IEC 61850 SYSTEMS

David Dolezilek[1]*, Dennis Gammel[1], William Fernandes[1]

[1]Schweitzer Engineering Laboratories, Inc., Pullman, Washington, USA
**dave_dolezilek@selinc.com*

Keywords: CYBERSECURITY, IEC 62351, IEC 62443, ISA99, IEEE 1686.

Abstract

The word “cyber,” originating from the Greek word meaning “skilled steering or guidance,” has taken on the modern meaning of using digital communications within and among intelligent devices to perform information gathering and commanded control. Information technology (IT) systems include networked communications among computers, business systems, and the internet. Operational technology (OT) systems include networked communications among industrial control system (ICS) devices performing automatic safety, operational, and monitoring processes.

In this paper, established ICS methods and standards are used to design defense-in-depth cybersecurity methods for digital communications within an energy control system (ECS) communications network. The ECS communications architecture is a mission-critical ICS and is divided into multiple levels with unique requirements and features from the process up through the station and finally to the control center. Using these levels, it is possible to identify interacting cyber defense technologies, the levels at which they should be deployed, and which devices they belong to (IEC 62443 Part 3) instead of the arbitrary defense-in-breadth strategy of requesting that every device include every cyber defense technology (IEC 62443 Part 4).

1 Introduction

This paper is an updated and abbreviated version of [1] and introduces the importance of designing system security instead of relying only on device security. The Purdue Model has become a useful reference for energy control system (ECS) architectures as a mission-critical subset of industrial control systems (ICSs). This model provides a method to identify and define the multiple distinct segments of the ECS network based on their information technology (IT) and operational technology (OT) characteristics. This model has driven the development of ISA99 and IEC 62443 defense-in-depth strategies, where cybersecurity features are distributed among multiple levels of the control system. This defense-in-depth strategy provides complete cybersecurity instead of the inadequate device-level features called out in IEC 62351 and IEC 62443 Part 4. Recent failures of the technology these device-level features are based on illustrate that they often create new, unintended vulnerabilities much worse than the challenges they were intended to mitigate.

2 Momentary and Sustained Outages in EDSs and ECSs

North American Electric Reliability Corporation (NERC) transmission availability data system definitions [2] include outage indices used by the Institute of Electrical and Electronics Engineers (IEEE) to define energy delivery system (EDS) reliability. A power system momentary outage is defined as an automatic outage with a duration of less than one minute. A power system sustained outage is defined as an automatic outage with a duration of a minute or longer [2].

IEC 60834 [3] requires that transmission and receipt of protection control signals be less than 10 milliseconds, and IEC 61850 [4] requires that they be less than 3 milliseconds. IEEE 1646-2004 [5] requires that protection information shared between intelligent electronic devices (IEDs) within a substation be within one-fourth of a cycle (~4 milliseconds in a 60 Hz system) and information shared externally be within 8 to 12 milliseconds.

A typical Generic Object-Oriented Substation Event (GOOSE) protection signal message burst ends 16 milliseconds after detection of the power system fault. Therefore, a secondary system communications network momentary outage of less than 16 milliseconds will not cause a failure of the protection system to automatically operate the primary system.

A sustained outage in the secondary system communications network may cause a failure of the protection system to automatically operate the primary system. The risk of a sustained outage and the consequences must be understood in order to accept the risk or change the secondary system to mitigate the vulnerability.

Key process indicators include the total number of protection signal delivery outage events, the duration of each event, the accumulated durations of events, and the duration of the longest outage.

3 N–1 Availability of EDSs and ECSs

As described in [6], the EDS is often networked to improve service capability and availability. Networking enables the system to experience an outage and still perform. Primary systems are composed of an undetermined quantity of components, referred to as N; N–1 reliability means that one of the devices can fail to serve its purpose and the system will continue to function.

Redundancy does not address the removal of the fault, and while the first fault exists the system will be in a N-0 state and no longer fulfill the design requirement of N–1. Therefore, redundancy may enable automatic operation to limit the effect of the fault to a momentary outage and the system will continue to function in the N-0 state. However, a second fault will result in a sustained outage that may cause loss of service until the outage is detected, isolated, and resolved by human interaction.

Design for availability using resiliency is defined as the ability to automatically detect and isolate each failure and react to restore service, mitigate the initial fault, and return the system to its N–1 state after a brief outage.

The ECS is essential to automatically operating the EDS equipment to clear faults. The ECS uses OT as a tool to protect, monitor, and control the EDS. Since the resiliency of the primary system relies on the availability of the ECS, the ECS must be more reliable and available than the primary system it is tasked with keeping in service.

IEC 62439 Part 1 describes numerous technologies to improve the availability of Ethernet communications [7]. IEC 62439 Part 5.1.1, Resilience in Case of Failure, describes how industrial systems such as EDSs rely on the correct function of the automation system. Industrial systems tolerate a degradation of the automation system for only a short time, called the grace time. Therefore, the automatic outage should be momentary in duration.

ECS and ICS automation systems may contain redundancy to cope with a single component failure, but mission-critical designs require resiliency. Methods differ on how to handle resiliency, but their key performance factor is the recovery time (i.e., the time needed to restore operation after the occurrence of a disruption). If the recovery time exceeds the grace time of the industrial system, protection mechanisms initiate a (safe) shutdown, which may cause significant loss of production and plant operational availability.

4 ICSs, Purdue Model, and Defense in Depth

As ICSs became more complex, IT methods failed because they intentionally ignore the special characteristics and restrictions of ICS and ECSs, some of which are as follows:

- Many ICS devices (e.g., protective relays) have the capacity to execute only their intended task and cannot implement demanding security controls like authentication or encryption.
- Firewalls and intrusion detection systems may introduce latency that can negatively affect the real-time communications and determinism of certain tasks.
- ICS processes have extremely high uptime requirements with no time for maintenance, patching, or other security-related activities. This makes nearly impossible the implementation of blacklisting technologies.
- In case of emergency, operators must interact quickly and precisely with the ICS. The use of complex passwords, for example, may create delays that can mean the difference between life and death.

The Purdue Enterprise Reference Architecture (also known as the Purdue Model) was developed during the 1990s by Theodore J. Williams and the Purdue University Consortium for Computer Integrated Manufacturing as a methodical approach to compartmentalizing the applications and features within the ICS.

Initially, the Purdue research did not take security or safety into account [8]. Its intended purpose was to improve factory ICS efficiency and reduce costs, with automation based on cyber processing and communications methods. Later, research on cybersecurity using the Purdue Model was based on IT influences and misrepresented attributes of OT as challenges or threats (e.g., distributed and embedded devices, real-time control).

Throughout the years, the Purdue Model has been used and adapted to different industries. In fact, the International Society of Automation's ISA99 framework is based on the Purdue Model and is used to describe the basic functions, composition, and levels of an ICS [9].

The ISA99 framework was developed by the Standards and Practices Committee 99 (SP99), but it is now aligned with IEC 62443 [10], which organizes a series of standards into four groups that address a wide range of topics related to ICS security.

The Purdue Model has been adapted by the United States Department of Homeland Security in conjunction with some research organizations to create a flexible defense-in-depth model to secure ICSs without affecting their performance.

Reference [11] describes using standards to segregate the components of an ECS as a specialized ICS. The ECS defense-in-depth levels are illustrated in Fig. 1.

A simplified description of each level is provided as follows:

- Level 0: Digital and analog data are sent to higher levels while controls are received to ensure the system is safe and stable. Physical security controls are required in this level, including closed-circuit television, physical barriers, and alarms.
- Level 1: The information from Level 0 is processed in this level to determine the necessary controls to issue. The integrity of the devices may be determined by baselining and periodic baseline verifications.
- Level 2: Monitoring, automation processes, and further controls reside in this level. Communication filtering and processing in this level may prevent certain attacks, like denial of service.
- Level 3: This level provides internal segmentation to the ICS, separating the machine-to-machine levels from the human-to-machine levels. This level ensures that only authorized communications are exchanged between upper and lower levels.
- Level 4: Data are concentrated in this level for analysis and monitoring. Encryption may be used to reduce the risks introduced by general purpose devices.

- Level 5: This level provides physical and logical separation between the ICS and the enterprise network. Physical security controls may be implemented, as well as virtual private networks to provide confidentiality, integrity, and encryption.
- Level 6: This level is technically not part of the ICS. It includes policies, procedures, risk analysis, and other human-based tools used to secure the ICS.

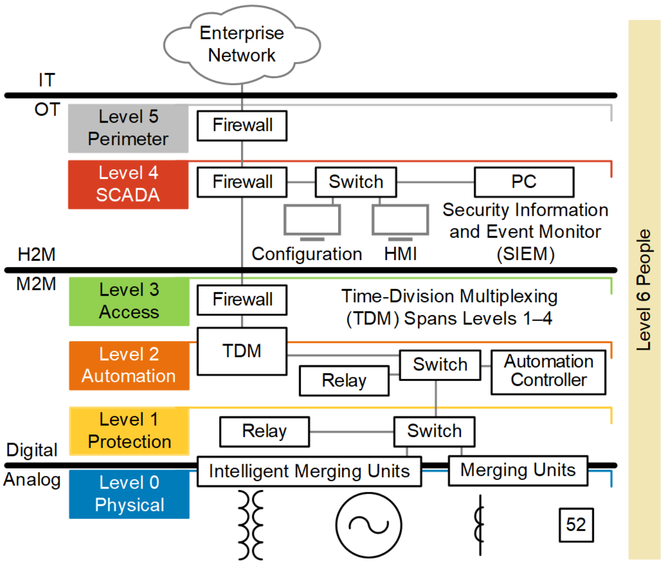
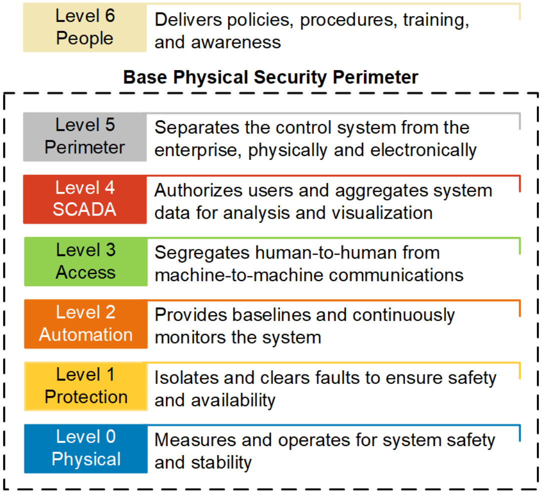


Fig. 1. ECS Defense-in-Depth Levels Diagram

The focus of this paper is cyber resilience and the security of the ECS to maintain availability to protect and control the EDS. Security is critical at all levels of a control system, but each level may have a different focus for its security, as represented in Fig. 2 [11].



Level 6 People	Delivers policies, procedures, training, and awareness

Base Physical Security Perimeter

Level 5 Perimeter	Separates the control system from the enterprise, physically and electronically
Level 4 SCADA	Authorizes users and aggregates system data for analysis and visualization
Level 3 Access	Segregates human-to-human from machine-to-machine communications
Level 2 Automation	Provides baselines and continuously monitors the system
Level 1 Protection	Isolates and clears faults to ensure safety and availability
Level 0 Physical	Measures and operates for system safety and stability

Fig. 2. Security Focus of Each Defense-in-Depth Level

5 Counteracting and Compensating Technologies for Communication Network Faults

Whenever operation depends on the correct function of the automation network, it may become necessary to increase the availability of the network through counteraction or compensation. Counteraction in the ECS is the act of adding technology to a system component to nullify the effects of some previous choice. The simplest and least expensive way to increase ECS availability and reduce maintenance is to use components with a demonstrated low failure rate and resiliency as described in IEC 62439 Part 1. As an alternative, IEC 62439 Part 3 considers the use of IT components with a high failure rate in the OT ECS and counteracting this choice with communications protocols that introduce redundancy.

Compensation in the ECS is the act of adding technology to one system component to intentionally avoid the adverse effects it would have on other components. Robust communications security systems are frequently patched or updated and use significant processing and memory to provide popular methods of obscuring information and preventing intrusion. The simplest and least expensive way to increase availability and reduce maintenance to the ECS is to compensate by adding a firewall with robust security that shields the protective relays and other IEDs.

The preferred IEC 62439 method for creating high-availability communications networks, described in IEC 62439 Part 1, is resiliency via recoverability, whereby faults are detected and isolated, and network traffic is rerouted without human interaction.

The alternative IEC 62439 counteraction methods of Parallel Redundancy Protocol (PRP) and High-Availability Seamless Redundancy (HSR), described in IEC 62439 Part 3, are defined as repairable and thus provide no resiliency. These methods result in sustained outages of indefinite duration and reduce the secondary system to an N-0 state.

PRP systems can be improved to mitigate the vulnerabilities of the repairable design by combining PRP with IEEE 802.1w Rapid Spanning Tree Algorithm (RSTA) as prescribed in IEC 62439 Part 1. Correctly implemented RSTA OT networks will recover after a momentary outage of less than 16 milliseconds and return the system to an N–1 state.

OT-based software-defined networking (SDN) is a packet switching technology that gives unprecedented control over network traffic and failover speeds. Instead of counteracting poor design choices, OT SDN works autonomously or provides compensation techniques to existing technologies to increase the reliability and security of the overall system [12].

6 NIST Threat Sources and Examples

The National Institute of Standards and Technology (NIST) describes a threat source as "the intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability," [13]. Categories include natural, technical, operational, environmental, human, and physical threats.

As an example, on February 15, 2019, a Transport Layer Security (TLS) 1.3 vulnerability was discovered that enabled hackers to eavesdrop on encrypted traffic [14]; before the guidelines were published, the vulnerability in the recommended version of TLS had been weaponized.

TLS is a cryptographic protocol used for internet communications and online transactions. Like other technologies, this cryptography method is "perishable" and must be replaced when new processors make it obsolete or when a vulnerability is found. Unfortunately, some IT designers promote it for use in OT devices. TLS is an example of the unintended consequences of an inappropriate deployment of technology creating the need to physically modify an in-service device. In March 2018, TLS 1.3 was finalized and the Internet Engineering Task Force (IETF) published it as RFC 8446 in August 2018. In December 2018, the comment period closed on NIST Special Publication 800-52 Revision 2 [15]. This documents states that all government TLS servers and clients must upgrade to TLS 1.3 by January 1, 2024. As noted, in February 2019 a TLS 1.3 vulnerability was weaponized by hackers to eavesdrop on encrypted traffic before the guidelines were even published [14], thus requiring the removal of each affected device from service for repair.

A second simple physical threat is the forget-and-flood feature in every Ethernet switch chip. When a switch does not know the destination of a received frame, it floods, or sends the frame to all ports except the port it was received on. Malicious and nonmalicious uses of this feature may physically prohibit the delivery of ECS protection messages via sustained bandwidth saturation.

7 IEC 62443 Defense in Depth

According to Reference [16], "The ISA/IEC 62443 series of standards, developed by the ISA99 committee as American National Standards and adopted globally by the International Electrotechnical Commission (IEC), is designed to provide a flexible framework to address and mitigate current and future security vulnerabilities."

The NIST Risk Management Framework (RMF) and Cybersecurity Framework (CSF) itemize controls to implement a program and reference international standards, such as IEC 62351 and IEC 62443, that provide details. The RMF core defines five main functions: identify, protect, detect, respond, and recover. Coincidentally, these are the same steps used to manage the EDS. The RMF and CSF provide actionable information to choose the correct implementation of the related technical standards.

ISA/IEC 62443 Part 3-3: System Security Requirements and Security Levels provides detailed technical control system requirements and defines the requirements for control system capability security levels. These levels reflect the Purdue Model levels for device function and capability to describe the appropriate security technologies to be deployed in devices at each level.

ISA/IEC 62443 Part 4-1-2018: Secure Product Development Lifecycle Requirements defines a secure product development lifecycle. This lifecycle includes security requirement definitions, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management, and product end-of-life guidelines.

7.1 IEC 62443 Device Compensation

IEC 62443-3-3 (for systems) and IEC 62443-4-2 (for components) define the required security functions for each ICS level. Therefore, the ICS level in which the device resides dictates the minimum capabilities of the device. The user-least-privilege strategy requires that devices not be required to support features that belong at a higher level of the ICS. This strategy allows for a device at a higher level to compensate for the intentional decision to not put a feature in a device at a lower level and keeps the device capability requirements limited to those necessary for that level.

An appropriate use of IEC 62443 Part 3-3 and Part 4-1 illustrates where safety and security technologies should be deployed among OT devices to maximize impact and reduce unintended vulnerabilities.

7.2 IEC 62443-4-1 Product Lifecycle Requirements

IEC 62443-4-1 Secure Product Development Lifecycle Requirements provides a comprehensive and important description of the differences between devices to be used in OT ECS versus Internet of Things (IoT), cloud, and fog devices, including:

- Encryption via compensation—defense-in-depth compensation mechanisms that allow indirect connection (7.2.1.c) and encryption external to the relay (12.1.b).
- Keeping security features at the appropriate level—safeguard via defense-in-depth compensating mechanisms at higher level (7.2.1.g).
- Keeping the device as simple as possible—secure design best practices include least-privilege design (7.4.1.c).

8 Unintended Consequences of IEC 62443 Part 4-2 Defense in Breadth

Defense in breadth is the concept of putting every possible security feature in every single device, ignoring the appropriate deployment based on the Purdue Model levels. This strategy is often promoted for devices with very short lifespans deployed in locations that cannot be protected by a defense-in-depth system. An example is a remote wireless sensor as part of an IoT, cloud, or fog application (not the mission-critical ECS) that publishes data but has no control with an end of life that coincides with the expiration of the internal encryption. Also known as edge computing or fogging, fog computing facilitates networking services between IoT and cloud end devices and cloud computing data centers.

IoT, cloud, and fog device data encryption convert data so that it can only be read by people or devices with access to a secret decryption key or password. This creates the challenge of making sure that all clients and data servers are updated to the same patch version at the same time. In addition to the challenge of patching firmware when the encryption expires, malware hidden inside encrypted traffic cannot be seen or stopped by most security technologies. This may be necessary for IoT, cloud, and fog applications but is not appropriate for the millions of devices deployed in ICS and ECS systems.

8.1 True Impact of Failure to Apply User Least Privilege

For instance, consider the earlier example of TLS 1.3. When considering the defect management portion of an OT device lifecycle, patch management creates a vulnerability and a high cost to the OT ECS. Laptops and smart phones are often upgraded automatically or on demand without consideration of a loss of use. OT devices require preplanned removal from service, which requires a planned EDS outage, ECS outage, or both. Also, personnel need to be onsite to apply and test the new TLS patch. Therefore, encryption should be deployed in a Level 3 device (shown as a firewall in Fig. 1) that shields the Level 1 and 2 devices on the protected local-area network (LAN).

8.2 True Cost of Failure to Apply User Least Privilege

The cost of patch activity for utilities can be around 5,000 euros per ECS device, including several hours of personnel time to travel, patch, and test. Additional expenses are incurred if an EDS outage is also required to safely remove the ECS device from service.

8.3 Prevention via Correct Application of IEC 62443

Recent activities for industrial IT and IoT devices have prompted IEC 62443 Part 4-2 to promote deploying Level 3 security features in Level 1 and 2 devices. While this may be acceptable for IoT devices deployed outside a firewall and with a two-year lifecycle, this is very problematic for OT devices. Thus, NIST RMF and CSF strategies recommend IEC 62443 Part 3 defense in depth and not Part 4 endpoint security, like TLS. Instead of a strength, these security technologies become a very large vulnerability when deployed in Level 1 and 2 devices. Each change forces an unwanted outage to patch the security firmware. A typical large utility with 12,000 OT devices would be faced with over 1,000 days of effort at a cost of 60M euros.

When TLS is deployed in a Level 3 device, like the firewall in Fig. 2, none of the protection and automation devices need to be patched. Only one device per substation needs be patched. This firewall device can be safely removed from service while personnel are onsite without affecting the safety and protection of the EDS.

Security is not a goal that can be met but is rather an ongoing process. New vulnerabilities are discovered every day, existing threats evolve, and people make mistakes. Recent activities illustrate that newly added security technologies can become attack vectors to otherwise isolated OT systems.

OT designs must prevent attacks and also anticipate that they will happen nonetheless. Attackers are often more skilled and motivated than defenders. IEC 62443 Part 3 explains defense-in-depth methods to compartmentalize devices and minimize what needs to be defended. This also minimizes the loss when a device is compromised.

9 Case Study of Large Utility's Evaluation of OT Device Access Control

Recently, a large European utility performed a thorough evaluation of the available international standards (IEC 62351, IEC 62443, and IEEE 1686) for ICS and ECS cybersecurity. These documents address the malicious human insider and outsider threats to the system. However, they do not adequately address nonmalicious human threats. More importantly, they do not address the other five threat categories at all. Based on these concerns, the utility IT and OT staff decided to adopt IEC 62443 Part 3 defense in depth, with security controls distributed among the six levels of the ECS. Due to the frequent disruption of OT devices caused by localized encryption and authentication, they decided not to adopt IEC 62443 Part 4-2.

Administration of OT devices is different than that of IT devices in that they are commissioned and then updated on, at most, a yearly basis. Control system networks have access restricted to fewer individuals on infrequent and controlled intervals. Where IT networks are centered on information confidentiality, OT networks are centered on information availability.

As an example, illustrated in Table 1, a utility with approximately 1,500 employees will have approximately twice the number of computers, phones, and similar devices assigned to those individuals as part of the organization's IT enterprise system. Table 1 depicts the number of OT devices and IT appliances such as routers, firewalls, servers, and other Ethernet packet-forwarding devices in their respective OT and IT systems. While users constantly interact with their human-to-machine devices, access to the more numerous OT devices is ideally never and at most less than once a year.

Table 1 Typical User Access for IT and OT Systems (for 1,500 Total Users)

Type	**Cyber Asset Type**	**User Access**	**Total Assets**	**Users With Access (out of 1,500)**
IT	Computers and phones	Constant	3,000	1,500
	IT appliances	Once per week	750	25
OT	All OT devices	< Once per year	12,000	40
	Relays (subset of OT devices)	< Once per year	8,000	20

Table 1 illustrates that the number of employees out of the 1,500 that can access the OT devices directly is a very small percentage of the organization's employees. Only about half that number are allowed access to the even greater number of utility substation assets (i.e., the relays).

Continuous access is neither necessary nor acceptable in OT networks. Human access to devices in an OT network is typically a scheduled event, planned and assessed for system impact. Unscheduled authorized human access to devices in an OT network is for emergency or mitigation events, which typically require greater scrutiny and analysis after human interaction with the ECS. For this reason, a different and simpler access control architecture that aligns with the defense-in-depth approach is necessary.

While users in IT systems accept and expect daily access to resources and systems, there is a tendency to work around or minimize the effectiveness of the access control mechanisms for OT devices and networks.

Effective OT security cannot rely on unwarranted, unnecessary, and often misunderstood trust in the most targeted and compromised organization asset, the human user.

10 Conclusion

The multilayer approach of defense in depth allows asset owners to implement the correct security controls in each layer of the ICS without degrading its performance. It allows the use of common standard protocols and it protects the ICS from internal and external attackers without hiding or obscuring the network. For all these reasons, defense in depth is the correct approach to properly securing modern ICSs against malicious and nonmalicious cyber attacks.

IEC 62443 Part 3 provides an appropriate and useful defense-in-depth strategy for OT networks. Based on work in the ISA99 and Purdue models for ICSs, the defense-in-depth strategy provides levels of appropriate security and prevents insecurity. Such insecurity is often the byproduct of unintended consequences resulting from vulnerabilities such as frequent firmware patches in protective relays that have internal encryption and TLS based on IEC 62443 Part 4-2.

The primary goal of the OT ECS system is to keep the primary EDS safe and functional. An outage in the communications system must be sufficiently short to enable at least one GOOSE message to reach its destination. A typical GOOSE message burst ends 16 milliseconds after detection of the power system fault in order to accomplish protection operation within the 20-millisecond worst-case operation time. Therefore, the duration of a momentary outage of the communications network must be less than 16 milliseconds for the secondary system to correctly serve the operation of the primary system.

Simplicity and security are achieved by removing the trust in the most targeted and compromised organization asset, the human user, and placing it solely with the organization. OT resource permissions in this new architecture should be nonpersistent and provided for only a limited window of time by a second party, taking separation of duty controls in account.

11 References

[1] Dolezilek, D., Gammel, D., Fernandes, W.: "Complete IEC 61850 Protection and Control System Cybersecurity Is So Much More Than Device Features Based on IEC 62351 and IEC 62443," proceedings of the 10th Annual Protection, Automation and Control World Conference, Glasgow, United Kingdom, June 2019.

[2] North American Electric Reliability Corporation, "Transmission Availability Data System Definitions," January 2013. Available: https://www.nerc.com/.

[3] IEC 60834, Teleprotection Equipment of Power Systems—Performance and Testing, 1999.

[4] IEC 61850, Communication Networks and Systems for Power Utility Automation, 2019.

[5] IEEE Standard 1646-2004, IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation.

[6] CIGRE JWG 34/35.11, "Protection Using Telecommunications," 2001.

[7] IEC 62439, Industrial Communication Networks—High Availability Automation Networks, 2016.

[8] Brodsky, J.: "What Was That Purdue Model Stuff, Anyway?" *SCADASEC Magazine*, March 2018. Available: http://scadamag.infracritical.com/index.php/2018/03/01/purdue-model-history/.

[9] The International Society of Automation, "ISA99, Industrial Automation and Control Systems Security." Available: https://www.isa.org/templates/two-column.aspx?pageid=124560.

[10] IEC 62443, Industrial Communication Networks—Network and System Security, 2009.

[11] Smith, J., Kipp, N., Gammel, D., et al.: "Defense-in-Depth Security for Industrial Control Systems," proceedings of the EEA Conference & Exhibition, Wellington, New Zealand, June 2016.

[12] Dolezilek, D. J.: "Using Software-Defined Network Technology to Precisely and Reliably Transport Process Bus Ethernet Messages," proceedings of the 14th International Conference on Developments in Power System Protection, Belfast, UK, March 2018.

[13] Computer Security Resource Center, "Threat Source," *National Institute of Standards and Technology*. Available: https://csrc.nist.gov/glossary/term/threat-source.

[14] Millman, R.: "TLS 1.3 Vulnerability Enables Hackers to Eavesdrop on Encrypted Traffic," *SC Media UK*, February 2019. Available: https://www.scmagazineuk.com/tls-13-vulnerability-enables-hackers-eavesdrop-encrypted-traffic/article/1525916.

[15] McKay, K., Cooper, D.: "(DRAFT) NIST Special Publication 800-52 Revision 2: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations," *National Institute of Standards and Technology*, November 2017. Available: https://csrc.nist.gov/.

[16] Automation.com, "ISA Announces ISA/IEC 62443-4-2-2018 Standard," *International Society of Automation*, September 2018. Available: https://www.automation.com/library/resources/isa-announces-isaiec-62443-4-2-2018-standard.

20191105 • TP6955