A SANS Whitepaper

Effective ICS Cybersecurity Using the IEC 62443 Standard

(Companion piece to “Managing ICS Security With IEC 62443”)

Written by **Jason Dely**

November 2020

Sponsored by:

Fortinet

Improving ICS security typically involves a thorough risk assessment followed by a security assessment (also known as a *vulnerability assessment*), both of which are supplemented by reports detailing vulnerabilities, weaknesses and recommendations. Then comes the flurry of activity in the form of risk mitigation plans focused on determining which findings truly warrant the investment involved in mitigation. This level of scrutiny has its benefits, but it tends to narrow the security problem down to a focused list of findings that represent a mere slice of the entire ICS security posture. After a review of the findings, mitigations can take anywhere from one to three years to complete, based on factors such as current ICS security maturity, agility and available budget. By then, it’s time for a whole new assessment.

Necessary improvements may get implemented, but what’s missing in this approach is cohesion. Making ICS security improvements is not just about addressing weaknesses by adding security controls. Those controls should be carefully selected, complementary and collectively support a clear understanding of how to prevent, monitor, detect and respond to cybersecurity incidents within those environments. Improving cybersecurity across an ICS cannot be placed into a simple sequential road map of phases. Ideally, depending on the security requirements and protection levels identified during the risk assessment process, the ICS should be segmented into security zones that may operate at different phases of maturity.

Analyst Program

IEC 62443 (hereafter referred to as "the Standard" in this paper) is a set of ICS security standards written by ICS experts for ICS owners, manufacturers and integrators across a range of applications and sectors. It provides technical requirements that foster a cohesive approach to security that takes into account varying phases of maturity. Using a step-by-step process incorporating "maturity phases," the Standard outlines a life-cycle approach as part of a cybersecurity program. By segmenting ICS into security zones, organizations can better focus mitigation efforts related to risk, vulnerabilities and compliance in both a localized and broad perspective within their ICS environment.

Now let's take a closer look at what the Standard is all about.

Overview of IEC 62443

IEC 62443 separates an ICS organization into security zones based on assessment of risks. The Standard provides guidance on how to select the zones and assign the security level (SL). Certain controls are required to meet each level. An organization must assess the gaps between its existing security controls and the Standard's definition of the assigned level. These zones are then assigned SLs ranging from 1 to 4, as shown in Figure 1.

IEC 62443 Protection Levels

Asset Owner, System Integrator and Product Supplier

What are the different levels?

To achieve optimum level of security (i.e., SL-T) and meet the security requirements, the SRs and REs are deployed depending on the protection required against the specific threats. The IEC 62443 protection levels are mentioned below.

Protection Levels

SL 0	No specific requirements or security protection necessary
SL 1	Protection against casual or coincidental violation
SL 2	Protection against intentional violation using simple means with low resoucres, generic skills and low motivation
SL 3	Protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills and moderate motivation
SL 4	Protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills and high motivation

Figure 1. IEC 62443 Protection Levels

Even when an organization separates its ICS environments into multiple zones, there is never perfect risk isolation among all zones because a weakened zone can affect surrounding zones in two ways. First, a disruption of services or operations within the weakened zone can cascade into other zones, depending on those services. Second, a zone compromise brings a threat closer to other zones. To overcome these challenges, the Standard suggests various requirement enhancements (REs), which we'll cover shortly.

Portions of the systems in an organization's ICS can be at different phases of maturity for several business-based or financial reasons. As stated in the Standard, "Organizations can achieve a more detailed evaluation of security maturity by assessing achievements within portions of the industrial automation and control system in terms of the phases and steps." Table 1 presents the Standard's maturity phases and steps.

Table 1. Security Maturity Phases

Phase	Step
Concept	Identification Concept
Functional analysis	Definition
Implementation	Functional design Detailed design Construction
Operations	Operations Compliance monitoring
Recycle and disposal	Disposal Dissolution

By meeting the security level targets for each of the zones, a natural cohesion exists that ultimately improves the entirety of ICS security posture. Figure 2 depicts how a segmented approach may look more complex but is actually simpler because it breaks things down into smaller, more cost-effective pieces.

A monolithic approach, shown on the left, is more difficult and costly because everything needs to be brought to a level 4, which requires excessive security control implementation.

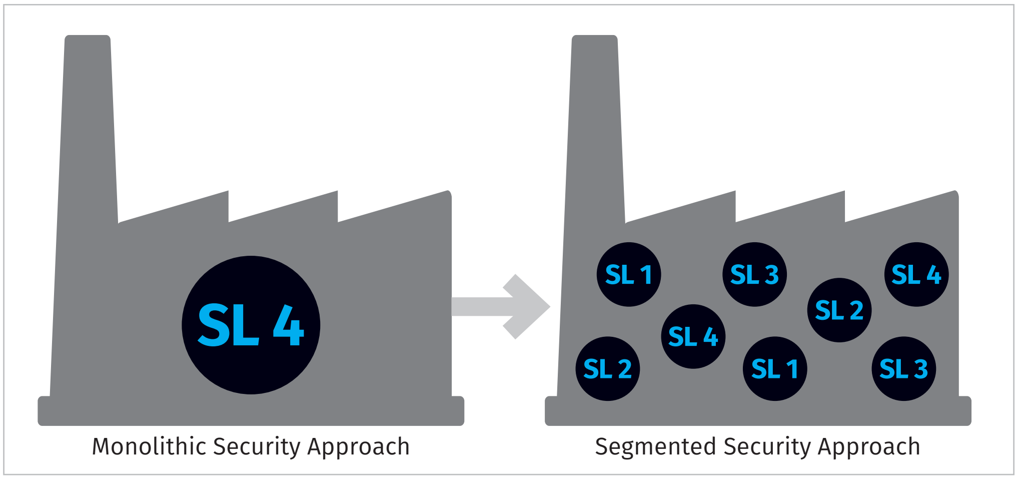

Figure 2. Monolithic vs. Segmented SL Measurements Across an Environment

To help users determine the SL requirements within each security zone, the Standard categorizes seven foundational requirements (FRs), expanded into a series of system requirements (SRs) and REs to improve security strength. A chart in the Standard depicts each SL with corresponding FRs as shown in Figure 3.

Foundational Requirements (FRs)

FR1 Identification and authentication control (IAC)
FR2 Use control (UC)
FR3 System integrity (SI)
FR4 Data confidentiality (DC)
FR5 Restricted data flow (RDF)
FR6 Timely response to events (TRE)
FR7 Resource availability (RA)

Example High-Level Operational Controls Mapping to FRs

FR1 Passwords and user authentication
FR2 User roles and authorization enforcement (RBAC)
FR3 Session handling, mechanism to recognize change
FR4 Encryption
FR5 Network segmentation
FR6 Logging and monitoring
FR7 System backup and recovery

Fortinet Security Solutions support Asset Owners achieve these requirements.

Figure 3. High-Level Mapping of Fortinet Products to Foundational Requirements

To assist with the definition of each SL, the Standard provides a threat definition for each level and a chart to map SRs and REs to FR Security Levels 1–4. The ICS threat landscape differs across each sector, industry type and organization. Therefore, although these are solid definitions and a good place to start, consider them specifically in relation to your organization's unique defense posture. Potentially, the SLs could pose unique differences for each security zone as well—threats, operational changes and technology such as Industrial IoT (IIoT) can change the attack surface of an ICS. SLs help establish goals, but goals must always be flexible and actively realigned to stay current with the global changes in threats. Table 2 maps SRs and REs to FR security levels.

Table 2. Mapping of SRs and REs to FR Security Levels 1–4

SRs and REs			SL 1	SL 2	SL 3	SL 4
FR 1	**Identification and authentication control (IAC)**					
SR 1.1	Human user identification and authentication	5.3	✔	✔	✔	✔
SR 1.1 RE 1	Unique identification and authentication	5.3.3.1		✔	✔	✔
SR 1.1 RE 2	Multifactor authentication for untrusted networks	5.3.3.2			✔	✔
SR 1.1 RE 3	Multifactor authentication for all networks	5.3.3.3				✔
SR 1.2	Software process and device identification and authentication	5.4		✔	✔	✔
SR 1.2 RE 1	Unique identification and authentication	5.4.3.1			✔	✔
SR 1.3	Account management	5.5	✔	✔	✔	✔
SR 1.3 RE 1	Unified account management	5.5.3.1			✔	✔
SR 1.4	Identifier management	5.6	✔	✔	✔	✔

Measuring the assigned SL of each defined security zone with seven FRs as well as the SRs and REs provides a more granular perspective on the defense posture of each security zone. The act of measuring also can provide an opportunity to apply the MITRE ATT&CK® for ICS Matrix to study the applicability and capability of attacker tactics and techniques against your security zones' countermeasures, existing or absent.[1] "The Role of Countermeasures" explains in more detail how countermeasures fit within the SL approach.

The Role of Countermeasures

Complying with the definitions of FRs and SRs within an SL can consist of using many different countermeasures that will vary based on the makeup of the security zone. When looking at a list of recommendations, identify opportunities and capabilities to expand countermeasures in the future that may benefit other security zones. Procurements and resources are applied to introduce countermeasures to meet a specific risk-reduction recommendation from a finding in an assessment report. With a breakdown of the requirements of each security zone with an assigned SL prior to the assessment, the decision and action taken to remediate can be advantageous across many security zones, including those outside the immediate scope of the assessment. The result is the capability to maximize return on investment both today and tomorrow. This approach should also include documenting feature expansions provided by the solutions that may have use in future identified countermeasures.

Zones, Subzones and Conduits

Each security zone and the communication path between them (conduit) is assigned a target security level (SL-T). To reach what the Standard considers a satisfactory security level ("achieved" security level or SL-A), several contributing factors must be present. The Standard covers the factors in Figure 4 but recognizes there are likely more.

These factors must be considered when establishing security zones and conduits, and their respective security levels. As we will cover, an ICS can be segmented into security zones, but communication paths may leave residual attack vectors between those segments. Therefore, those paths and the associated neighboring security zones must be evaluated and meet SL-A in order for the security zone under review to meet SL-A.

SL(achieved) = f(x1, … , xn, t)

Where the factors xi (1 <= i <= n) include but are not limited to the following:

x1	SL (capability) of countermeasures associated with the zone or conduit and inherent security properties of devices and systems within a zone or conduit
x2	SL (achieved) by the zones with which communication is to be established
x3	Type of conduits and security properties associated with the conduits used to communicate with other zones (applicable to zones only)
x4	Effectiveness of countermeasures
x5	Audit and testing interval of countermeasures and inherent security properties of devices and systems within a zone or conduit
x6	Attacker expertise and resources available to attacker
x7	Degradation of countermeasures and inherent security properties of devices and systems
x8	Intrusion detection
t	Time

Figure 4. Required Factors to Reach IEC 62443's "Achieved" Security Level

[1] "ATT&CK® for Industrial Control Systems," https://collaborate.mitre.org/attackics/index.php/Main_Page

The Purdue Model: Reference Architecture for IEC 62443

What is commonly referred to as the *Purdue Reference Model* (derived from the Purdue Enterprise Reference Architecture [PERA] based on principles established by Purdue Laboratory for Applied Industrial Control [PLAIC]) functions as a reference architecture for the Standard. The use and assignment of the levels can be referenced back to its roots in the 220-page 1989 ISA Publication "PERA Reference Model for Computer Integrated Manufacturing (CIM)."[2] This publication was written from the viewpoint of industrial automation to "help in advancing the technology of computer integrated manufacturing and in solving some of the problems plaguing our industries today." ("Today" for the authors meant 1989.) The levels were used as a way to define a "sitewide network architecture" separated into levels distinguished by four principles (response time, resolution, reliability and repairability), used primarily in the context of data.

The principles of the model are not wrong and are still valid today, especially from the perspective of the value of data in an ICS. There are, however, areas where this model is not enough. First, the problems of 1989 were different from those we see today. With the increased use of and relationship to the ICS and operations, there are wireless communication technologies, cloud services, IoT, remote access, critical outsourced services bounded by SLAs and, of course, cybersecurity. The use of the model today (shown in Figure 5)—and likely even in 1989—is not meant to exactly mirror all organizations' ICS network architectures under the same construct, but rather as an educational tool that can be used to describe, educate and leverage for innovated problem solving.

Why Security Zones and Subzones Matter

As in 1989 (see "The Purdue Model: Reference Architecture for IEC 62443"), the Standard provides an ICS perspective of understanding and concepts for organizations to build upon to solve and improve ICS security challenges. One of the more powerful concepts that provides a security foundation when thoughtfully applied is that of security zones, subzones and conduits. Security zones are the basis for segmenting an ICS.

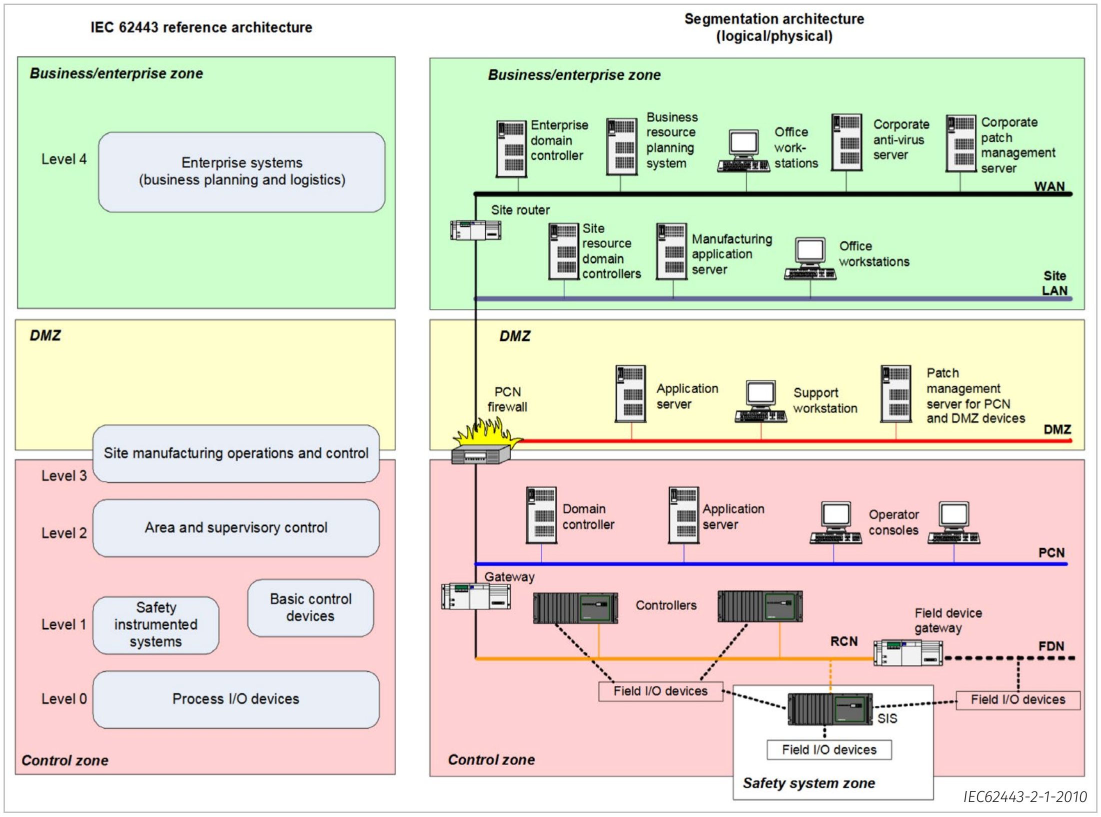
IEC 62443 reference architecture
Segmentation architecture (logical/physical)
Business/enterprise zone
Level 4
Enterprise systems (business planning and logistics)
DMZ
Site manufacturing operations and control
Level 3
Level 2
Area and supervisory control
Level 1
Safety instrumented systems
Basic control devices
Level 0
Process I/O devices
Control zone
Business/enterprise zone
Enterprise domain controller
Business resource planning system
Office work-stations
Corporate anti-virus server
Corporate patch management server
WAN
Site router
Site resource domain controllers
Manufacturing application server
Office workstations
Site LAN
DMZ
PCN firewall
Application server
Support workstation
Patch management server for PCN and DMZ devices
DMZ
Domain controller
Application server
Operator consoles
PCN
Gateway
Controllers
Field device gateway
RCN
FDN
Field I/O devices
SIS
Field I/O devices
Field I/O devices
Control zone
Safety system zone
IEC62443-2-1-2010

Figure 5. Reference Architecture Alignment with an Example Segmentation Architecture

[2] "Purdue Reference Model for CIM," www.pera.net/Pera/PurdueReferenceModel/ReferenceModel.html

An ICS can be best described as a system of systems. Depending on the sector and industry type, the ICS can be conceptually broken down into smaller groupings of 1) physical systems, such as machines, and 2) application assets that perform specific operational functions or share an operational risk. A zone is also 3) an informational asset that may exist only within these individual groups or may flow externally with other groups. A security zone can be any of these three assets or groups of assets that share a common security requirement, or goal, and can be logically brought together and concealed into a logical boundary. Figure 6 presents these groupings.

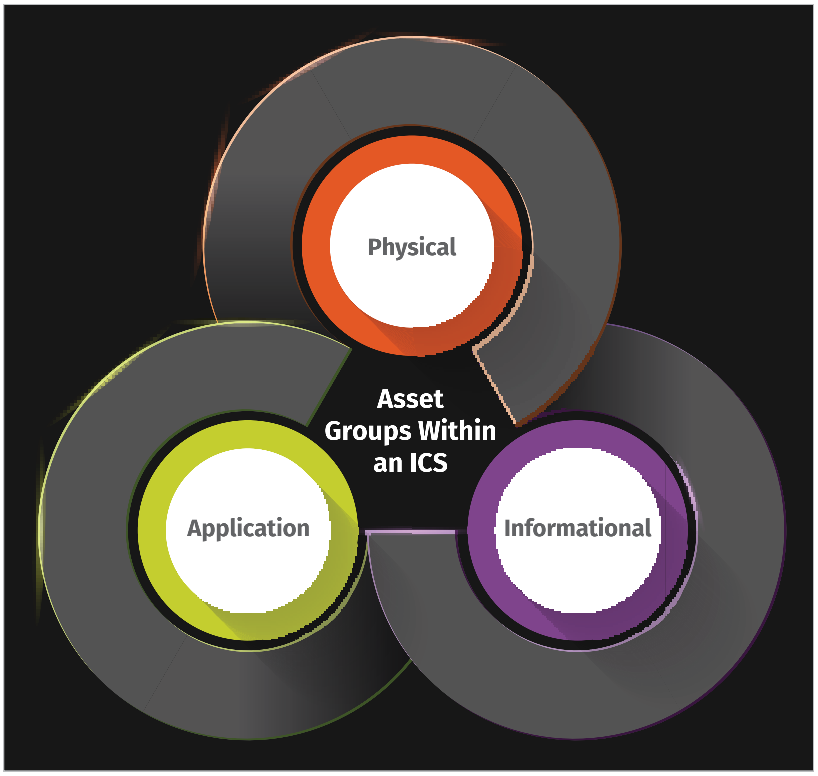

Figure 6. Three Asset Groups Within an ICS

An ICS may be structured where a small portion, such as a boiler, requires a slightly higher level of security but can otherwise benefit from the security level of the surrounding assets. For these cases, a subzone can be utilized. When performing segmentation, a security zone and subzone are just logical constructs of ICS operations and should be viewed outside the context of the actual physical network and components. After you review and understand the required communication paths between security zones, you can overlay this segmentation construct with the physical control system's hardware and network.

As stated, there are situations where information must flow within, into and out of a security zone by means of communication. This also includes the intermittent communications found by use of, but not limited to, programming terminals, mobile devices and portable media devices. The Standard refers to these communication channels as *conduits*, which can be identified as trusted or untrusted. Communications within a zone are largely recognized as trusted conduits. Untrusted conduits are communications from other security zones that are either not at the same security level or occur over a communication channel that is not at the same security level. The concepts and use of security zones and conduits are illustrated in Figure 7.

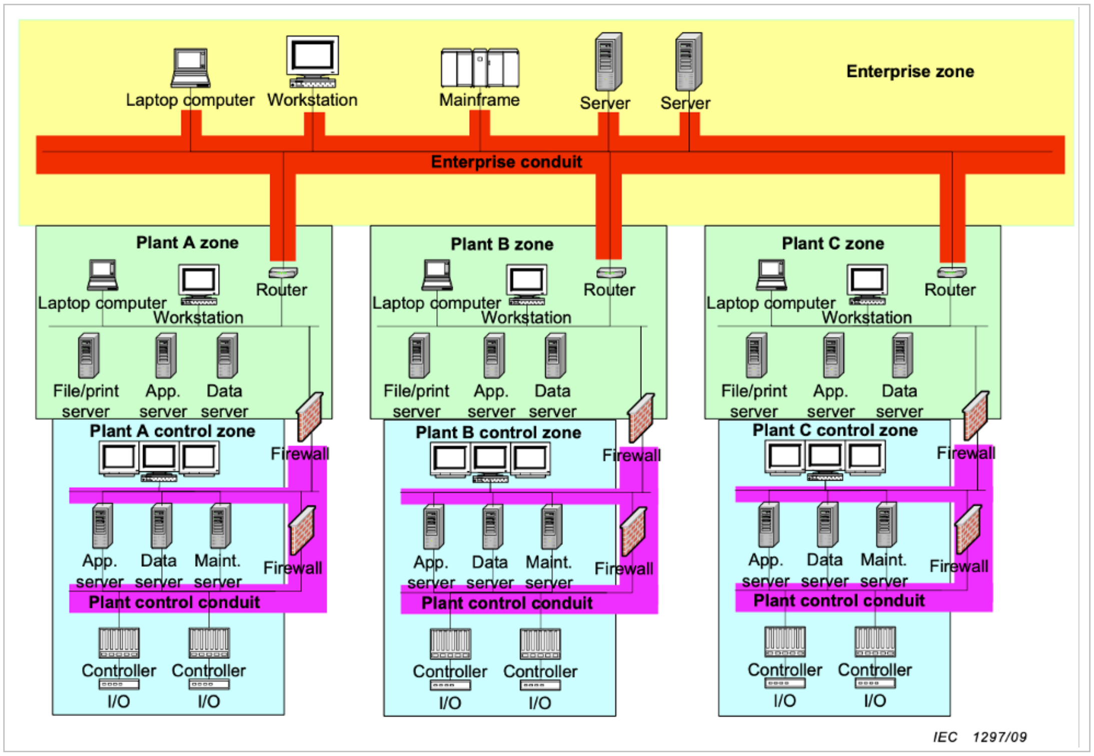

Figure 7. Relationships Between Conduits and Zones

For many organizations, segmentation can be a difficult process. This is why the zones should be abstracted without too much focus on the actual hardware and software. Only after the SLs are applied should the ICS equipment (such as network gear, PLCs, drives, computers, firewalls, services, protocols) be overlaid. This process will clearly depict all the shared hardware, network paths and software present in the environment. That information can identify opportunities that can help minimize assignment of higher SLs across many zones, thereby minimizing cost. Every environment is different, but the processes used can include the following principles:

- Lower security levels require fewer security controls.
- Hierarchal zoning and subzoning provide defense in depth.
- Zone boundaries provide choke points for network security monitoring.
- Server and computer application segmentation can introduce other opportunities.
- Use of network access control at switch level can help extend zone boundary controls.

Examples of Segmentation Challenges

With distributed control systems (DCS), the asset owner typically accepts the entire DCS as a single security zone. A DCS vendor provides a turnkey solution with a tightly controlled architecture of computers, software, network and programable automation controllers. So even if there were an opportunity to add subzones within the DCS environment, the asset owner would mostly be denied by the vendor due to validated system tests under support by the vendor. At the same time, however, the vendor provides a level of service and security with their offering. For these organizations, they should review the SLs, FRs and SRs with the DCS vendor. Otherwise, their segmenting efforts should be applied to systems outside the DCS, including boundaries for individual DCS, support systems and any safety instrumented systems.

As shown in Figure 8, SCADA owners tend to have clearly defined security zones mostly aligned with their network topology, but such situations have a higher probability of untrusted conduits used for critical communications.

SCADA owners also need to explore how to maintain isolation between each primary and backup control center to maintain integrity to prevent both from being compromised during the same security incident. Even if the communication medium was legacy telephony instead of ethernet, the architecture would typically remain the same.

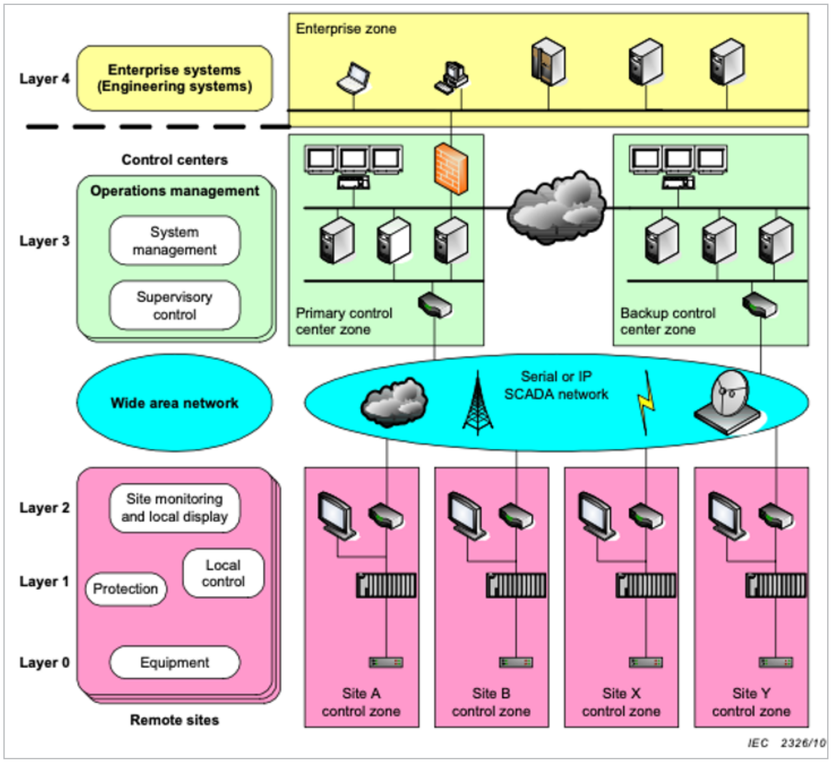

Figure 8. Reference SCADA Architecture Alignment with an Example Segmented Architecture

Some ICS environments can be troublesome because the control systems may have a significant data relationship with enterprise information systems, creating an operational dependency that must accommodate large security zones. Additionally, the information systems tend to reside in the enterprise, making it difficult to build independent hierarchal zones for defense in depth. In these architectures, it may help to use switches with network access control to produce multiple subzones in existing and new environments.

Lastly, legacy systems were engineered for cost and uptime efficiencies and do not always reflect the benefits of using security zones. In many cases, a collapsed system architecture may position fewer components spanning multiple security zones. The components are more than capable of handling production and operational efficiencies but may not meet today's security requirements. Replacing the controls systems is an expensive endeavor that leaves fewer assignable security zones, possibly resulting in more assets, which then require a higher security level. Identifying the zones if the control system were to be replaced, however, can be useful for future planning.

Managing FRs and SRs

After the security zones and conduits are identified, along with their respective SLs and associated requirements, the review and implementation of controls can commence. Communication access and external conduits both play a critical role in protecting the boundaries of security zones. Fortinet provides integrated capability in these areas through its FortiSwitch, FortiGate (with FortiOS) and FortiAnalyzer/FortiManager products. A deeper look into three specific access control points will demonstrate how a Fortinet solution could help maximize an organization's investment to manage these common use cases. These control points, according to the Standard, would be considered conduits:

- Security zone interface (either logical or virtual)
- Wireless (802.11) network interface
- Virtual private network (VPN) interface

The analysis followed this criterion: The security zone interface was treated unilaterally whether the communication path was straight off a wired connection, a wireless network or a VPN interface. Additionally, each wireless interface and VPN interface were treated as independent controlled access points. In this way, whether a communication path comes through either a wireless or VPN, it must transact across two control access points—the first to access either the wireless or VPN, and the second to access the security zone interface. Consequently, many of the controls identified to protect the security zone interface can be used on wireless and VPN as applicable.

The complete breakdown of the product review analysis can be found in Table 3 in the Appendix.

Security Zone Interface

Challenges

Implementing access control at an ICS boundary typically begins with policy configuration of source IP, destination IP, source port and destination port. Determining the policies, however, can be an exhaustive process and there are many ways to go about identifying what is and is not needed, and what has a temporal requirement (especially high-risk services). If analyzed thoroughly as part of the segmentation process, many of the critical communications already have been identified. What typically remains is to weed through the remaining policies to decide on an appropriate course of action.

Other features useful for telemetry systems, such as in a SCADA, include application control functionality on industrial protocols. This feature can be useful to prevent unwanted write events from lower-trust systems. It's also a useful feature in preventing a basic DoS attack by abuse of some ICS protocols, such as those that send arbitrary communication close events or connection initialize commands that may fill the connection limit of a device.

Due to cost, system latency and technology limitations, many organizations are faced with having to limit the ICS boundary to the extremities of their ICS network. To stay competitive in today's digital marketplace, however, many organizations are adopting IIoT concepts and technologies. Where once the convergence point of different business unit networks was clearly identifiable, this trend has blurred the line between IT, ICS and cloud resources. Not all sectors or organizations are seeking the adoption of IIoT or cloud resources for their ICS, at least from the standpoint of having the far-reaching communication and processing capabilities directly into their ICS network from outside networks. For those organizations that must consider extending their perimeter protections into their ICS network at strategic locations in their network, such strategic placement could provide the right amount of delay or detection to catch a threat attempting to move laterally within an ICS pivoted from a compromised pathway used by an IIoT device.

Coverage by Fortinet Solution

Because it is a firewall first and foremost, FortiGate supplies the expected features as a core functionality of the product. When this product is introduced into an existing environment, its **`learn`** functionality could prove more useful over time than other, more hands-on methods of manually adding rules while scouring hits caught by an any-any rule. The **`learn`** function does require some additional effort to determine what traffic is necessary or non-malicious, but it allows the product to be placed immediately into the system, where it learns over an acceptable period of time to catch, at minimum, the most critical traffic to be analyzed for necessity and risk.

With application control as a core function, FortiGate supports many industrial protocols.[3] Examine the use of these protocols and choose to block specific protocol features that will provide measurable effectiveness against capable threats.

FortiSwitch with FortiNAC supplies network access control, which can provide the capability to authorize and/or quarantine unauthorized devices brought onto the network. This capability prevents third-party contractors from arbitrarily connecting their own equipment or any other rogue devices. Think carefully about using network access control and choose it only if it provides measurable effectiveness against capable threats. Improper planning can limit flexibility required to recover quickly from various types of security or nonsecurity events.

Coupling FortiSwitch and FortiGate with FortiLink can enable micro-segmentation to support a zero trust security policy. Implementation of such a policy can manage the lateral communication among lower level networks within the perimeter of the ICS network. A zero trust policy is the most effective method to stop or detect lateral movement within an ICS network. A zero trust security policy is an advanced defense, especially with ongoing business trends across sectors. These trends, such as data analytics, have driven an increased demand to access data closer to the source (sensors, for instance). Coordinated change management plans will need to be adopted when using this solution to accommodate system and configuration changes required by the operations team. These changes most likely will be planned, but rare unplanned changes may be required for emergency situations.

People, Process and Technology

In practice, implementing any protection at the security zone interface requires advance knowledge of ICS communications and active onboarding/auditing of the operations team, vendors and controls engineering teams. We strongly recommend additional engagement of the asset owners, data owners or data recipients at either end of the communication. The team members will vary depending on the assets and data, whom the policies are written for and whom it affects. In some cases, a RASI[4] chart can help manage the change control process.

Each policy must follow a rigid process when designing, testing, enabling and auditing, and it must include an emergency disablement in support of unplanned operation events. Avoid creating a situation where loss of visibility and loss of control are a self-inflicted event.

Many ICS threats attack trusted systems. Decide carefully whether to utilize advanced features that can have disruptive effects on operations or create unnecessary cost to overhead. A misplaced sense of security and added complexity does not help achieve overall security goals.

[3] For more information, see www.fortiguard.com

[4] Responsibility, Authority, Support, Inform. For an example, see http://kilbrideconsulting.com/var/m_9/9f/9f8/38868/408089-RASI%20Chart.pdf?download

Wireless (802.11) Network Interface

Challenges

The use of wireless networks varies widely across sectors and industry types, but its security functionality can be incompatible with wireless-enabled ICS devices and systems. When possible, many ICS owners prefer to ban or heavily limit the use of wireless in their systems. However, even those organizations are feeling the pressure to add more data analytics to maximize revenue of their ICS, making wireless an extremely cost-effective technology compared to the cost of pulling physical wiring in an ICS environment. Organizations still need to evaluate security implications of using wireless networks. Manufacturing, for example, has been using wireless for almost as long as Wi-Fi has been around. Wireless use in automated guided vehicles, tow motor systems and other machine-level features has proven the technology to be a viable option. Security reviews and improvements of those networks should be ongoing, not only in terms of threats, but also the availability and integrity of those systems because they play a critical role in operations.

Coverage by Fortinet Solution

The FortiGate solution incorporates a wireless controller capability that provides cohesion between wireless interface security and the security zone interface. Along with the expected standard features, the incorporated IPS protects the wireless network from known 802.11 protocol attacks. Before employee-provided laptops are given network access, assets can be quarantined while the endpoint protection is audited.

People, Process and Technology

There are many use cases for wireless networks within an ICS. A formal policy and access request process should be rolled out. During a major shutdown and commissioning of new equipment, a team may roll out a temporary wireless network to allow more effective workflow. These events should be discussed, captured and, if needed, incorporated into an ICS wireless policy and program.

Unlike the use of wireless in the enterprise, which requires broader access to global resources, an ICS wireless typically can be engineered to support access only to specific hosts using specific, mostly ICS, protocols and users. In that way, ICS wireless limits abuse from weakened security capabilities, stolen security credentials or unknown protocol vulnerabilities.

VPN Interface

Challenges

VPN in an ICS covers both user level (remote operators, vendors and contractors) and system level. As remote access became popular, many system and machine builders began offering remote support capabilities to offload the cost of travel for support staff on different continents. This capability significantly improved the uptime and recovery of an organization's operations. However, the methods to implement it have been fraught with security issues and inconsistencies.

At a system level, VPN has become a recognizable function to enable protected site-to-site operations. Many of these sites have limited space or hostile industrial environmental conditions.

Coverage by Fortinet Solution

The FortiGate product has a ruggedized version specifically for hostile industrial environments. Its packaged solution delivers many features in a minimal footprint, which is highly desirable for ICS sites. Multifactor authentication (MFA) provided through FortiToken makes this feature more readily available for smaller organizations looking for an all-in-one type of solution.

People, Process and Technology

Many organizations have chosen to implement jump hosts for remote VPN users to have isolated access to ICS data and limited systems.

In most cases, VPN technology is protection from an untrusted network. Like all VPN solutions, a rigid process needs to be in place to design, implement, manage and maintain it. This process includes applying security updates and auditing configurations in a timely manner.

Similar to wireless networks, the use of VPNs in an ICS can be engineered to support access to only specific hosts using specific, mostly ICS, protocols and users. VPNs limit abuse from weakened security capabilities, stolen security credentials or unknown protocol vulnerabilities.

A jump host is used to reduce exposure of the remote user's device, while connected over VPN, to the local system. This dedicated host has restricted access to specific resources on the local ICS network, typically through the use of a firewall, and is also supplied with the tools required to accomplish the remote user's task. A well-architected VPN and jump host solution provide combined layers of defense.

This implementation has proven invaluable for remote users, such as vendors or contractors, and also has been utilized for contractors working on-premises to minimize the necessity for them to plug external laptops into the networks. A guest network is typically provided, placing the contractor back out to the internet and requiring them to remote back to the environment over a VPN and jump host solution. As a result, organizations' security teams are able to audit contractors while they perform on-premises activities.

Implementation Strategy

Many solutions cover many controls required by the target SL of any given security zone or conduit. Complicating things further, many options can be configured in support of an individual control. Achievement of a security level is, therefore, not as simple as it may appear in the Standard, even with the appropriate controls selected. A method to help determine whether a control is met can include:

- A thorough review of each and every option with the vendor to understand the features that support that control
- Assessment and measurement of the control by an internal or external team

Maintaining the control requires actively monitoring the control by questioning its ongoing necessity or identifying gaps against SL changes, maintaining a rigid change control process, and applying knowledge of vendor feature changes and updates. FortiManager can support these efforts.

Ultimately, an objective of determining at least some of the security zones and conduits is to apply network security monitoring activities. Most controls introduced into either security zones or conduits can produce information. When centralized, this information can be applied with context to the immediate and surrounding control, which then can be used as insight into early threat detection.

During a cybersecurity incident, additional countermeasures may need to be added to a control to either contain a threat or provide capability to maintain safe and reliable operations.

Summary

Vendors provide multiple security features in their products, but it can be difficult to tactically align those features to given security goals. It is common for an ICS to serve many different functions for an organization with different risk levels and criticality. For alignment, first understand what the varying security goals are at areas throughout the environment, and secondly, understand how to meet those goals without implementing every possible control for every possible area.

With guidance from IEC 62443 and implementation of Fortinet's solutions, one can approach the security of an ICS strategically. Evaluating assigned security levels within identified security zones and conduits against functional and system requirements provides a cohesive approach to security.

For informative papers related to this and many other ICS cybersecurity topics, please visit the SANS Reading Room.[5]

[5] SANS Reading Room, www.sans.org/reading-room/whitepapers/ICS

Appendix

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 1 – Identification and Authentication					**FR 1 Product Mapping: Fortigate, FortiWiFi/FortiAp, FortiAuthenticator, FortiToken, FortiClient, FortiEDR, FortiAnalyzer, FortiManager**		
FR 1 – SRs and REs	**Security Levels**				**Relevance**	**Compliance**	**Solution Description**
	SL 1	SL 2	SL 3	SL 4	IACS/Fortinet	Full/Partial/None	P: Product, C: Configuration, N: Note
SR 1.1 – Human user identification and authentication	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator C: Product(s) integration
SR 1.1 RE 1 – Unique identification and authentication		✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiToken C: Product(s) integration
SR 1.1 RE 2 – Multifactor authentication for untrusted networks			✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiToken C: Product(s) integration
SR 1.1 RE 3 – Multifactor authentication for all networks				✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiToken C: Product(s) integration
SR 1.2 – Software process and device identification and authentication		✔	✔	✔	Both	Full	P: FortiEDR, FortiClient, FortiGate C: Product(s) integration
SR 1.2 RE 1 – Unique identification and authentication			✔	✔	Both	Full	P: FortiEDR, FortiClient, FortiGate C: Product(s) integration
SR 1.3 – Account management	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration
SR 1.3 RE 1 – Unified account management			✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration
SR 1.4 – Identifier management	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration
SR 1.5 – Authenticator management	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration
SR 1.5 RE 1 – Hardware security for software process identity credentials			✔	✔	Both	Partial	N: Fortinet do not offer hardware security modules such as HSM or TPM for IACS; however, Fortinet product(s) has built-in feature to meet the requirement
SR 1.6 – Wireless access management	✔	✔	✔	✔	Both	Full	P: FortiAP/FortiWiFi, FortiGate, FortiAuthenticator C: Product(s) integration
SR 1.6 RE 1 – Unique identification and authentication		✔	✔	✔	Both	Full	P: FortiAP/FortiWiFi, FortiGate, FortiAuthenticator, FortiToken C: Product(s) integration
SR 1.7 – Strength of password-based authentication	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator C: Product(s) integration
SR 1.7 RE 1 – Password generation and lifetime restrictions for human users			✔	✔	Both	Full	P: FortiGate, FortiAuthenticator C: Product(s) integration
SR 1.7 RE 2 – Password lifetime restrictions for all users				✔	Both	Full	P: FortiGate, FortiAuthenticator C: Product(s) integration
SR 1.8 – Public key infrastructure certificates		✔	✔	✔	Both	Full	P: FortiGate C: PKI and digital certificate configuration within the product(s)
SR 1.9 – Strength of public key authentication		✔	✔	✔	Both	Full	P: FortiGate C: PKI and digital certificate configuration within the product(s)
SR 1.9 RE 1 – Hardware security for public key authentication			✔	✔	Both	Partial	N: Fortinet do not offer hardware security modules such as HSM or TPM for IACS; however, Fortinet product(s) has built-in feature to meet this requirement
SR 1.10 – Authenticator feedback	✔	✔	✔	✔	Both	Full	P: FortiGate C: Network traffic encryption if/where applicable
SR 1.11 – Unsuccessful login attempts	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiAnalyzer, FortiManager C: Product(s) integration
SR 1.12 – System use notification	✔	✔	✔	✔	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAnalyzer C: Product(s) integration
SR 1.13 – Access via untrusted networks	✔	✔	✔	✔	Both	Full	P: FortiGate C: Security policies
SR 1.13 RE 1 – Explicit access request approval		✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 2 – Use control (UC)					FR 2 Product Mapping: Fortigate, FortiWiFi/FortiAp, FortiAuthenticator, FortiToken, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, FortiSandbox, FortiSIEM		
FR 2 – SRs and REs	Security Levels				Relevance	Compliance	Solution Description
	SL 1	SL 2	SL 3	SL 4	IACS/Fortinet	Full/Partial/None	P: Product, C: Configuration, N: Note
SR 2.1 – Authorization enforcement	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration
SR 2.1 RE 1 – Authorization enforcement for all users		✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration
SR 2.1 RE 2 – Permission mapping to roles		✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration
SR 2.1 RE 3 – Supervisor override			✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration
SR 2.1 RE 4 – Dual approval				✔	Both	Partial	N: IACS asset owner or manufacturer or integrator need to ensure such capability is available within the IACS. Fortinet product(s) can complement with additional features e.g. Multi-factor authentication to meet the requirement
SR 2.2 – Wireless use control	✔	✔	✔	✔	Both	Full	P: FortiAP/FortiWiFi, FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration
SR 2.2 RE 1 – Identify and report unauthorized wireless devices			✔	✔	Both	Full	P: FortiAP/FortiWiFi, FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration
SR 2.3 – Use control for portable and mobile devices	✔	✔	✔	✔	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration
SR 2.3 RE 1 – Enforcement of security status of portable and mobile devices			✔	✔	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration
SR 2.4 – Mobile code	✔	✔	✔	✔	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAnalyzer, FortiSandbox C: Product(s) integration
SR 2.4 RE 1 – Mobile code integrity check			✔	✔	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAnalyzer, FortiSandbox C: Product(s) integration
SR 2.5 – Session lock	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration
SR 2.6 – Remote session termination		✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration
SR 2.7 – Concurrent session control			✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration
SR 2.8 – Auditable events	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiAnalyzer, FortiManager C: Product(s) integration
SR 2.8 RE 1 – Centrally managed, systemwide audit trail			✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiAnalyzer, FortiManager, FortiSIEM C: Product(s) integration
SR 2.9 – Audit storage capacity	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiAnalyzer, FortiManager C: Product(s) integration
SR 2.9 RE 1 – Warn when audit record storage capacity threshold reached			✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiAnalyzer, FortiManager C: Product(s) integration
SR 2.10 – Response to audit processing failures	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiAnalyzer, FortiManager C: Product(s) integration
SR 2.11 – Timestamps		✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiAnalyzer, FortiManager C: Product(s) integration
SR 2.11 RE 1 – Internal time synchronization			✔	✔	Both	Full	P: FortiGate N: The product can function as NTP server to provide time to the network connected assets; however, it may not be suitable for real-time time synchronization requirements within the IACS
SR 2.11 RE 2 – Protection of time source integrity				✔	Both	Full	P: FortiGate N: Capability is limited to the product(s) and any assets connected to/via the product(s)
SR 2.12 – Non-repudiation			✔	✔	Both	Full	P: FortiGate N: Capability is limited to the product(s) and any assets connected to/via the product(s)
SR 2.12 RE 1 – Non-repudiation for all users				✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiAnalyzer, FortiManager C: Product(s) integration

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 3 – System integrity (SI)					**FR 3 Product Mapping: Fortigate, FortiWiFi/FortiAp, FortiAuthenticator, FortiToken, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, FortiSandbox, FortiSIEM, FortiTester, FortiResponder**		
FR 3 – SRs and REs	**Security Levels**				**Relevance**	**Compliance**	**Solution Description**
	SL 1	SL 2	SL 3	SL 4	IACS/Fortinet	Full/Partial/None	P: Product, C: Configuration, N: Note
SR 3.1 – Communication integrity	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiAnalyzer, FortiManager C: Product(s) integration
SR 3.1 RE 1 – Cryptographic integrity protection			✔	✔	Both	Full	P: FortiGate, FortiAnalyzer, FortiManager C: Product(s) integration
SR 3.2 – Malicious code protection	✔	✔	✔	✔	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAnalyzer, FortiSandbox C: Product(s) integration
SR 3.2 RE 1 – Malicious code protection on entry and exit points		✔	✔	✔	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAnalyzer, FortiSandbox C: Product(s) integration
SR 3.2 RE 2 – Central management and reporting for malicious code protection			✔	✔	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAnalyzer, FortiManager, FortiSandbox C: Product(s) integration
SR 3.3 – Security functionality verification	✔	✔	✔	✔	Both	Full	P: FortiTester and FortiResponder N: The product can be offered as a service
SR 3.3 RE 1 – Automated mechanisms for security functionality verification			✔	✔	Both	Full	P: FortiTester, FortiResponder N: The product can be offered as a service
SR 3.3 RE 2 – Security functionality verification during normal operation				✔	Both	Full	P: FortiTester, FortiResponder N: The product can be offered as a service
SR 3.4 – Software and information integrity	✔	✔	✔	✔	Both	Full	P: FortiTester, FortiResponder N: The product can be offered as a service
SR 3.4 RE 1 – Automated notification about integrity violations			✔	✔	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAnalyzer C: Product(s) integration
SR 3.5 – Input validation	✔	✔	✔	✔	Both	Partial	N: Fortinet product(s) are compliant with the requirement; however, IACS asset owner or manufacturer or integrator need to ensure the capability is also available within the IACS.
SR 3.6 – Deterministic output	✔	✔	✔	✔	Both	Partial	N: Fortinet product(s) are compliant with the requirement; however, IACS asset owner or manufacturer or integrator need to ensure the capability is also available within the IACS.
SR 3.7 – Error handling		✔	✔	✔	Both	Partial	N: Fortinet product(s) are compliant with the requirement; however, IACS asset owner or manufacturer or integrator need to ensure the capability is also available within the IACS.
SR 3.8 – Session integrity		✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiToken, FortiAnalyzer, FortiManager C: Product(s) integration
SR 3.8 RE 1 – Invalidation of session IDs after session termination			✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiToken, FortiAnalyzer, FortiManager C: Product(s) integration
SR 3.8 RE 2 – Unique session ID generation			✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiToken, FortiAnalyzer, FortiManager C: Product(s) integration
SR 3.8 RE 3 – Randomness of session IDs				✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiToken, FortiAnalyzer, FortiManager C: Product(s) integration
SR 3.9 – Protection of audit information		✔	✔	✔	Both	Full	C: Restrict access to the Fortinet product(s) that offer centralized logging and monitoring capability
SR 3.9 RE 1 – Audit records on write-once media				✔	Both	Full	C: Restrict access to the Fortinet product(s) that offer centralized logging and monitoring capability

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 4 – Data confidentiality (DC)					FR 4 Product Mapping: Fortigate		
FR 4 – SRs and REs	Security Levels				Relevance	Compliance	Solution Description
	SL 1	SL 2	SL 3	SL 4	IACS/Fortinet	Full/Partial/None	P: Product, C: Configuration, N: Note
SR 4.1 – Information confidentiality	✔	✔	✔	✔	Both	Full	P: FortiGate C: Using the product(s), implement encryption of relevant information in transit
SR 4.1 RE 1 – Protection of confidentiality at rest or in transit via untrusted networks		✔	✔	✔	Both	Full	P: FortiGate C: Using the product(s), implement encryption of relevant information in transit for untrusted networks
SR 4.1 RE 2 – Protection of confidentiality across zone boundaries				✔	Both	Full	P: FortiGate C: Using the product(s), implement protection/encryption of relevant information in transit between the zones
SR 4.2 – Information persistence		✔	✔	✔	Both	Partial	N: IACS asset owner or manufacturer need to ensure such capability is available within the IACS. Fortinet product(s) has built-in capability to meet the requirement.
SR 4.2 RE 1 – Purging of shared memory resources			✔	✔	Both	Partial	N: IACS asset owner or manufacturer need to ensure such capability is available within the IACS. Fortinet product(s) has built-in capability to meet the requirement.
SR 4.3 – Use of cryptography	✔	✔	✔	✔	Both	Partial	N: IACS asset owner or manufacturer need to ensure such capability is available within the IACS. Fortinet product(s) has built-in capability to meet the requirement.

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 5 – Restricted data flow (RDF)					FR 5 Product Mapping: FortiGate, FortiSwitch, FortiNAC, FortiClient, FortiEDR, FortiAnalyzer		
FR 5 – SRs and REs	Security Levels				Relevance	Compliance	Solution Description
	SL 1	SL 2	SL 3	SL 4	IACS/Fortinet	Full/Partial/None	P: Product, C: Configuration, N: Note
SR 5.1 – Network segmentation	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiNAC C: Product(s) integration and implementation of zones and conduits within Layer 3 and/or Layer 2 networks
SR 5.1 RE 1 – Physical network segmentation		✔	✔	✔	IACS	None	N: IACS asset owner or manufacturer or integrator need to ensure physical network segmentation for relevant IACS assets
SR 5.1 RE 2 – Independence from non-control system networks			✔	✔	Both	Full	P: FortiGate, FortiNAC C: Products(s) integration and implementation of zones and conduits within Layer 3 and/or Layer 2 networks
SR 5.1 RE 3 – Logical and physical isolation of critical networks				✔	Both	Full	P: FortiGate, FortiNAC C: Product(s) integration and implementation of zones and conduits within Layer 3 and/or Layer 2 networks. Applicable for logical segmentation
SR 5.2 – Zone boundary protection	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiNAC, FortiAnalyzer C: Product(s) integration and implementation of zones and conduits within Layer 3 and/or Layer 2 networks and centralized logging and monitoring
SR 5.2 RE 1 – Deny by default, allow by exception		✔	✔	✔	Both	Full	P: FortiGate, FortiNAC, FortiAnalyzer C: Product(s) integration and implementation of zones and conduits within Layer 3 and/or Layer 2 networks
SR 5.2 RE 2 – Island mode			✔	✔	IACS	Partial	N: The requirement is applicable for IACS. Fortinet product(s) can offer such capability.
SR 5.2 RE 3 – Fail close			✔	✔	IACS	Partial	N: The requirement is applicable for IACS. Fortinet product(s) can offer such capability.
SR 5.3 – General purpose person-to-person communication restrictions	✔	✔	✔	✔	Both	Full	P: FortiGate C: Using the product(s), implement deny all network communication except allowed by the security policy
SR 5.3 RE 1 – Prohibit all general purpose person-to-person communications			✔	✔	Both	Full	P: FortiGate C: Using the product(s), implement deny all network communication except allowed by the security policy
SR 5.4 – Application partitioning	✔	✔	✔	✔	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAnalyzer C: Product(s) integration

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 6 – Timely response to events (TRE)					FR 6 Product Mapping: FortiGate, FortiClient, FortiEDR, FortiAnalyzer, FortiManager		
FR 6 – SRs and REs	Security Levels				Relevance	Compliance	Solution Description
	SL 1	SL 2	SL 3	SL 4	IACS/Fortinet	Full/Partial/None	P: Product, C: Configuration, N: Note
SR 6.1 – Audit log accessibility	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiAnalyzer, FortiManager C: Product(s) integration
SR 6.1 RE 1 – Programmatic access to audit logs			✔	✔	Both	Full	P: FortiAnalyzer C: Integration with IACS may be required for provisioning access to the logging and monitoring information available within Fortinet product(s) e.g. via syslog etc
SR 6.2 – Continuous monitoring		✔	✔	✔	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAnalyzer, FortiManager C: Product(s) integration

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 7 – Resource availability (RA)					FR 7 Product Mapping: FortiGate, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, Fabric-Ready Partner Solutions		
FR 7 – SRs and REs	Security Levels				Relevance	Compliance	Solution Description
	SL 1	SL 2	SL 3	SL 4	IACS/Fortinet	Full/Partial/None	P: Product, C: Configuration, N: Note
SR 7.1 – Denial of service protection	✔	✔	✔	✔	Fortinet	Full	P: FortiGate C: Using the product(s), implement DoS protection policies
SR 7.1 RE 1 – Manage communication loads		✔	✔	✔	Fortinet	Full	P: FortiGate C: Using the product(s), implement DoS protection, SYN flood protection, rate-limit, traffic shaping policies
SR 7.1 RE 2 – Limit DoS effects to other systems or networks			✔	✔	Fortinet	Full	P: FortiGate C: Using the product(s), implement DoS protection, SYN flood protection, rate-limit policies
SR 7.2 – Resource management	✔	✔	✔	✔	Both	Full	P: FortiGate C: Using the product(s), implement, rate-limit and connection restriction policies
SR 7.3 – Control system backup	✔	✔	✔	✔	Both	Partial	P: FortiEDR Manager, FortiAnalyzer, FortiManager, Fabric-Ready Partner Solutions C: The product(s) support configuration backup for Fortinet products and can be integrated with Fabric-Ready partner solutions that offer capability to meet the requirement. IACS asset owner or manufacturer or integrator need to ensure the capability is also available within the IACS
SR 7.3 RE 1 – Backup verification		✔	✔	✔	Both	Partial	P: FortiEDR Manager, FortiAnalyzer, FortiManager, Fabric-Ready Partner Solutions C: The product(s) support configuration backup for Fortinet products and can be integrated with Fabric-Ready partner solutions that offer capability to meet the requirement. IACS asset owner or manufacturer or integrator need to ensure the capability is also available within the IACS
SR 7.3 RE 2 – Backup automation			✔	✔	Both	Partial	P: FortiEDR Manager, FortiAnalyzer, FortiManager, Fabric-Ready Partner Solutions C: The product(s) support configuration backup for Fortinet products and can be integrated with Fabric-Ready partner solutions that offer capability to meet the requirement. IACS asset owner or manufacturer or integrator need to ensure the capability is also available within the IACS
SR 7.4 – Control system recovery and reconstitution	✔	✔	✔	✔	Both	Partial	P: FortiEDR Manager, FortiAnalyzer, FortiManager, Fabric-Ready Partner Solutions C: The product(s) support configuration backup for Fortinet products and can be integrated with Fabric-Ready partner solutions that offer capability to meet the requirement. IACS asset owner or manufacturer or integrator need to ensure the capability is also available within the IACS
SR 7.5 – Emergency power	✔	✔	✔	✔	Both	Partial	N: Fortinet product(s) are available with redundant power inputs/supplies and can be configured in high-availability and fault-tolerant configuration. IACS asset owner or manufacturer or integrator need to ensure the capability is also available within the IACS.
SR 7.6 – Network and security configuration settings	✔	✔	✔	✔	Both	Full	P: FortiGate N: Fortinet product(s) support baseline configuration and dedicated management interface for configuration and operations management
SR 7.6 RE 1 – Machine-readable reporting of current security settings			✔	✔	Both	Full	P: FortiAnalyzer, FortiManager C: Product(s) integration
SR 7.7 – Least functionality	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiEDR, FortiClient C: Product(s) integration and implementation of security policies to restrict unnecessary functions/ports/protocols/services
SR 7.8 – Control system component inventory		✔	✔	✔	Both	Full	P: FortiGate, FortiAnalyzer, Fabric-Ready Partner Solutions C: Product(s) integration

About the Author

Jason Dely, SANS co-author of ICS612: ICS Cybersecurity In-Depth and instructor for ICS515: ICS Active Defense and Incident Response, has 20 years of operational, technical and security experience, spanning multiple industry verticals, such as power utility, water utility, oil and gas, manufacturing, mining and chemical. He contributes to developing and implementing technical components of the SANS ICS and SCADA product offerings. Jason is also the principal consultant and founder at Northern Strong Security Inc., based in Ontario, Canada.

Sponsor

SANS would like to thank our sponsor for this paper:

FORTINET®