SANS

Analyst Program

Whitepaper

Effective ICS Cybersecurity Using the IEC 62443 Standard

Companion piece to "Managing ICS Security With IEC 62443"

Written by **Jason Dely**

Originally Published November 2020
Updated June 2023

FORTINET

Many owners and operators of industrial control systems (ICSs) recognize the need to both improve and effectively manage ICS cybersecurity. An abundance of security issues and vulnerabilities lurks within an ICS, mainly an effect of designing, deploying, and operating these systems on legacy technologies, methodologies, and ideologies. Today, ideologies are changing somewhat, but because the core ICS technologies have not evolved, movement is slow. Clear and present dangers such as remote access and attacks targeting ICSs have forced our methodologies to adapt but only to the extent that cultural, workforce, and technological limitations will allow. It is easy enough to investigate these systems and scrutinize their security, but equal attention must be given to the complexities and difficulties that operations staff deal with when operating these large, complex controls and, likely, the physical systems they are expected to run 24/7. For critical infrastructure, this means continuous delivery of service. The problem becomes not just managing cybersecurity issues but also managing operational risk and, by extension, cybersecurity issues.

A focus on identification and remediation of cybersecurity issues without understanding their relationship to operational risks reduces the security problem to a list of findings that represent a mere slice of the entire ICS cybersecurity posture. After a review of these findings, mitigations can take anywhere from one to three years to complete, based on factors such as current ICS cybersecurity maturity, agility, and available budget. By then, it's time for a whole new assessment, despite the lack of any measure of how those previous efforts benefited security or ensured the operational effectiveness under threat of a cyberattack. Some necessary improvements may get implemented, but what's missing is cohesion.

Making ICS cybersecurity improvements is not just about addressing weaknesses by adding security countermeasures. Countermeasures should be carefully selected for effectiveness in mitigating ICS operational risk and for their ability to complement ongoing security operations as they strive to maintain those mitigations and thwart active threats. The countermeasures should collectively support a clear understanding of how to prevent, monitor, detect, and respond to cybersecurity incidents. Improving cybersecurity across the ICS cannot be placed into a simple, sequential road map of phases. Ideally, depending on the security requirements identified during an ongoing risk assessment process, the ICS should be segmented into security zones that may operate at different phases of maturity.

IEC 62443 (hereafter referred to as "the standard" in this paper) is a set of ICS cybersecurity standards written by ICS experts for ICS owners, manufacturers, and integrators across a range of applications and sectors. The standard provides advice on designing an ICS cybersecurity program and technical guidance that fosters a cohesive approach to security, one that considers the varying phases of the maturity of an organization's ICS cybersecurity program. Using a step-by-step process incorporating maturity phases, the standard outlines a life-cycle approach as part of an ICS 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 throughout their ICS environment.

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

Overview of IEC 62443

IEC 62443-3-2 separates an ICS organization into security zones and conduits based on assessment of risks. The standard provides guidance on how to select or design the zones and conduits and how to assign a security level (SL). Certain countermeasures are required to meet each SL. A typical ICS owner and operator 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.

Even when an organization separates its ICS environments into multiple zones, perfect risk isolation is never possible 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 with operational relationships to those services. Second, a zone compromise brings a threat closer to other zones because communication pathways likely exist between zones. To overcome these challenges, the standard introduces a special type of zone called a "communications conduit" (hereafter referred to as a "conduit"). By identifying and analyzing the communication channels present within these conduits, an organization can determine the appropriate level of communications protection within and between zones.

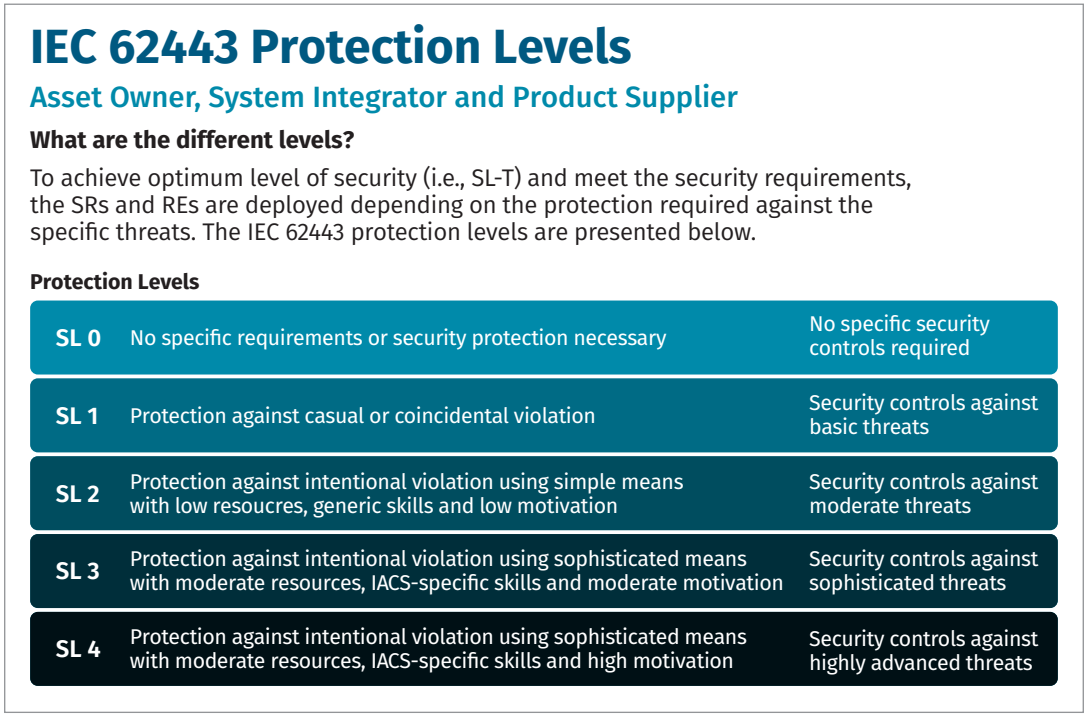

Figure 1. IEC 62443 Security Levels

Getting Started with IEC 62443

The standard provides an entire process for establishing an ICS security program, which it calls the "cybersecurity management system" (CSMS). This paper focuses on the high-level relationship of the elements that make up the CSMS: risk analysis, addressing risk with CSMS, and monitoring and improving the CSMS.

As mentioned in the introduction, cybersecurity is a tool to help manage an organization's risk to its ICS environment. Such management requires clearly understanding the risks in order to select and deploy effective countermeasures. The process outlined in the standard includes many steps, but some key ones are highlighted in this paper. A high-level risk assessment, for example, will identify the financial, health, safety, and environmental impacts based on a compromised ICS. This critical step will bring clarity to the organization on what a bad day would look like for each risk. With this knowledge, the organization can create a prioritized list of each risk to help focus efforts and resources during or after assessing the vulnerabilities in the environment. Risk to the organization is not static and can change as a result of internal and external influences. The risk process must be triggered periodically and in response to risk-relevant events, such as changes in the system's design or functionality, new threats, and organization changes.

The CSMS addresses risk over three parallel approaches: security policy and awareness, security countermeasures, and implementation. The security policy and awareness approach is often overlooked in many ICS cybersecurity activities. Consider, too, that security policies are not only present to ensure that people are behaving as expected; they can also be used to help maintain the effectiveness of implemented countermeasures. For example, many firewalls have been deployed into an ICS network that later lost effectiveness mainly because there was no enforcement from the organization to ensure rules were deployed and/or removed through a rigid, repeatable process.

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 with an assumed risk mitigation goal already in place.

Following a CSMS ensures a natural cohesion that ultimately improves the entirety of ICS cybersecurity posture.

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

Security Levels

The organization must determine its desired SL for each security zone and work toward achieving it. In other words, if the organization wants to achieve an SL of 4, it must ensure that the implementers of the security controls are aware of the organization's goal so it can achieve that level.

Figure 2 depicts how a segmented approach may look more complex than a monolithic approach but is simpler and more effective because it breaks things down into smaller, more focused, and more cost-effective pieces.

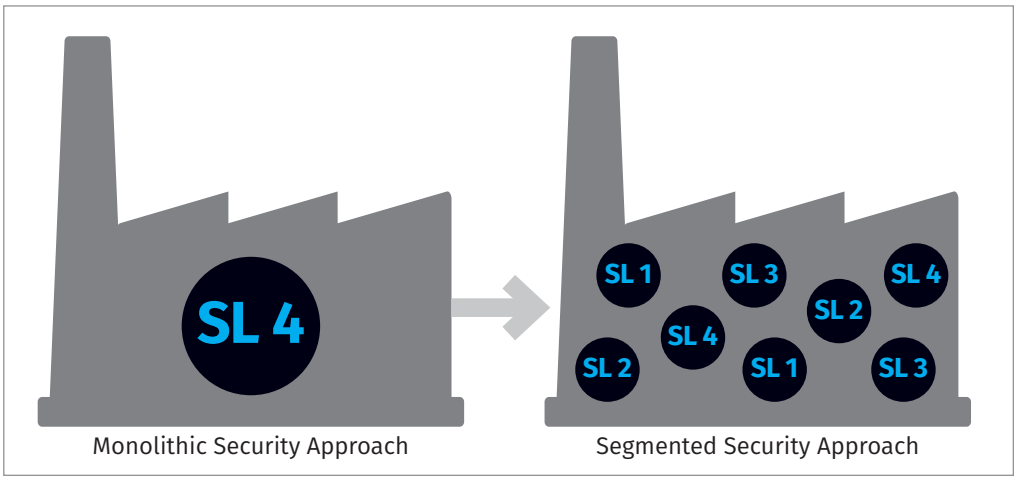

Figure 2. Monolithic vs. Segmented SL Measurements Across an Environment

The monolithic approach is more difficult to achieve and maintain because every zone needs to be brought to SL 4, which requires extensive countermeasure implementation, management, and overall cost to the ICS cybersecurity program. The monolithic security approach may very well be necessary, but most ICS environments contain many inconsistences in technology, people, and processes that introduce nuisances that will greatly affect the implementation time and outcome if overlooked. These nuisances can include countermeasure incompatibilities and operational differences between systems and teams. Diminishing (or eliminating) the nuisances associated with operational and technical differences, onboarding, and training will take time and needs to be factored into the CSMS.

The segmented security approach, shown on the right in Figure 2, allows for measurable effectiveness of the implemented changes across the environment and provides an opportunity to map out a maturity strategy for the organization to achieve and manage its identified risk-based objectives within financial resources.

IEC62443-3-3 categorizes seven foundational requirements (FRs), expanded into a series of system requirements (SRs) and requirement enhancements (REs). See Figure 3.

Foundational Requirements (FRs)	Example High-Level Operational Controls Mapping to FRs
FR1 Identification and authentication control (IAC)	**FR1** Passwords and user authentication
FR2 Use control (UC)	**FR2** User roles and authorization enforcement (RBAC)
FR3 System integrity (SI)	**FR3** Session handling, mechanism to recognize change
FR4 Data confidentiality (DC)	**FR4** Encryption
FR5 Restricted data flow (RDF)	**FR5** Network segmentation
FR6 Timely response to events (TRE)	**FR6** Logging and monitoring
FR7 Resource availability (RA)	**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

The standard provides a chart to map these SRs and REs to SLs 1 to 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 needs. Potentially, the SLs may need to be modified depending on the differences in each security zone in threats, operational changes, and technology used (industrial IoT, for example), all of which 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 changes to the threat landscape. This is why an organization's risk analysis process should be triggered periodically and after every risk-relevant event. By doing so, the organization is tracking security risks, and the list of applicable SRs is always current to keep the organization in an actively defendable posture.

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	✔	✔	✔	✔

Monitoring and improving the CSMS is crucial to ensure and measure the overall effectiveness of the ICS cybersecurity posture. This step in the CSMS can be a once-per-year activity, but organizations are encouraged to perform it at any time to ensure conformance and effectiveness. Conformance validates that the steps to address the risk have been taken. Measuring the assigned SL of each defined security zone with the seven FRs as well as the SRs and REs provides a more granular perspective on the defensive posture of each security zone. The act of measuring can also provide an opportunity to apply the MITRE ATT&CK® for ICS Matrix to analyze the applicability of tactics, techniques, and procedures (TTP) and behaviors used by threat activity groups against each security zone's countermeasures, existing or absent.[1,2] The sidebar called "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 require using many 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 that may benefit other security zones as well as the analysis of the TTP or behaviors of relevant threat activity groups. A detailed cybersecurity risk assessment, in which a target SL (SL-T) per zone is established and the countermeasures that will help one zone get to the desired SL-T are highlighted, could also benefit other security zones, potentially maximizing the investment of time and effort.

Introduce countermeasures that meet an assessment report's specific risk-reduction recommendations but also review all security zone requirements because the selected countermeasure may be advantageous across multiple security zones, including those outside the immediate scope of the assessment. Additionally, when selecting countermeasures, identify opportunities where countermeasures can provide capabilities in detection and response activities as well as in protection. 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 be useful in future identified countermeasures.

[1] "MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy," March 2020, https://attack.mitre.org/docs/ATTACK_for_ICS_Philosophy_March_2020.pdf

[2] "Threat Analytics and Activity Groups," February 26, 2018, www.dragos.com/blog/industry-news/threat-analytics-and-activity-groups

Zones, Subzones, and Conduits

Each security zone and conduit is assigned a target SL, or SL-T. To reach what the standard considers a satisfactory security level (an 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. As written in the standard, these factors are complex and difficult to implement, but many factors can impact the effectiveness of selected countermeasures. This is why it is important not only to select and validate the countermeasures but also to consider the implications when deciding on those measures. For example, an organization might want to examine the impact of countermeasure function dependency on a compromised service in a different security zone. As important as it is to choose a countermeasure that allows us to achieve a specific security level and risk mitigation, it is equally important to evaluate the residual or introduced risk when using these countermeasures.

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 SL-A

These factors must be considered when establishing security zones and conduits, as well as their respective security levels for each FR. As we will discuss, 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.

The Purdue Model: Reference Architecture for IEC 62443

What is commonly referred to as the Purdue Reference Model is derived from the Purdue Enterprise Reference Architecture (PERA), which is based on principles established by the Purdue Laboratory for Applied Industrial Control (PLAIC). It functions as a reference architecture for the standard. The use and assignment of the application-related levels can be referenced back to its roots in a 220-page 1989 ISA publication, "PERA Reference Model for Computer Integrated Manufacturing (CIM)."[3] That 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" meaning 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 still valid today, especially from the perspective of the value of data in the 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 an 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 on the next page)—and likely even in 1989—is not meant to exactly mirror all organizations' ICS network architectures under the same construct, but rather serves as a tool that can be used to describe, educate, and leverage for innovative problem solving.

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

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, along with concepts that organizations can build upon to solve and improve ICS security challenges. One of the more powerful concepts that provides a foundation of security when thoughtfully applied is that of security zones, subzones, and conduits. Security zones are the basis for segmenting an ICS.

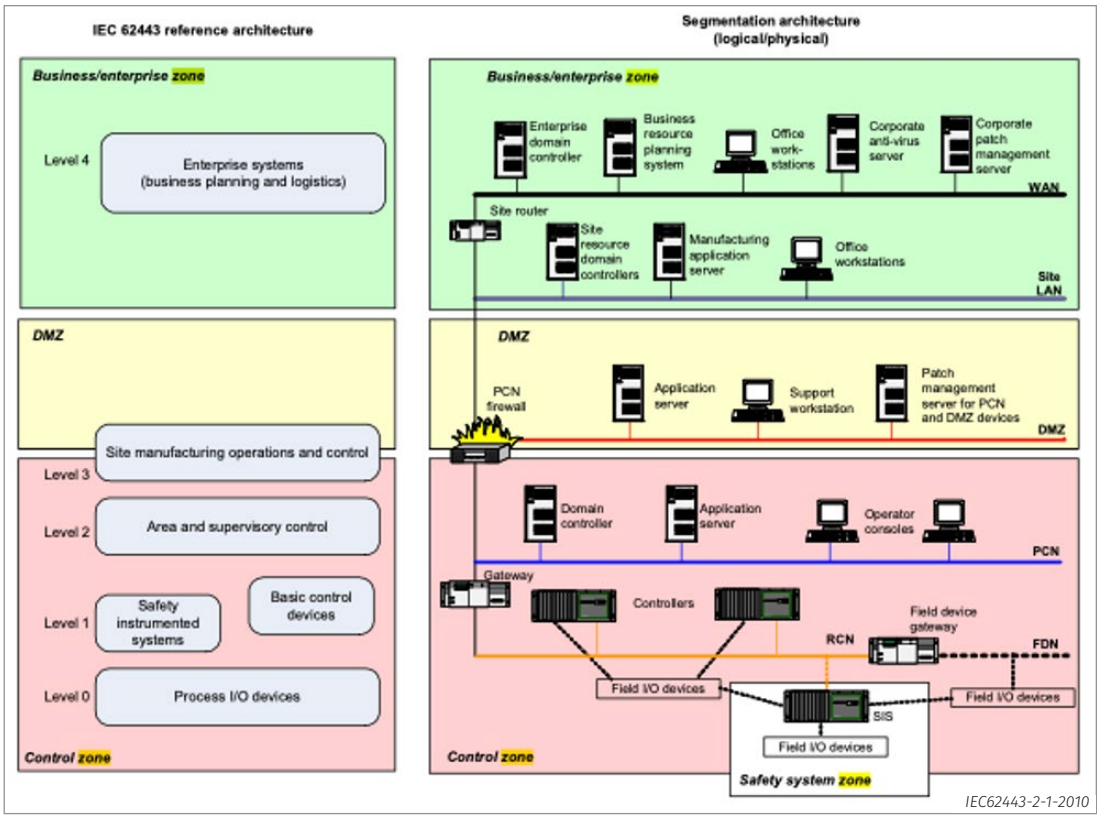

Figure 5. Reference Architecture Alignment with an Example Segmentation Architecture

An ICS is best described as a system of systems. Differing by sector and industry type, an ICS can be broken down conceptually into smaller operational asset groupings of three interdependent asset types:

1. Physical systems, such as machines, that perform specific operations
2. Application, such as a collection of ICS devices, networks, and software, orchestrated together to perform specific operational function or share direct operational risk
3. Data, such as pressure values or work order details, that may be generated within or may flow from or to other groups

An operational asset group should represent the smallest autonomous operation for the organization. Multiple operational asset groups make up the overall plant or factory operations. When defining these operational asset groups, assign a level of consequence or severity from impact used to derive the SL. The assignment of consequence or severity considers operational, financial, health, safety, and environmental factors. A security zone will be an individual operational asset group or a collection of operational asset groups that share a common security requirement (in this case, an SL) or goal, and can be logically brought together and concealed into a logical boundary. Figure 6 presents these groupings.

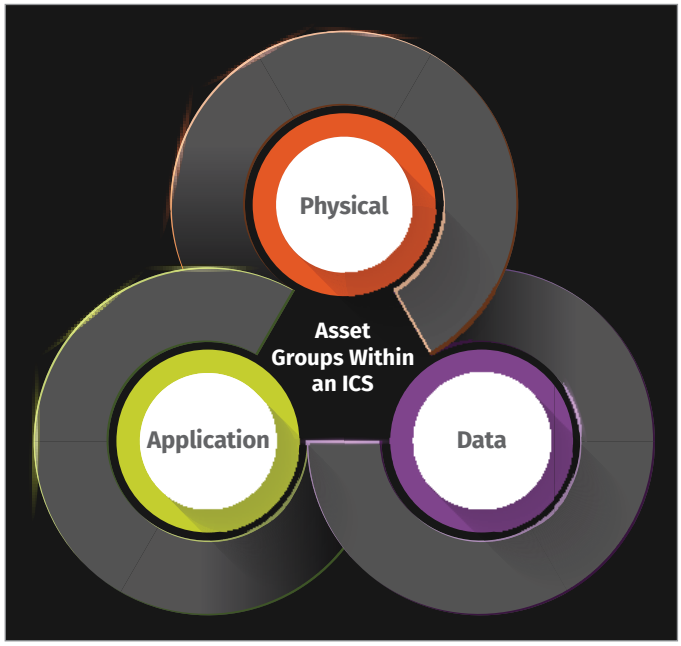

Figure 6. Three Asset Groups Within an ICS

An ICS may be structured where an operational asset group, 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.

There are situations where information must flow within, into, and out of a security zone by means of conduits. Conduits facilitate grouped communication links (channels) established to move information within and between zones. This includes, but is not limited to, the intermittent communications among programming terminals, mobile devices, portable media devices, and vendor connections. Conduits and channels can be identified as trusted or untrusted. Conduits that do not cross zone boundaries are largely recognized as trusted. Untrusted channels or conduits are determined when either party is not at the same security level as the reference zone. A channel inherits the security properties of the conduit from the perspective of communications media. However, with the use of secure communications capabilities, a trusted conduit or channel can virtually extend a security zone. A thorough study of communications between zones and endpoints is necessary for determining the appropriate selection and deployment of countermeasures. The illustration in Figure 7 is an example of the relationships between security zones and conduits.

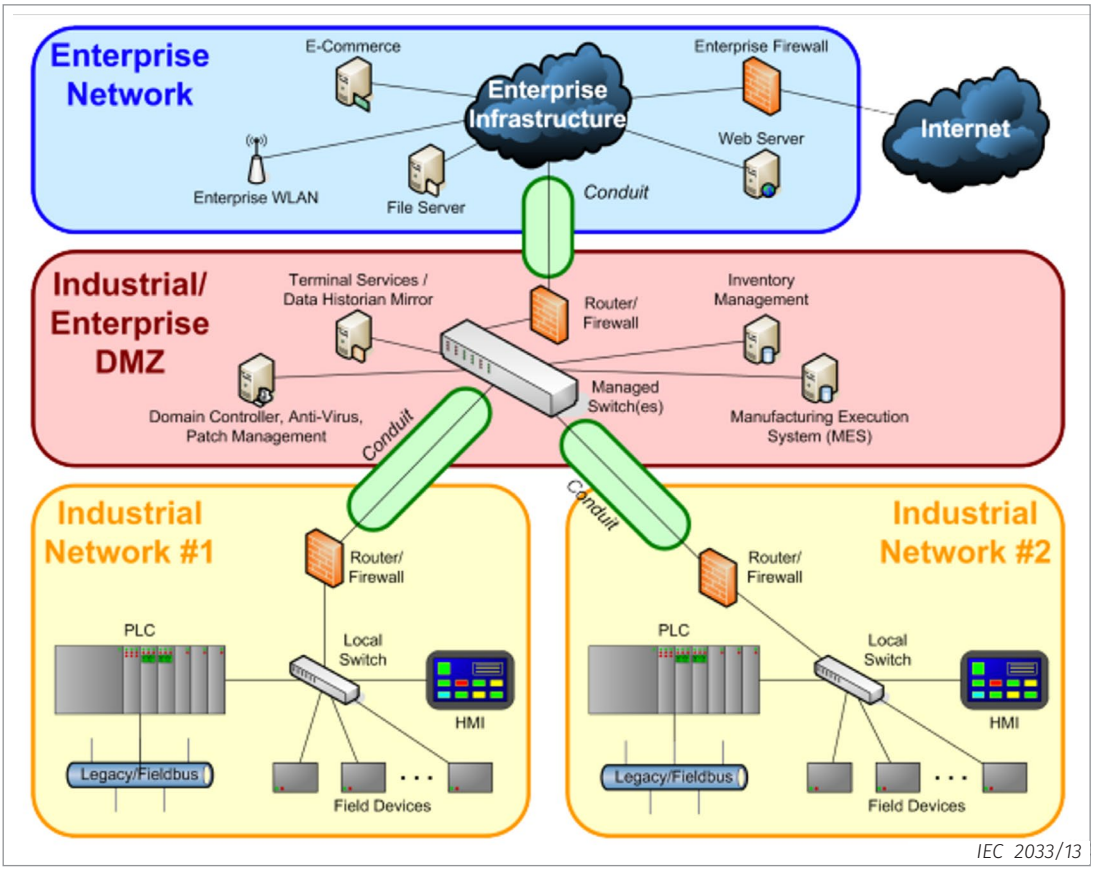

Figure 7. High-Level Manufacturing Example Showing Zones and Conduits

For many organizations, segmentation is a challenge, especially if a brownfield facility needs to implement a current deployment of ICS technologies. This is why zones should be abstracted, without too much focus on the actual hardware and software. Only after SLs are applied should the actual ICS technologies (such as network gear, PLCs, drives, computers, firewalls, services, protocols, etc.) be overlaid. This process will clearly depict all the shared hardware, network paths, and software between zones in the environment. When zones share technologies, the assigned SL between those zones must adopt the higher SL to align the risk-reduction requirements to the

consequence and severity protections requirements. This information can identify technology segmentation and realignment 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 less security controls.
- Hierarchal zoning and subzoning provide architectural defense in depth.
- Zone and subzone boundaries provide north-south and east-west choke points for network security monitoring.
- ICS, network, and software application segmentation can introduce additional security cost/benefit opportunities.
- Use of network access control at Layer 2 can help extend zone boundary controls.

Examples of Segmentation Challenges

Let's say that a vendor of distributed control systems (DCSs) provides a turnkey solution with a tightly controlled architecture of computers, software, network, and programmable automation controllers. 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 its offering. The DCS vendor's client organizations should review the SLs, FRs, and SRs with the vendor. Otherwise, their segmenting efforts should be applied to systems outside of, but providing production service to, the DCS-controlled production assets, including boundaries for individual DCS and non-DCS production assets and any safety instrumented systems that may exist outside of the DCS scope.

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.

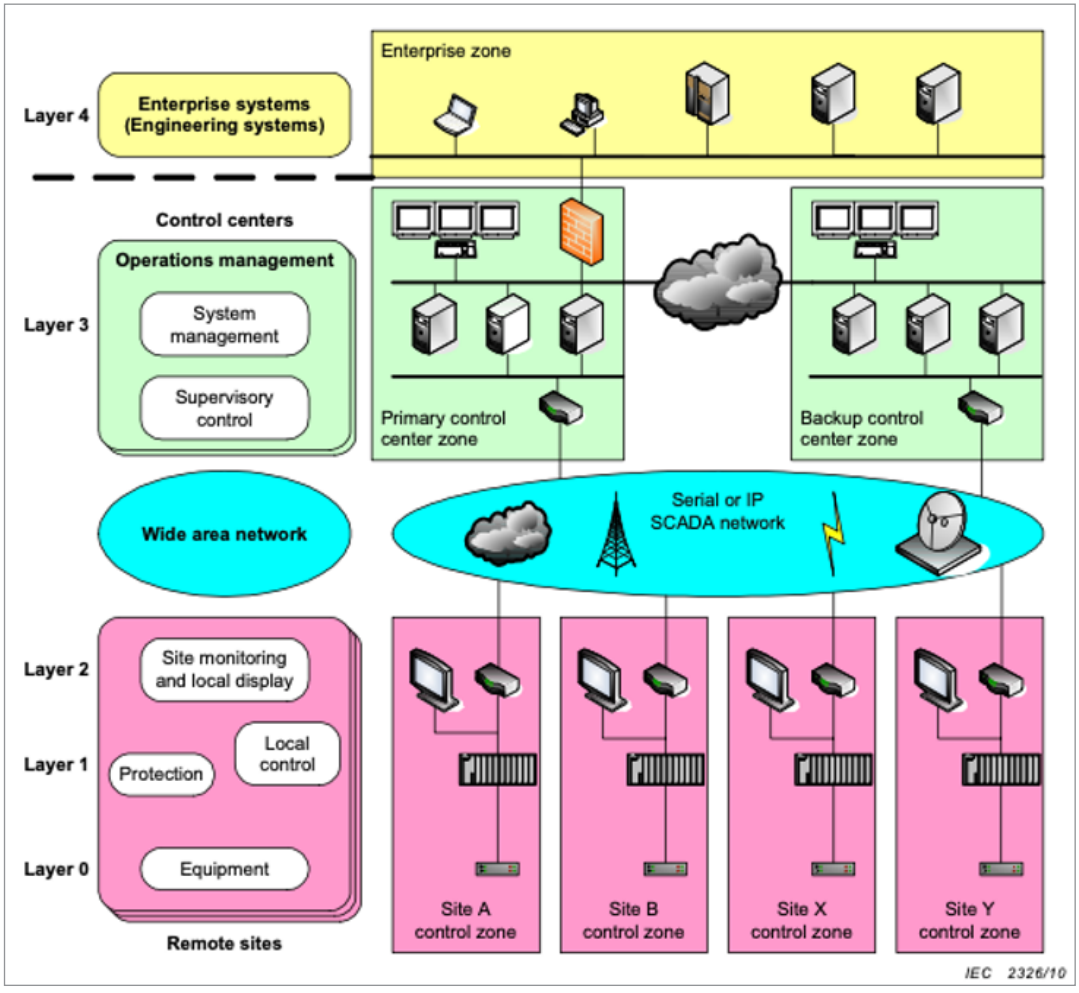

Figure 8. Reference SCADA Architecture Alignment with a Sample Segmented Architecture

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

Manufacturing environments (see Figure 7) 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. Many information systems, such as enterprise resource planning (ERP) systems, manufacturing execution systems (MESs), laboratory information management systems (LIMSs), and warehouse management systems (WMSs), are tightly coupled with the enterprise, making it difficult to build independent hierarchal zones for defense in depth. The intercommunication relationships between these systems and the ICS can be complex, with no clear boundaries for segmentation from an ideal ICS secure network design perspective. Using switches with role-based and network access control capabilities to produce multiple subzones in existing and new environments may be an effective segmentation strategy.

Lastly, legacy systems were engineered to optimize cost and uptime efficiencies, usually with no consideration of 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 control systems is expensive and results in fewer assignable security zones, with possibly more assets, which might require higher security levels. Hence, identifying the zones as if the control systems will need to be replaced at some time can be useful for future planning.

Countermeasure Challenges

After the security zones and conduits are identified, along with their respective SLs and associated requirements, the review and implementation of controls can commence.

Unlike common IT technologies used within an ICS (such as Windows OS), the security controls that can be applied to ICS technologies are limited by what is provided by the ICS vendors. Adding additional security agents and software to embedded ICS technologies is rarely an option. Vendors may provide security patches to their devices, but protection of security zones must move beyond a vulnerability-based approach and consider threat behavioral analytics for maintaining protection. Understanding this protection approach will demonstrate how Fortinet aids threat behavioral analytics through its FortiSIEM products.

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, from the perspective of the standard, center on the following 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 via a wired connection, a wireless network, or a VPN interface. Additionally, each wireless interface and VPN interface was treated as an independent controlled access point. In this way, whether a communication path comes through either a wireless network or a VPN, it must transact two control access points; the first to access either the wireless network 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 either wireless networks or VPNs, as applicable.

The complete breakdown of the product review analysis can be found in the appendix.

Threat Behavioral Analytics Protection

Challenges

Multiple challenges must be overcome to maintain security-patch levels within an ICS. The obvious area of focus in this vulnerability-based protection is the common IT technologies used (such as Windows servers). These technologies have a continuous flow of patches to address proactively discovered vulnerabilities and reactively respond to discovered security flaws in these systems. A recognized and trusted mechanism exists to automatically maintain the security patch levels of deployed systems. Unfortunately, the uptime, integrity, and, in some cases, regulatory demands of ICSs require a rigorous and costly testing and acceptance process for changes (including patching) made to these systems. This is true for both DCS and non-DCS systems.

Common IT technologies make up only a small number of the overall networked ICS assets. Those other assets are a mix of embedded devices running proprietary versions of embedded OS and real-time operating systems (RTOSs). These devices may have fewer (but a growing number of) vulnerabilities, yet patch maintenance is even more challenging to maintain. Most attacks utilize the capabilities and technologies already built into the environment. And the known attacks that have caused disruption or destruction against ICS devices have been tailored for the environment.

Threat behavioral analytics protection uses threat intelligence generated through the ongoing monitoring and analysis of threat activity groups that can be utilized to assess, build, and test ICS defenses. Threat intelligence reports typically contain indicators of compromise (IoCs) and TTPs. IoCs are specific technical elements of an attack that are not only immediately deployable in passive defense security controls but also temporal (while plausibly limited in use between organizations). TTPs, on the other hand, allow for a broader range of attacker behaviors. The IoC is a specific but changeable component of a TTP. Instead of looking for a specific IoC, a security operations team can look for matched or similar behavior. These TTPs are mapped against MITRE ATT&CK® for ICS to not only identify where in a kill chain an adversary was detected, but also to evaluate the depth and breadth of the security controls and detection capabilities across a specific threat activity group's behavior. Mapping MITRE ATT&CK® for ICS against a deployed ICS can be a daunting and extensive process.

Coverage by Fortinet

MITRE ATT&CK® for ICS is part of FortiSIEM and FortiEDR, with rules written using Dragos, Nozomi, and FortiGate ICS events.

Three new MITRE ATT&CK for ICS dashboards have been created to show rule coverage, incident coverage, and kill chain analysis for ICS techniques. A discovery method has been added for Nozomi ICS devices via Nozomi API, and the discovered OT/IoT devices are shown in CMDB in a heads-up display. At the time of this writing, Fortinet provided 84 MITRE ATT&CK® for ICS technique detection rules out of the box. Similar support for other vendors can be added.

Security Zone Interface

Challenges

Limiting communications at an ICS boundary typically involves a policy configuration of source IP, destination IP, source port, and destination port within a network firewall. 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 around high-risk services). If analyzed thoroughly as part of the design process for zones and conduits, many of the critical communications will already have been identified. What typically remains is to capture and analyze all communications channels and determine which applications are responsible for the traffic. Once all traffic is analyzed, the implementer can determine whether the traffic is necessary and, if not, put controls in place to block the traffic.

Traffic inspection and application-level control on industrial networks is useful where ICS protocol communication is required across a zone boundary. 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. Deep operational knowledge in how the specific use of these protocols is necessary to effectively apply application-level control within industrial networks.

Most organizations have a clear separation of IT (office) and OT (ICS). In today's manufacturing environments, connectivity from beyond the IT environment is becoming more popular to accommodate OEMs that want to connect to their machines, the remote support of processing experts and employees, and cloud-based operations dashboards, all of which have pierced the traditional IT/OT line. In addition, third-party service providers need access to their equipment located within the OT environment.

In support of IIoT adoption, the International Society of Automation is developing a new standard, ISA-TR62443-4-3-DC: Application of the 62443 Standards to the Industrial Internet of Things.

Coverage by Fortinet

Because it is a next-generation firewall first and foremost, FortiGate supplies the expected features as a core functionality. FortiGate's **`learn`** functionality can be more useful than more hands-on methods of 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 nonmalicious, but it allows FortiGate to be introduced 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.[4] Examine the use of these protocols and choose to block specific protocol features that will provide measurable effectiveness against capable threat activity groups.

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. Users should think carefully about using network access control and choose it only if it provides measurable effectiveness against capable threat activity groups. Improper planning can limit the flexibility required to recover quickly from security and other events.

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

Coupling FortiSwitch and FortiGate with FortiLink can enable microsegmentation to support a zero-trust architecture. Implementation of such an architecture with role-based access controls from FortiAuthenticator and FortiToken can manage the east-west communications among lower-level networks within the perimeter of an ICS network. A zero-trust architecture is the most effective method to stop or detect lateral movement within an ICS network. This advanced defense is essential in businesses where data analytics, for example, has driven increased demand to access data close to the source (sensors, for instance). Coordinated change management plans will need to be adopted when using zero trust to accommodate system and configuration changes required by the operations team. These changes most likely will be planned, but 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 they affect. In some cases, a RASI chart can help manage the change control process.[5]

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 control is self-inflicted.

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.

Wireless (802.11) Network Interface

Challenges

New wireless 802.11 standards are developed as technologies improve and security requirements change. As new standards are released, manufacturers of ICS devices typically lag in adopting them in their products. The network infrastructure connecting these ICS devices, however, will typically be refreshed more often. Backwards compatibility is available with newer wireless solutions, although the existing wireless-enabled ICS devices and systems will not benefit from any additional security capabilities the new standard provides. To appropriately mitigate risks associated with operating different 802.11 standards, additional analysis, configuration, validation, and testing will likely be needed during a wireless upgrade project.

[5] A RASI chart is a method used to clarify roles and responsibilities. RASI stands for "responsible, approve, support, inform." For an example, see http://kilbrideconsulting.com/var/m_9/9f/9f8/38868/408089-RASI%20Chart.pdf?download

The use of wireless networks varies widely across sectors and industry types. For many reasons beyond security, many ICS owners prefer to ban or heavily limit the use of wireless in their systems whenever possible. However, even those organizations are feeling the pressure to add more data analytics to maximize revenue of their ICS, making wireless more attractive because it is a cost-effective technology that does not require pulling wiring. Organizations still need to evaluate the 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 shown that the technology is a viable option. Continuous security reviews and improvements of those networks should be performed, not only in terms of threats, but also in regards to the availability and integrity of those systems because they play a critical role in operations.

Coverage by Fortinet

The FortiGate 802.11 wireless solution mirrors Fortinet zone and conduit capabilities in providing cohesion between wireless interface security and the security zone interface. Along with expected features, the incorporated intrusion prevention system (IPS) protects the wireless network from known 802.11 protocol attacks. Before any laptop is given network access, it can be quarantined while the endpoint protection is audited. Virtual patching, application/asset/data flow visibility, role-based access control and zero trust are some of the capabilities included in the Fortinet product.

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

VPN Interface

Challenges

VPN usage in an ICS context covers both the user level (remote operators, vendors, and contractors) and the system level. As remote access became more widely accepted, many system and machine builders began offering remote support capabilities. This capability significantly improved uptime and accelerated 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 are located in hostile industrial environments.

Coverage by Fortinet

FortiGate has a ruggedized version designed specifically for hostile industrial environments. It 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 support secured access to ICS data and limited systems.

This implementation allows remote users, such as employees, vendors, or contractors, to access only specific internal systems. Some organizations also use this access for contractors working on-premises as a way of keeping their external laptops off the network. In those situations, a guest network is typically provided, placing the contractor on the internet and requiring them to access the environment over their approved VPN and jump-host solution. As a result, organizations' security teams can audit contractors while they perform on-premises activities. A clearly documented use case for each user's access and anticipated activities should exist to assist with detecting and limiting misuse and abuse.

In most cases, VPN technology provides some protection when a network is accessed from an untrusted device. As with all VPNs, a rigid process needs to be in place to design, implement, manage, and maintain the VPN technology. This process includes actively monitoring and applying security updates, continuously monitoring VPN usage and logs, and auditing and maintaining configurations, users, and devices in a timely manner.

As with wireless networks, the use of VPNs in an ICS can be engineered to support access to only specific hosts and users using specific, mostly ICS, protocols. VPNs can 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 to the local system while the device is connected over VPN. This dedicated host has restricted access to specific resources on the local ICS network, typically using 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 provides combined layers of defense.

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 with the vendor of every option 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 second, 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 ICS strategically. Evaluating assigned SLs 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.

Appendix A

Fortinet Product	Product Description
FortiEDR FortiClient	FortiEDR delivers real-time automated endpoint protection with orchestrated incident response across IT and OT endpoints. A single integrated platform with flexible deployment options and a predictable operating cost, FortiEDR provides real-time, proactive risk mitigation, endpoint security, pre-infection protection via a kernel-level, next-generation antivirus engine, post-infection protection, and forensics.
FortiClient EMS	FortiClient is an endpoint agent that provides visibility and control of software and hardware inventory across the entire Fortinet Security Fabric, allowing organizations to discover, monitor, and assess endpoint risks in real time. It also provides secure remote access (VPN client). FortiClient, along with the FortiClient Enterprise Management Server (EMS), is an integral part of Fortinet's zero-trust network access (ZTNA) offering. FortiClient includes these ZTNA, secure access service edge (SASE), and endpoint protection (EPP) capabilities: • ZTNA enables remote users to access their corporate applications while ensuring strict authentication and verifiable endpoint security posture before any access is granted. • SASE ensures that remote users can securely connect to the corporate network following the same corporate security policies regardless of their location. SASE integrates seamlessly with ZTNA to deliver a transparent user experience while offering security protection for all endpoints from advanced threats. • EPP offers vulnerability detection and protection, auto-patching antivirus, application firewall, anti-ransomware, and endpoint management.
FortiSwitch	FortiSwitch is a secure access switch family that delivers outstanding performance, scalability, and manageability while allowing OT environments to extend networking and security across their network infrastructure. FortiSwitch seamlessly integrates with the Fortinet Security Fabric via FortiLink and can be managed by FortiCloud or FortiGate. The unified management of FortiSwitch via FortiGate offers complete visibility and control of users and devices in the network.
FortiAP	FortiAP is a series of Wi-Fi access points that can be managed by FortiCloud or FortiGate. These access points offer high throughput, optimal coverage, and enterprise-class 802.11ax services. FortiAPs can seamlessly integrate with the Fortinet Security Fabric.
FortiExtender	FortiExtender provides a bridge between local Ethernet LANs and wireless LTE/5G WAN connections. FortiExtender can support diverse wireless applications with a high level of backhaul redundancy using a single LTE/5G modem platform over redundant SIM cards attaching to different mobile networks. FortiExtender can be used as the LTE/5G backhaul of an on-premises FortiGate with maximum wireless LTE/5G signal strength. It can be centrally managed by FortiGate.
FortiGate	FortiGate is the flagship next-generation firewall and next-generation intrusion prevention system (NGFW/NGIPS) product family from Fortinet, delivering best-in-class security, high-speed networking, hardware-accelerated performance features using purpose-built security processors for NGFW/NGIPS, and built-in, market-leading SD-WAN. FortiGate comes in different form factors and sizes, including ruggedized appliances to withstand the harsh environmental conditions often facing industrial applications.
FortiToken	FortiToken enables two-factor authentication via a one-time password (OTP) application with push notifications or a hardware time-based OTP token. FortiToken Mobile (FTM) and the hardware OTP tokens are fully integrated with FortiClient, are secured by FortiGuard, and are available for direct management and use within the FortiGate and FortiAuthenticator security products. FortiGate, FortiToken, and FortiAuthenticator form an integrated solution that is easy to implement, use, and manage for multifactor authentication.
FortiAuthenticator	FortiAuthenticator offers single sign-on and user authorization for the Fortinet secured enterprise network. It identifies users, queries access permissions from third-party systems, and forwards the access requests to FortiGate to implement identity-based security policies. FortiAuthenticator supports a wide array of methods and tools for authentication and authorization, such as Active Directory, RADIUS, LDAP, SAML SP/IdP, PKI, and multifactor authentication.
FortiNAC	This network access control product enhances the Fortinet Security Fabric with visibility, control, and automated response for everything that connects to the network. FortiNAC provides protection against malicious access, extends access control to third-party devices, offers greater visibility for devices, supports dynamic network access control, and orchestrates automatic responses to a wide range of networking events.
FortiAnalyzer	FortiAnalyzer is a centralized log management, analytics, and reporting platform that provides customers with single-pane orchestration, automation, and response for simplified security operations, proactive identification, remediation of risks, and complete visibility of the entire attack surface. FortiAnalyzer can collect different types of logs and events from Fortinet products via Fortinet Security Fabric integration.
FortiManager	FortiManager provides automation-driven centralized management. It allows end users to centrally manage FortiGate, FortiSwitch, and FortiAP devices in their network with a centralized management platform.
FortiSIEM	FortiSIEM provides unified event correlation and risk management for multivendor implementations. It enables analytics from diverse information sources including logs, performance metrics, SNMP traps, security alerts, and configuration changes. It feeds all the information into an event-based analytics engine and supports real-time searches, rules, dashboards, and ad hoc queries. FortiSIEM offers Purdue-level classification for assets, logs, and event correlation and it also supports MITRE ATT&CK for ICS framework for log analysis. Integration with third-party OT security tools is supported out of the box.
FortiSOAR	FortiSOAR is a holistic security orchestration, automation, and response (SOAR) workbench that lets security operations center (SOC) teams efficiently respond to the ever-increasing influx of alerts, automate repetitive manual processes, and cope with their chronic shortage of resources. Its patented and customizable security operations platform provides automated playbooks and incident triaging, and real-time remediation for enterprises to identify, defend, and counter attacks. FortiSOAR optimizes SOC team productivity by proving more than 3,000 actions and seamlessly integrating with over 300 security platforms. This results in faster responses, streamlined containment, and mitigation times reduced from hours to seconds. FortiSOAR includes ICS-specific capabilities, such as MITRE ATT&CK for ICS framework for asset and event correlation, IT/OT asset inventory dashboards, compliance dashboards for OT-specific cybersecurity regulations and frameworks, and more.
FortiProxy	A secure web proxy that protects employees against internet-borne attacks by incorporating multiple detection techniques, such as web filtering, DNS filtering, data loss prevention, antivirus protection, intrusion prevention, and advanced threat protection.

Fortinet Product	Product Description
FortiWeb	A web application firewall (WAF) that secures cloud-based resources and DevOps environments by protecting against known and unknown threats, including sophisticated ones such as SQL injection, cross-site scripting, buffer overflows, and DDoS attacks.
FortiDeceptor	FortiDeceptor provides honeypot and deception technology to deceive, expose, and eliminate external and internal threats early in the attack kill chain, proactively blocking these threats before any significant damage occurs. Integrated with FortiEDR and FortiGate, FortiDeceptor automates the blocking of the attackers targeting IT and OT systems and devices by laying out a layer of decoys and lures designed to redirect attackers' focus while revealing their presence on the network.
FortiSandbox	FortiSandbox provides top-rated AI-powered breach protection that integrates with the Fortinet Security Fabric platform to address both rapidly evolving and targeted threats, including ransomware and crypto-malware, across a broad digital attack surface. Designed specifically for OT, FortiSandbox automates zero-day advanced malware detection and response in order to detect in real time threats targeting OT systems and protocols.
FortiNDR	FortiNDR offers next-generation, AI-driven breach protection technology to defend against various cyber-threats, including advanced persistent threats through a trained Virtual Security Analyst™. The virtual analyst helps with identifying, classifying, and responding to threats, including well-camouflaged ones. Employing deep neural networks based on advanced AI and artificial neural network, FortiNDR provides fast security investigation (less than one second) by harnessing deep-learning technologies that assist in an automated response to remediate different types of attacks.
FortiSASE	A cloud-delivered service, FortiSASE is an architecture that combines network, security, and WAN capabilities to provide endpoints (remote users, devices, and branches) with secure access to the internet, cloud, and data center network. It uses network security technologies including firewall-as-a-service (FWaaS), secure web gateway (SWG), ZTNA, and cloud access security broker (CASB). It relies on WAN technologies including SD-WAN.
FortiGuard Security Services	FortiGuard Security Services are powered by FortiGuard Labs, a global threat research and response team that leverages machine learning (ML) and AI systems around the globe to collect real-time threat intelligence. FortiGuard Security Services are offered through subscription bundles and includes several advanced threat protection services for enterprise networks, web, cloud, OT, etc. The Industrial Security Service and IoT Detection Service are among the FortiGuard subscription offerings. Industrial Security Service offers more than 2,000 IPS signatures for ICS/OT applications as well as protocols that support deep packet inspection (DPI) and more than 500 IPS signatures for ICS-specific threat and vulnerability protection.
FortiCamera FortiRecorder	A suite of secure, network-based video surveillance cameras and recorders that bolster protection against cyber-physical attacks.

Appendix B

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 1 – Identification and authentication control (IAC)					**FR 1 Product Mapping: FortiGate, FortiWiFi/FortiAP, FortiAuthenticator, FortiToken, FortiPAM, FortiClient, FortiEDR, FortiAnalyzer, FortiManage**		
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, FortiPAM 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) 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) meet 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, FortiPAM, 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, FortiPAM, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, FortiSandbox, FortiSIEM, FortiSOAR**		
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, FortiPAM, FortiManager C: Product(s) integration.
SR 2.1 RE 2 – Permission mapping to roles		✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiPAM, FortiManager C: Product(s) integration.
SR 2.1 RE 3 – Supervisor override			✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiPAM, 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, system-wide audit trail			✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiPAM, FortiAnalyzer, FortiManager, FortiSIEM, FortiSOAR 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, FortiSwitch N: The product (s) can function as NTP server to provide time to the network connected assets. Precise time synchronization functionality over network e.g., IEEE 1588v2 PTP is available only in select product(s).
SR 2.11 RE 2 – Protection of time source integrity				✔	Both	Full	P: FortiGate N: Capability is limited to any network asset(s) connected to/via the product(s).
SR 2.12 – Non-repudiation			✔	✔	Both	Full	P: FortiGate N: Capability is limited to any network asset(s) connected to/via the product(s).
SR 2.12 RE 1 – Non-repudiation for all users				✔	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAuthenticator, FortiPAM, 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 centralised 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 centralised 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) have 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) have 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) have 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 security 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 security 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 security 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 security zones and conduits within Layer 3 and/or Layer 2 networks and centralised 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 security 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, FortiSIEM**		
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, FortiSIEM 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, FortiDDoS, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, FortiSOAR, 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, FortiDDoS 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, FortiSOAR, Fabric-Ready Partner Solutions C: Product(s) integration.

Sponsor

SANS would like to thank this paper's sponsor: