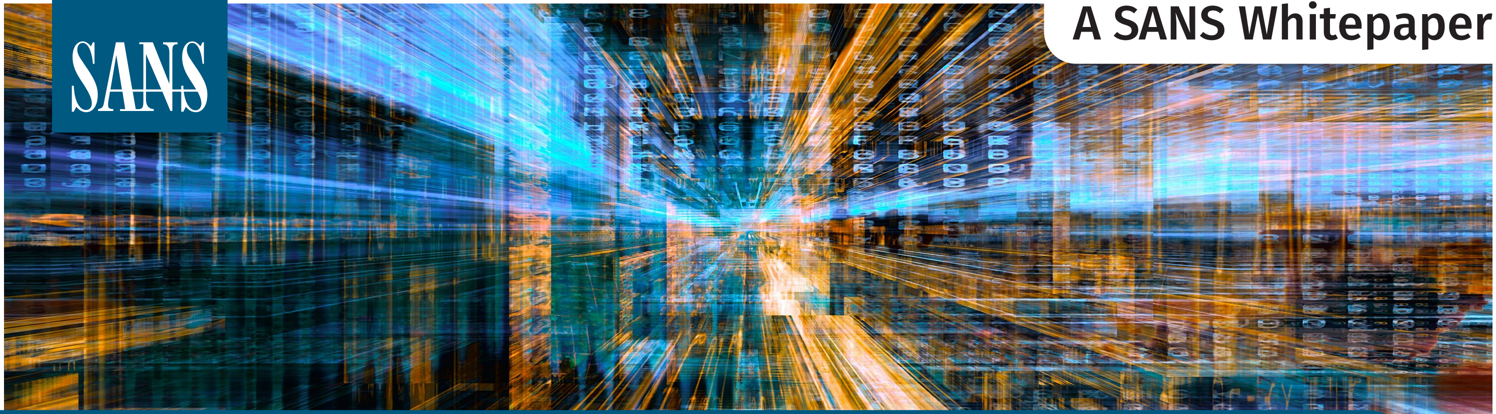
A SANS Whitepaper



Managing ICS Security with IEC 62443

(Companion piece to "Effective ICS Cybersecurity Using the IEC 62443 Standard")

Written by **Jason Dely**

November 2020

Sponsored by:

Fortinet

Standards give us a common vocabulary to help us understand a particular subject as well as solve a particular problem. Similarly, cybersecurity standards direct and guide organizations to meet their security goals. Managers looking to meet their companies' security goals can accelerate their knowledge of the problem and achieve those goals by leveraging the advice of the industry experts who authored the standards.

Following the IEC 62443 series of standards (hereafter in this paper referred to collectively as "the Standard"), also known as *IACS*, can help strategically mature an organization's industrial controls systems (ICS), or, as the Standard calls them, *industrial automation and control systems*. The Standard provides all sectors with a common framework to manage and mitigate security vulnerabilities in industrial automation control systems. Most industrial customers are only interested in what their sector is doing, but the IEC 62443 series of standards are representative of *all* sectors and should therefore be consumed by individual sectors.

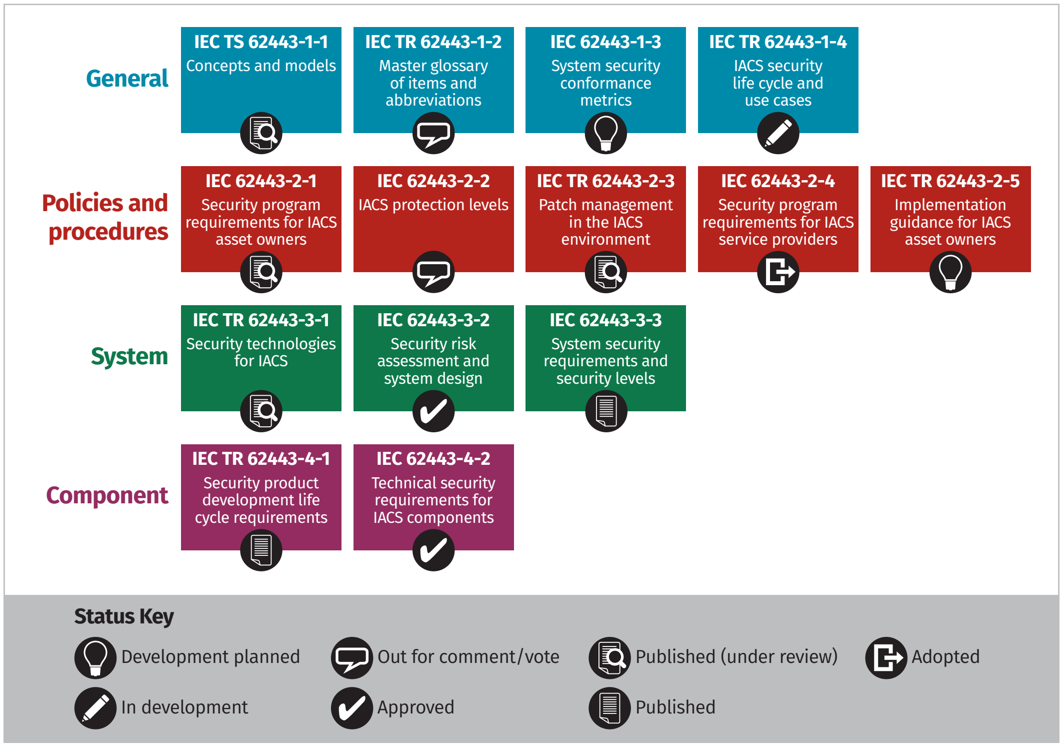
In a companion whitepaper, "Effective ICS Cybersecurity Using the IEC 62443 Standard,"[1] we looked at the structure and purpose of IEC 62443 and how Fortinet products can assist in implementing the security requirements stated within the Standard. In this paper, we examine how to use the Standard to strategically reduce your ICS cybersecurity risk.

[1] SANS Institute, Effective ICS Cybersecurity Using the IEC 62443 Standard," November 2019, www.sans.org/reading-room/whitepapers/analyst/effective-ics-cybersecurity-iec-62443-standard-39960 [Registration required.]

©2020 SANS™ Institute

What Is IEC 62443?

The IEC 62443 series of standards contains frameworks an organization can apply to its unique, clearly understood needs and situation. The Standard can also provide guidance about how to choose products that will effectively improve an organization's ICS defensive posture while balancing the implications of costs and risk reduction. Figure 1 is a graphical representation of the Standard's various planned and published work products.



General	IEC TS 62443-1-1 Concepts and models 🔍	IEC TR 62443-1-2 Master glossary of items and abbreviations 💬	IEC 62443-1-3 System security conformance metrics 💡	IEC TR 62443-1-4 IACS security life cycle and use cases ✎	
Policies and procedures	IEC 62443-2-1 Security program requirements for IACS asset owners 🔍	IEC 62443-2-2 IACS protection levels 💬	IEC TR 62443-2-3 Patch management in the IACS environment 🔍	IEC 62443-2-4 Security program requirements for IACS service providers ⇥	IEC TR 62443-2-5 Implementation guidance for IACS asset owners 💡
System	IEC TR 62443-3-1 Security technologies for IACS 🔍	IEC 62443-3-2 Security risk assessment and system design ✓	IEC 62443-3-3 System security requirements and security levels 📄		
Component	IEC TR 62443-4-1 Security product development life cycle requirements 📄	IEC 62443-4-2 Technical security requirements for IACS components ✓			

Status Key

💡 Development planned
💬 Out for comment/vote
🔍 Published (under review)
⇥ Adopted
✎ In development
✓ Approved
📄 Published

Figure 1. Parts of the IEC 62443 Standards Series[2]

Balancing a defensive posture with costs and risk reduction is achieved by taking the organization's monolithic ICS cybersecurity risk and segmenting individual ICS operational networks and systems into smaller sizeable security risks, or "zones." Tackling the problem in smaller, measurable and manageable segments is not only less daunting but also more financially prudent because it avoids big expenditures that ultimately may be unnecessary.

Without using the Standard, any organization attempting to implement a set of common cybersecurity controls throughout the entire ICS will have varying degrees of success with each of those controls. Some controls may be extremely costly. Some organizations may discover that the technology does not support the control. Some controls will fail to align well with business operations. For those improvements driven by policy, the unachievable controls (such as systems in violation) will fall into several documented policy exceptions.

In this kind of monolithic ICS cybersecurity program, where one set of controls is applied across the entire ICS environment, exceptions generally preclude the achievement of successful risk reduction. Precious time and resources are used in the follow-up requests for exception and measuring the specific risk increases. If the exceptions prove risky and a solution is already rolled out, an organization is left with no alternative other than to invest in an additional solution to meet the requirements of the control—or accept the risk.

Meeting and maintaining the implementation of the Standard is the responsibility of everyone involved in controlling an organization's ICS cybersecurity risk.

[2] IEC, https://webstore.iec.ch/preview/info_iec62443-4-2%7Bed1.0%7Db.pdf

Alternatively, the Standard's use of "security zones" allows each individual segment to be measured and categorized based on individual business risk. The Standard provides guidance on how to determine both the zones and the security level. Certain controls are required to meet each level. An organization must then assess the gaps between its existing security controls and the Standard's definition of the assigned level. These zones are assigned security levels (SL) ranging from 1 to 4.

The description of the SL along with guidance on how to produce the segments exists within the Standard and is also found in Table 1. The final assignment of levels to each zone is left up to each organization's risk management process across each sector. 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 requirement enhancements (REs) to improve security strength. A chart in the Standard, Table 1 maps each SL with corresponding SRs and REs.

Table 1. Mapping of SRs and REs to FR Security Levels 1-4[3]

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	✔	✔	✔	✔

To assist with the definition of each SL, the Standard provides a threat definition for each baseline 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 risk exposure. Potentially, the SLs could pose unique risk levels for each security zone as well—threats, operational changes and technology such as IIoT (industrial internet of things) can change the attack surface of an ICS. SLs help establish goals to reduce risk, but goals must always be flexible and actively realigned to stay current with the global changes in threats. Table 1 maps SR and RE baselines to the FR for each security level. For more information on how to apply the Standard, consult the companion paper, "Effective Cybersecurity Using the IEC 62443."[4]

Meeting and maintaining the implementation of the Standard is the responsibility of everyone involved in the ICS cybersecurity risk to the organization. This group includes product suppliers or manufacturers (such as vendors) intended to be used in industrial control systems. All control systems rely heavily on many different technologies developed by many different product manufacturers, all of which rely on the integration of multiple systems to ensure reliable and safe operations. Some of those manufacturers have existed since the early 1900s and, over time, have developed and sold many technologies

[3] Table reference: IEC62443-3-3-2013

[4] SANS Institute, "Effective ICS Cybersecurity Using the IEC 62443 Standard," November 2019.

to improve the efficiencies and productivity of operations. Concerns about ICS cybersecurity began many years prior to 2009, when the first technical specification from the series, IEC/TS 62443-1-1, was introduced.

Those specifications recognized the necessity for owners as well as vendors to improve their ICS security. The Standard has not overlooked this need and released the document ANSI/ISA-62443-4-1-2018 – "Security for industrial automation and control systems Part 4-1: Product security development life-cycle requirements." In an attempt to help vendors improve the security of their products and supported systems, the Standard offers manufacturers the opportunity to be IEC 62443 Conformance Certified by the ISA Security Compliance Institute (commonly known as ISASecure).[5] This conformance process is a step in the right direction; however, only a fraction of the millions of product types that exist, new or old, are certified. The conformance certification affects new products only. Having this certification is beneficial but presents complexities for sectors to adopt at scale. For instance, some older products are planned to be in operation for many more years. Additionally, manufacturers face steep costs to have each of their products certified and would need to pass those costs on to customers, which in turn inhibits market acceptance. This process does not, however, prevent an organization from practicing good security in its own ICS.

Regulations such as NIS-D are designed to ensure critical infrastructure organizations are establishing an ICS cybersecurity framework based on IEC 62443 and are free of any violations.[6] One should not simply comply with the Standard. To truly benefit from its tenets, each organization must evaluate and align the provided concepts, framework and controls with an accurate representation of cybersecurity risk to their operations.[7] This process requires an alignment of people and roles within and possibly outside the organization to define security zones and determine which security levels to assign to each zone. In addition to the traditional corporate risk managers, security managers and other IT roles, other critical roles needed for success will include some or all of the following: operations managers, plant managers, automation engineers, instrumentation engineers, process engineers, mechanical engineers, health safety and environment managers, ICS vendors, ICS OEMs and ICS systems integrators. The actual job titles, roles and responsibilities will vary by organization and sector.

Complex ICS environments are often comprised of different business units with different business needs and challenges. These environments also may have different vendors or other external business relationships. In such conditions, the process of defining responsibilities and accountability for establishing security zones and levels will be difficult to manage. The use of a RACI[8] responsibility assignment matrix per security zone will help identify, organize and manage the security needs of each zone.

IEC 62443 Does Not Stand Alone

As a recognized body of knowledge for ICS cybersecurity that is sanctioned by an internationally recognized standards organization, IEC 62443 is referenced by other standards and frameworks such as NERC CIP,[9] NIS-D and NIST CSF, shown in Figure 2.

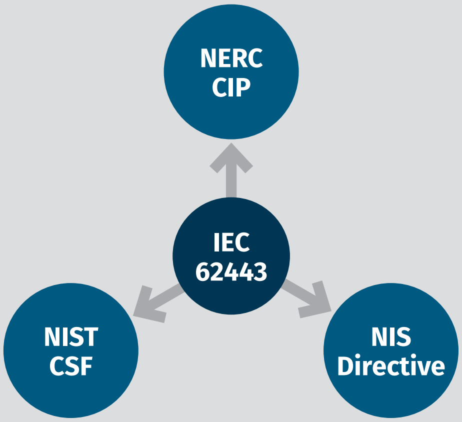


Figure 2. IEC 62443's Relationship to Other Standards

[5] The International Society of Automation (ISA) was the founding organization of IEC 62443.

[6] For more information about NIS-D, see "Aligning Your Security Program with the NIS Directive," September 2020, www.sans.org/webcasts/aligning-security-program-nis-directive-115790 [Registration required.]

[7] See the companion paper, "Effective ICS Cybersecurity Using the IEC 62443 Standard," November 2019.

[8] RACI is an acronym derived from four key responsibilities: responsible, accountable, consulted and informed.

[9] For more information about NERC CIP, see "How to Use NERC CIP: An Overview of the Standards, Their Deployment, and How to Use Fortinet Products for Compliance," June 2020, www.sans.org/webcasts/nerc-cip-overview-standards-deployment-fortinet-products-compliance-114305 [Registration required.]

Defining Goals and Objectives

The task of improving ICS cybersecurity posture begins with a well-established security program. This program may have some similarities to a corporate security program, such as ISO/IEC 27001-based security implementation, but must align with the nuances found in ICS. The IEC 62443-2-1 standards document provides a framework and guidance for any organization to set up a cyber security management system (CSMS) specific to its ICS. Elements include risk analysis, addressing risk with the CSMS, and monitoring and improving the CSMS as depicted in Figure 3.

This document provides a mapping for users of ISO/IEC 27001 because many of the components are shared in this standard but deliberate adjustments were made to align with ICS.

Running a separate program for an ICS establishes the core business rationale, risk identification, classification and assessment specific to operations it covers. Consider integrating aspects of a business network cybersecurity program with an ICS network program. Doing so will support corporate risk-reduction cost effectiveness and overall security operations. Aspects of this alignment also support the potential of future IT and ICS technology/application convergence while maintaining the needs of an ICS cybersecurity program. As shown in Figure 4, an established CSMS works to prevent the project approach to ICS cybersecurity, which has been its downfall in the past.

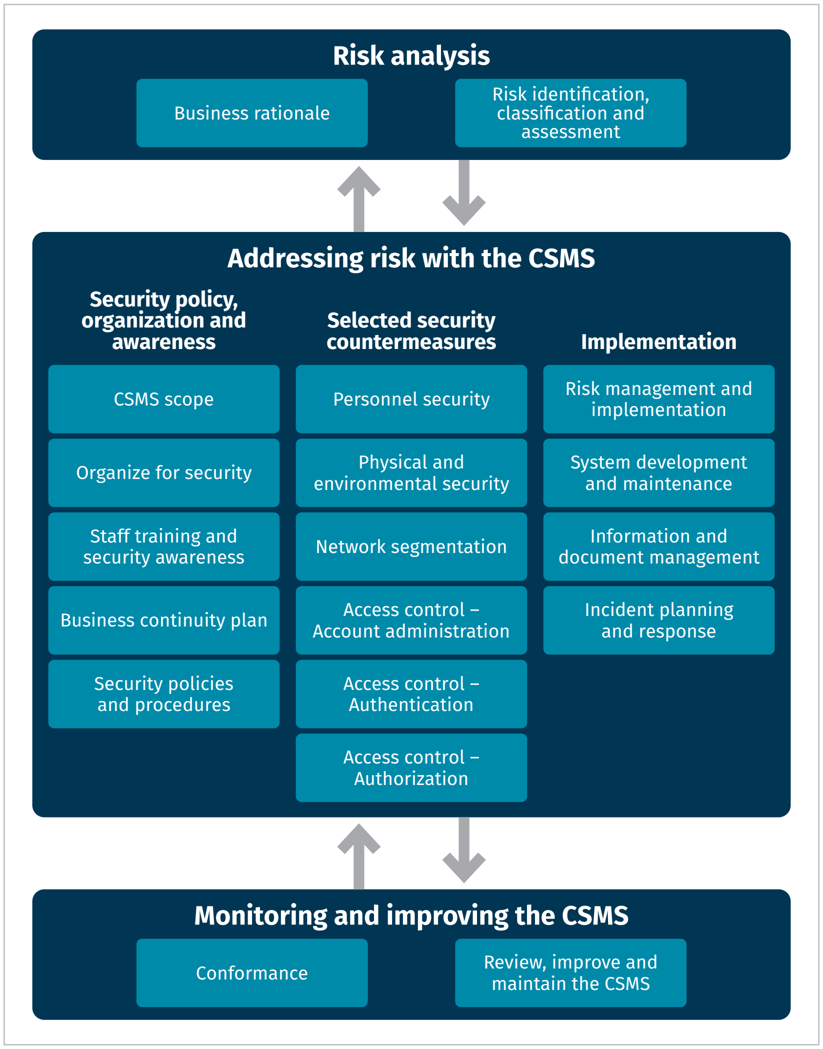

Risk analysis
Business rationale
Risk identification, classification and assessment
Addressing risk with the CSMS
Security policy, organization and awareness
Selected security countermeasures
Implementation
CSMS scope
Organize for security
Staff training and security awareness
Business continuity plan
Security policies and procedures
Personnel security
Physical and environmental security
Network segmentation
Access control – Account administration
Access control – Authentication
Access control – Authorization
Risk management and implementation
System development and maintenance
Information and document management
Incident planning and response
Monitoring and improving the CSMS
Conformance
Review, improve and maintain the CSMS

Figure 3. Elements of a Cybersecurity Management System

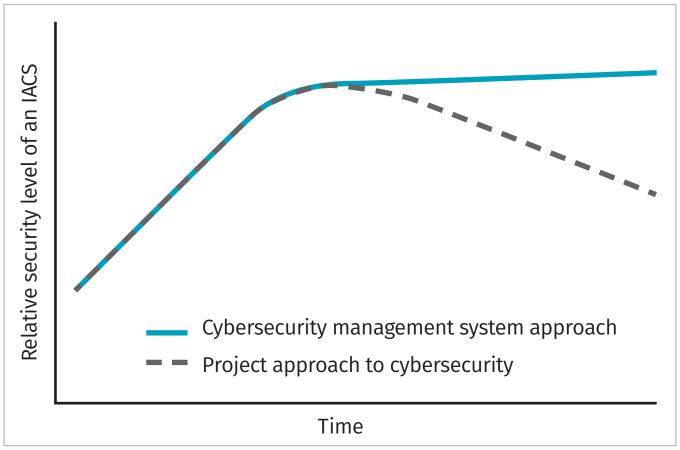


Figure 4. Cybersecurity Level Over Time

This life-cycle approach to cybersecurity spans the maturity phases shown in Table 2.

Each phase is covered in the IEC 62443 standards documents and should be thoroughly reviewed and implemented to meet the cybersecurity needs of the ICS. With the operational and technology complexities found in an ICS, rolling out the program can be portioned across multiple ICS operations rather than as a whole, with each portion measured against its own risk level and maturity scale.

All sectors and organizations that operate ICS are at various security postures. Some may be just starting out and others may already be well underway. In either case, the implemented strategy followed for ICS perimeter controls and countermeasures will define the effectiveness of critical risk reduction.

Table 2. 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

The Value of a Perimeter Control

Having a distinct perimeter between the control systems environment and the rest of the organization and external world provides a significant advantage and, for most, is the best starting point for addressing ICS risk and improving security posture. This perimeter defines clear business boundaries. It also guides decisions regarding external user and data and system connectivity based on the interests of ICS operations and cybersecurity. Most organizations will not need to perform an assessment before embarking on activities to define and control these perimeters. With an established ICS perimeter, it is more difficult to refine and build upon a more refined security posture. A more refined risk assessment analysis process provides guidance into focused risk management of internal ICS operations.

Risk Assessment Process

With the zones defined and security levels assigned, deciding which areas to improve may not be so clear. Larger organizations with multiple facilities will struggle to finance mitigation of all weaknesses. IEC 62443-3-2 is a guide that covers a process of assessing ICS risk that incorporates the risk factors and mitigations that are unique to an enterprise network. Consider the following when deciding where to begin and where to end.

- Although countermeasures may seem easier to implement at security level 1, changes in security zones at security level 4 typically result in more benefit to an organization.
- ICS operations typically contain multiple security zones, but this does not mean they operate in isolation of each other.
- Inter-zone operational dependencies, communications and information exchange (referred to as “conduits” in the Standard) will exist and will need to be analyzed for risk.
- Establishing the target security level needed to reduce risk establishes justification to implement.

Countermeasures

An assessment may identify a list of recommended countermeasures. Each countermeasure will have an associated cost to implement and maintain. Many organizations would prefer to limit the number of security products and features introduced into their environment, and it's important to realize that not all countermeasures must be in the form of security products and features. Because industrial control systems are engineered systems, they may be designed in alternative ways, with some more expensive to implement and operate than others. Seeking subtle opportunities, such as a change in communication path or segmenting a server application, can reduce the risk of a zone or conduit, thereby potentially lowering the security level or limiting the investment required to implement and maintain countermeasures. Additionally, re-architecting aspects of an environment will help build in a layered defense model and reduce the exposure of higher-risk zones. Simply *having* a countermeasure is not enough. The countermeasure must be managed appropriately over the course of its lifetime to ensure effectiveness. Figure 5 depicts a strategy for a secure product life cycle but could also be considered for maintaining countermeasures as well.

Many organizations would prefer to limit the number of security products and features introduced into their environment, and it's important to realize that not all countermeasures must be in the form of security products and features.

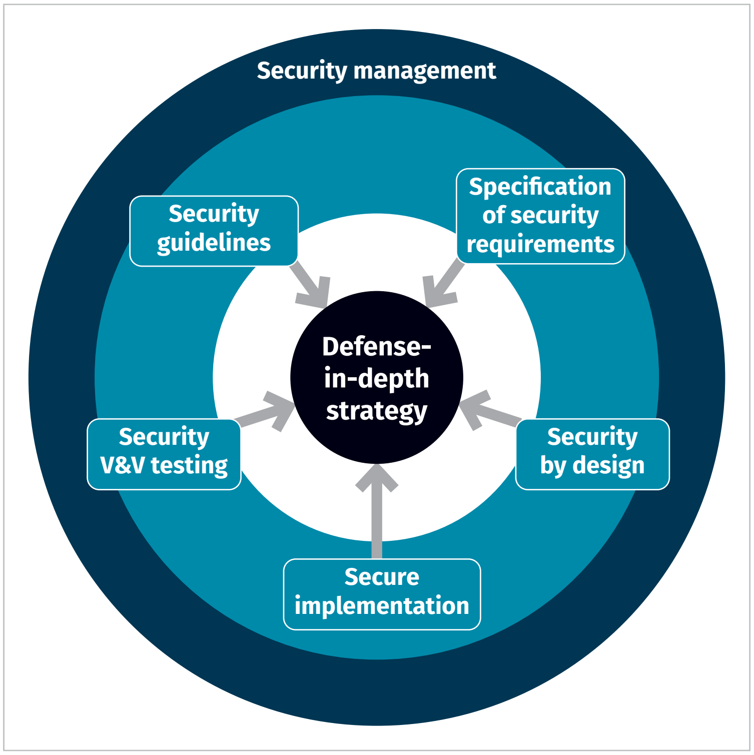


Figure 5. Coordinated Defense Layers

When selecting and implementing countermeasures, the CSMS development process requires an update to business continuity and incident response. Adding countermeasures to address specific risks can have unforeseen effects on the business operations but also may provide opportunities for improved monitoring, detection and response capabilities. Although minimizing the expenditure is important, cybersecurity is an ecosystem that benefits significantly from ICS cybersecurity monitoring and response activities. Although not specifically covered in the Standard, organizations would be wise to consider network security monitoring and incident response capabilities when selecting countermeasures.

Three primary functions should be considered when selecting and implementing countermeasures that support security monitoring and response activities: visibility, control and actionable response.

Simply having *a countermeasure is not enough. The countermeasure must be managed appropriately over the course of its lifetime to ensure effectiveness.*

Visibility. Visibility means having strategic sight of the underlying current state of the control systems build, the current state of operations and the interactions of a control system. Properties can include, but are not limited to:

- Cyber asset inventories
- Network traffic
- CPU processes
- Auditable login logs
- System event logs
- System documents/drawings
- Available security features
- Implemented security controls
- Contextual understanding of operations

Identify opportunities and capabilities to expand countermeasures in the future that may benefit other security zones.

Security controls. Security controls are safeguards or countermeasures strategically selected and implemented to:

- Strategically align to and implement sophistication of threats
- Reduce or minimize the risk, or effect, of a cyber-related event
- Support the reliability and safety of operations
- Provide detection and incident response capabilities

Actionable response. Actionable response is the capability to execute predefined processes, or playbooks, in response to ICS cybersecurity-related events and incidents. This capability includes, but is not limited to:

- Identifying and classifying the criticality of cyber-related events and incidents
- Notifying and communicating structure during an incident (including regulatory obligations)
- Performing an appropriate level of incident response aligned to the criticality of an incident
- Enabling or manipulating security controls, as appropriate, to isolate or contain the security zone from hostility during an incident response, managing the reliability and safety of an ICS during any cyber-related incident or activity

Complying with the requirements of each security level for each zone 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. Taking remediation actions can be advantageous across many security zones, including those outside the immediate scope of an assessment. The result is the capability to maximize return on investment both today and tomorrow. Be sure to document feature expansions provided by the solutions that may have use in future countermeasures.

Key Benefits with Fortinet

Because many industrial control systems were not designed with today's knowledge of ICS security requirements, organizations that have them may face challenges to implement technologies to improve security. Identifying what solution requires the least monetary investment with the largest return is not always a straightforward process. An organization may have a primary ICS vendor whose products make up their core equipment. It also may be saddled with ICS acquisitions that cannot be affordably converted. Nevertheless, it can ensure the plant is operating effectively within system and business tolerances. In such cases, it may make sense to seek a security vendor that can provide solutions to any existing risk challenges.

Fortinet provides coordinated coverage across a variety of security controls, including three of the most common challenges: boundary (zone and conduit) security, wireless security and remote access. Additionally, as a vendor that provides solutions for IT and ICS systems, Fortinet brings together capabilities to address advanced security requirements in demand for IIoT and cloud services such as micro-segmentation, application control and intrusion prevention/detection systems.

Some organizations have successfully implemented security controls to address these challenges, but many have not considered how to operationalize security monitoring and incident response in these areas. Operating disparate security solutions in an ICS requires more attention to be properly managed and maintained or, as seen many times, the security solution will become forgotten in the operation.

Layered defense is more than just adding security incident prevention capabilities. It is also about creating opportunities to identify incidents that have not been prevented, understand the threat and address the incident. For at least the three primary challenges mentioned earlier in this section, Fortinet provides a centralized management and monitoring capability. Figure 6 highlights how the Fortinet solution can align with the reference architecture documented in the Standard.

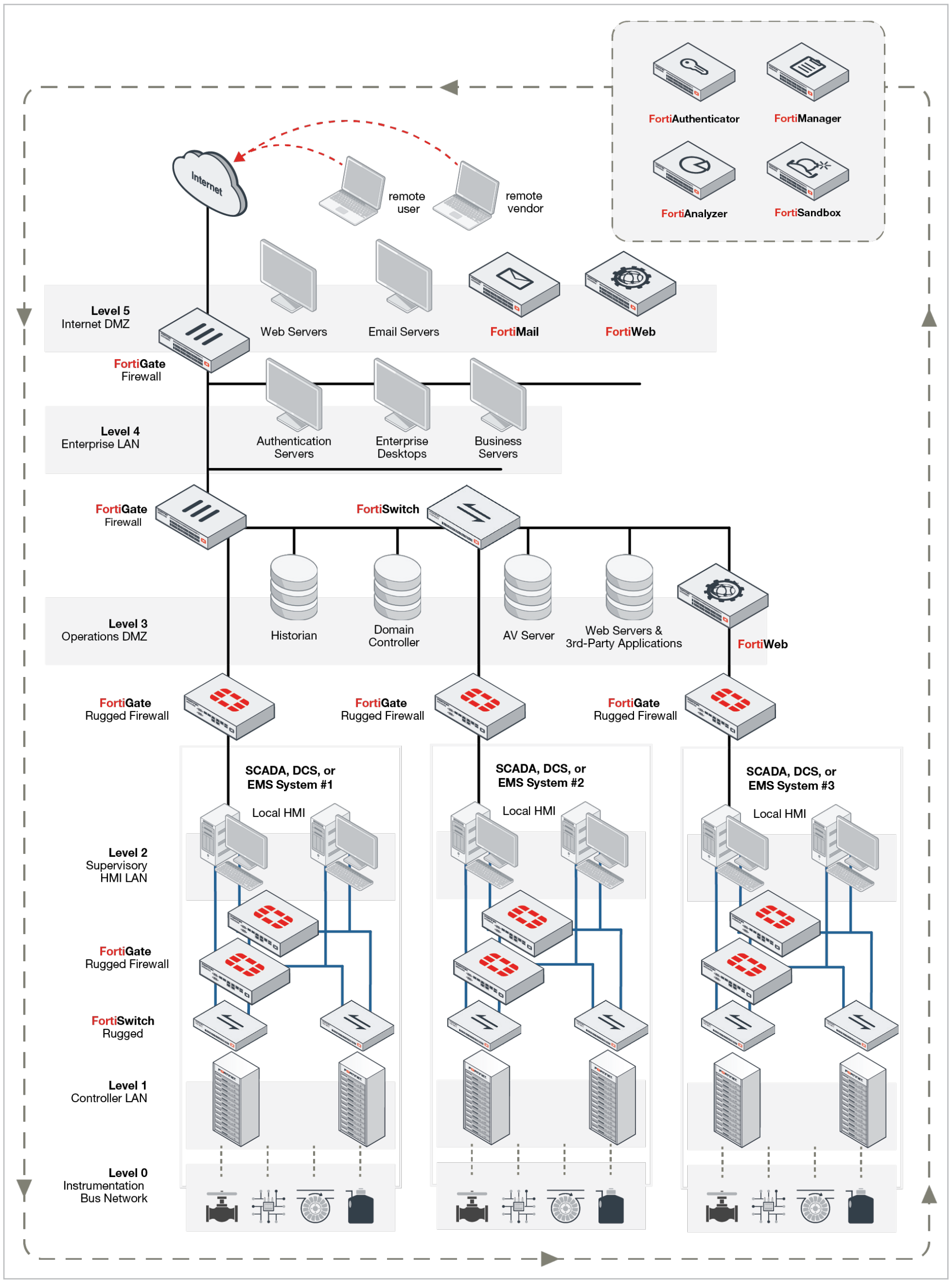


Figure 6. How the Fortinet Solution Aligns with IEC 62443

This solution is scalable and aligns with various security levels. To help meet security level 4 requirements, Fortinet also provides advanced features that are commonly requested and improved upon in the industry, such as multifactor authentication (MFA), ICS protocol inspection and sub-zones utilizing network access control.

MFA is an increasing necessity when providing external access to an ICS. VPN credential theft from support personnel, vendors and contractors, or directly from internal IT systems, is a common method that threat actors use to gain a trusted foothold into the environment. Threat actors' intent on compromising an ICS is looking for high-confidence access with covert interaction for extended campaigns in these environments. Having MFA capability as part of a perimeter solution is critical in reducing the effectiveness of credential theft and preventing unauthorized access.

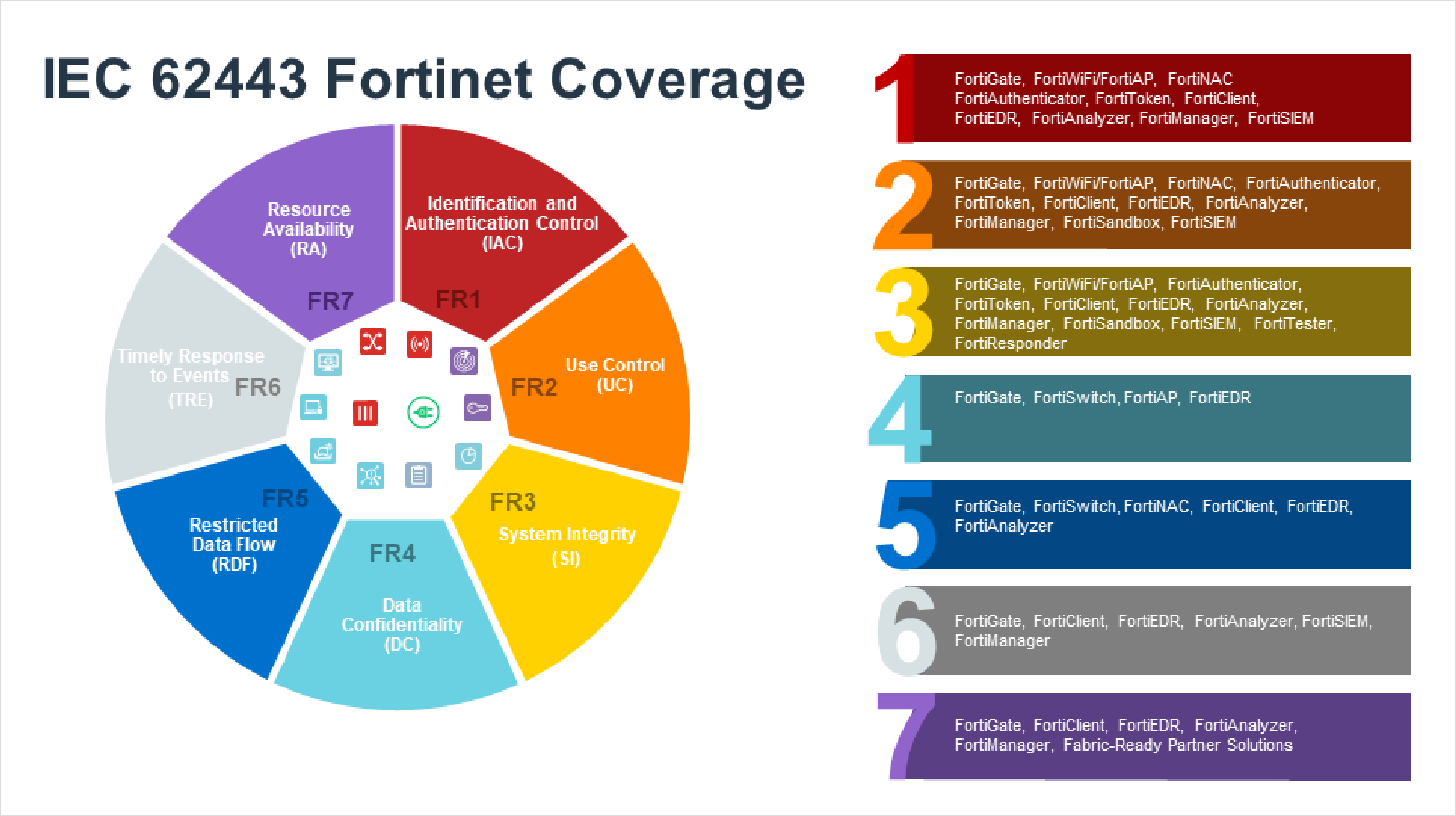
ICS protocols provide many features vendors can use to achieve system designer requirements. Hackers can abuse the features of these protocols, however, to effectively change the state of an operation. It is also well known that most of these protocols lack authentication and authorization capabilities, which allows for unsolicited interactions with ICS components and services. An inspection capability from a network product, like FortiGate, can strategically implement rules to block unused features of the protocol that could be abused and cause an undesirable effect on operations.

The Standard describes zones and sub-zones. Although the final zones defined by an organization typically align directly with gateways and other network segmented efforts, there are times when a sub-zone (also known as micro-segmentation) that coordinates with a small group of components or services within a larger subnet may be more suitable. It may not be justifiable to simply move these assets onto their own subnet and place it behind a firewall. Additionally, moving them may not be feasible due to latency and jitter, or even physical location, requirements where network switches are better suited. **Network access control (NAC)** is a growing capability that can support these niche use cases. FortiNAC and FortiSwitch offer this capability. For a mapping of the Fortinet solutions to the IEC 62443 framework, please see the illustration in the Appendix.

Conclusion

Through the relationships of the models provided in IEC 62443, implementation of this standard can help increase the security posture of an organization and ICS as a strategic, affordable and effective security program. Utilizing solutions such as the ones offered by Fortinet may improve the effectiveness of collaborating visibility, security controls and actionable response. Prevention, monitoring and response allow an organization to improve ICS security to align with the Standard and strengthen security operations.

Appendix



IEC 62443 Fortinet Coverage

Resource Availability (RA)
FR7
Identification and Authentication Control (IAC)
FR1
Timely Response to Events (TRE)
FR6
Use Control (UC)
FR2
FR5
Restricted Data Flow (RDF)
FR4
Data Confidentiality (DC)
FR3
System Integrity (SI)

1. FortiGate, FortiWiFi/FortiAP, FortiNAC FortiAuthenticator, FortiToken, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, FortiSIEM
2. FortiGate, FortiWiFi/FortiAP, FortiNAC, FortiAuthenticator, FortiToken, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, FortiSandbox, FortiSIEM
3. FortiGate, FortiWiFi/FortiAP, FortiAuthenticator, FortiToken, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, FortiSandbox, FortiSIEM, FortiTester, FortiResponder
4. FortiGate, FortiSwitch, FortiAP, FortiEDR
5. FortiGate, FortiSwitch, FortiNAC, FortiClient, FortiEDR, FortiAnalyzer
6. FortiGate, FortiClient, FortiEDR, FortiAnalyzer, FortiSIEM, FortiManager
7. FortiGate, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, Fabric-Ready Partner Solutions

Image updated on 4-15-2022

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®