Life Is On | Schneider Electric

# Practical Overview of Implementing IEC 62443 Security Levels in Industrial Control Applications

by Daniel DesRuisseaux
Director, Industry Cybersecurity Program
Schneider Electric

## Executive Summary

The demands of modern IIoT applications increases the complexity of systems infra-structure and puts additional pressure on IT and OT security. As the frequency and sophistication of cyber-attacks increase, operations must leverage industry stand-ards to achieve consistent protection.
This paper will address how IEC62443 can be applied to industrial control systems and help readers understand the various priorities and steps required to help miti-gate cyber threats.

# Table of Contents

## Introduction

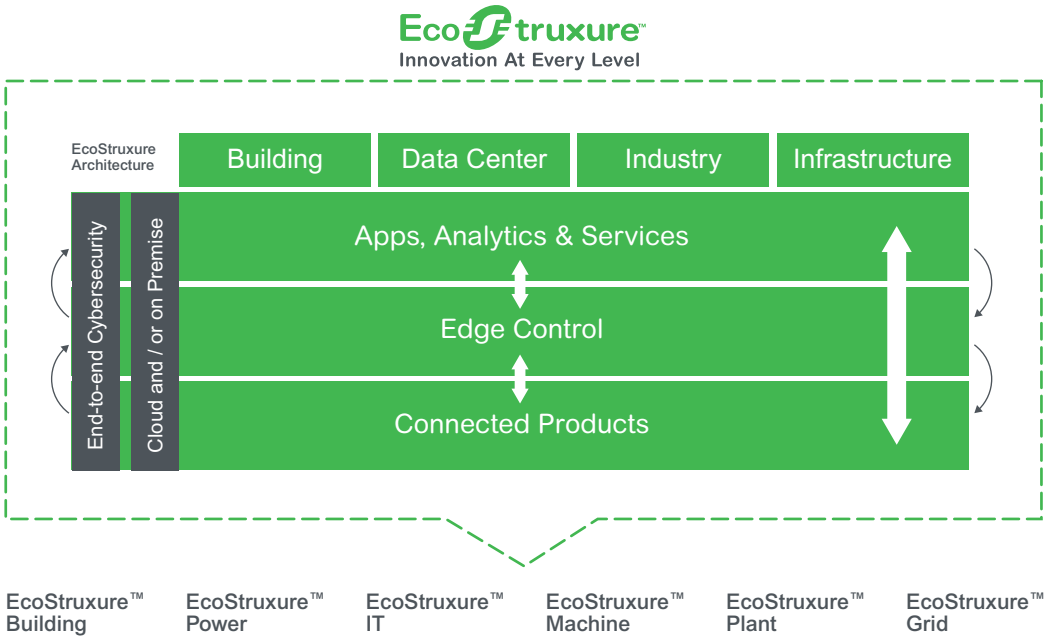
Industrial Control Systems (ICS) have experienced an exponential increase in cyberattacks over the last decade. The industry has responded to cybersecurity threats by creating standards to assist end users and equipment vendors through the process of securing industrial control systems. There are a number of key standards available in the market today. IEC 62443 has been developed by both the ISA99 and IEC committees to improve the safety, availability, integrity, and confidentiality of components or systems used in industrial automation and control. The IEC 62443 series of standards can be utilized across industrial control segments, and has been approved by many countries. IEC 62443 is evolving to become a key standard in the industry, and Schneider Electric is building its cybersecurity strategy around the standard.

This document is designed to introduce concepts to an individual with limited exposure to cybersecurity in industrial control systems. The document is designed to provide implementation guidance using practical examples. Note that this is a generic document designed to introduce concepts – the guidance provided herein should not be used to secure industrial control systems without examining specific networks in detail.

## EcoStruxure

EcoStruxure™ is Schneider Electric's open, interoperable, IoT-enabled system architecture and platform. EcoStruxure leverages advancements in the Internet of Things (IoT), mobility, sensing, cloud, analytics, and cybersecurity to deliver Innovation at Every Level. This includes Connected Products, Edge Control, and Apps, Analytics and Services. EcoStruxure has been deployed in 450,000+ installations, with the support of 9,000 system integrators connecting over one billion devices.

**Figure 1**




One of the key requirements of EcoStruxure architectures is underlying, end to end cybersecurity. In this whitepaper, we will examine how Schneider Electric utilizes standards-based techniques to secure its EcoStruxure solutions.

# Cybersecurity Concepts

In this section, concepts will be introduced that are necessary for understanding recommendations presented later in the paper.

## Security Assurance Levels

The IEC 62443 standard includes the concept of security assurance levels. The specification defines a series of requirements designed to bring system security to one of the four defined levels. A summary of each level coupled with a characterization of the type of attacker the security level is designed to address is presented in the table below.

**Table 1**

| Security Level | Target | Skills | Motivation | Means | Resources |
|---|---|---|---|---|---|
| SL1 | Casual or coincidental violations | No Attack Skills | Mistakes | Non-intentional | Individual |
| SL2 | Cybercrime, Hacker | Generic | Low | Simple | Low (Isolated Individual) |
| SL3 | Hacktivist, Terrorist | ICS Specific | Moderate | Sophisticated (Attack) | Moderate (Hacker Group) |
| SL4 | Nation State | ICS Specific | High | Sophisticated (Campaign) | Extended (Multi-disciplinary Teams) |

End users interested in providing a solution that is designed to address attacks from generic hackers or cybercriminals for example should implement a system with features specified in security assurance level 2. Note that the characterizations provided in the table are generic classifications to provide high level guidance to customers – implementing SL2 featured does not guarantee that a system can stop an attack from all hackers or cybercriminals.

## Defense in Depth

Defense in depth is the coordinated use of security countermeasures to protect the integrity of information assets in a network. Proper implementation of a defense in depth strategy involves the implementation of six steps. A brief summary of each step is provided below.

- *Create a Security Plan* – The most important step in the overall defense in depth process involves creating a security plan. In the security plan, personnel create a detailed audit of all of the equipment connected to the industrial control network, map how the equipment is connected, review the security configuration of equipment, and assess potential system vulnerabilities. The security plan includes the impacts of products, architectures, people, and corporate processes. A completed security plan is required before any additional steps can be taken to improve system security. Otherwise, the personnel may think a system is secure without being cognizant of potential attack vectors.

- *Separate Networks* – Once a detailed network map is created in the security plan, networks can be separated by a major function. An example would be dividing a network into an enterprise, plant, process, and field zones. All conduits between the zones should be identified.

- *Perimeter Protection* – In this step, conduits between zones are properly protected. An important part in this step includes securing remote access.

- *Network Segmentation* – In this step, zones created in step two can be divided into smaller zones based on location or function. The perimeters of these segmented zones are protected. It is important to note that the security level assigned to each zone can vary. For example, the security level tied to equipment in a monitoring role can be set to Level 1, while the security level ascribed to a safety system can be set to Level 3. The level of each segmented zone does not have to be same as its neighbors.

- *Device Hardening* – Adding features to ICS devices to improve their ability withstand a cyberattack. This reduces the likelihood that network elements will be compromised should a hacker gain access to a network.

- *Monitor and Update* – Actively monitoring the network activity to detect potential threats, and patch products as new software/firmware is made available to address vulnerabilities or to add security features.

Many industrial customers lack cybersecurity domain expertise. Schneider Electric has created a cybersecurity services practice to help these customers. Schneider security experts can help customers design and implement defense in depth strategies. Schneider Electric also offers a service enabling the vendor to actively monitor customer networks.

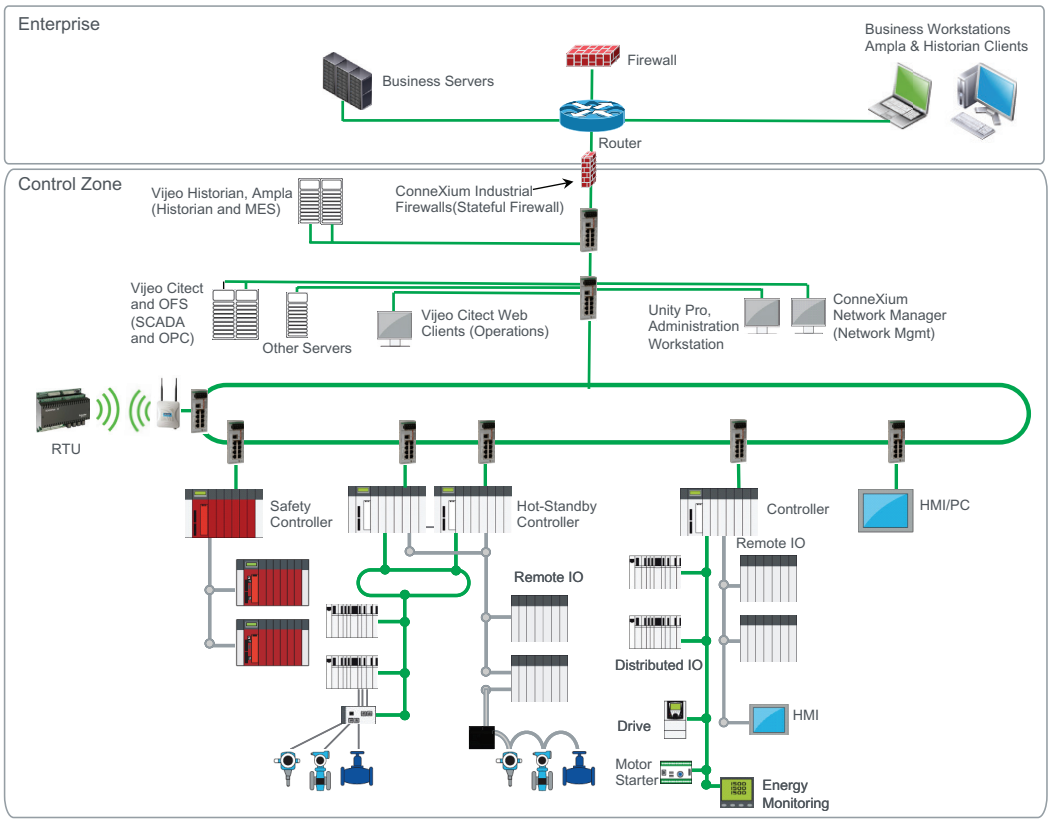
## Compensating Controls

Another important concept is compensating controls. If a product does not have the required security functionality, the system can still meet the requirements if the required functionality is provided by a different component in the system. For example, let's assume that a system uses an older PLC. The PLC lacks some of the required security features, but placing a firewall in front of the PLC provides the needed functionality to protect the PLC. The addition of the firewall will allow the system to pass the certification requirement.

## Format Overview

A sample network will be used to help illustrate the changes required to improve security at each of the target security levels. The sample network is presented below.

**Figure 2**




ICS components are deployed throughout the network, including controllers, safety systems, drives, and HMIs. The sample network is a generic industrial control system that could be used in a variety of industrial segments.

This paper will examine cybersecurity requirements for Ethernet based networks. Elements connected using serial based interfaces are not considered in the scope of the document.

In the remainder of this paper, the sample network referenced above will be modified to illustrate changes that will allow it to meet the requirements specified in each of the IEC 62443 security levels. The paper will focus on the first three security levels, as these will encompass the bulk of industrial applications. We will focus on system requirements as specified in the IEC 62443-3-3 system standard. Each of the security levels will be presented and coupled with a description of changes. The paper assumes that when the security level is increased, it will be increased for the entire network (specific network segments will not be set at different security levels) to simplify presentation.

The suggested changes will be the minimum required to enable the system to meet the target level. For example, a simple firewall can be used to segment networks in security level 1. A more advanced deep packet inspection firewall or a unidirectional gateway would provide greater security than a simple firewall, but additional security capabilities are not specified at this level – they may be specified at advanced levels. Customers can always use techniques specified in advanced levels to improve security in their systems.

The paper will also focus on products and architectures. Other aspects that can be defined in a security plan (personnel training, corporate security policies, etc.) will not be discussed.

## Security Level 1

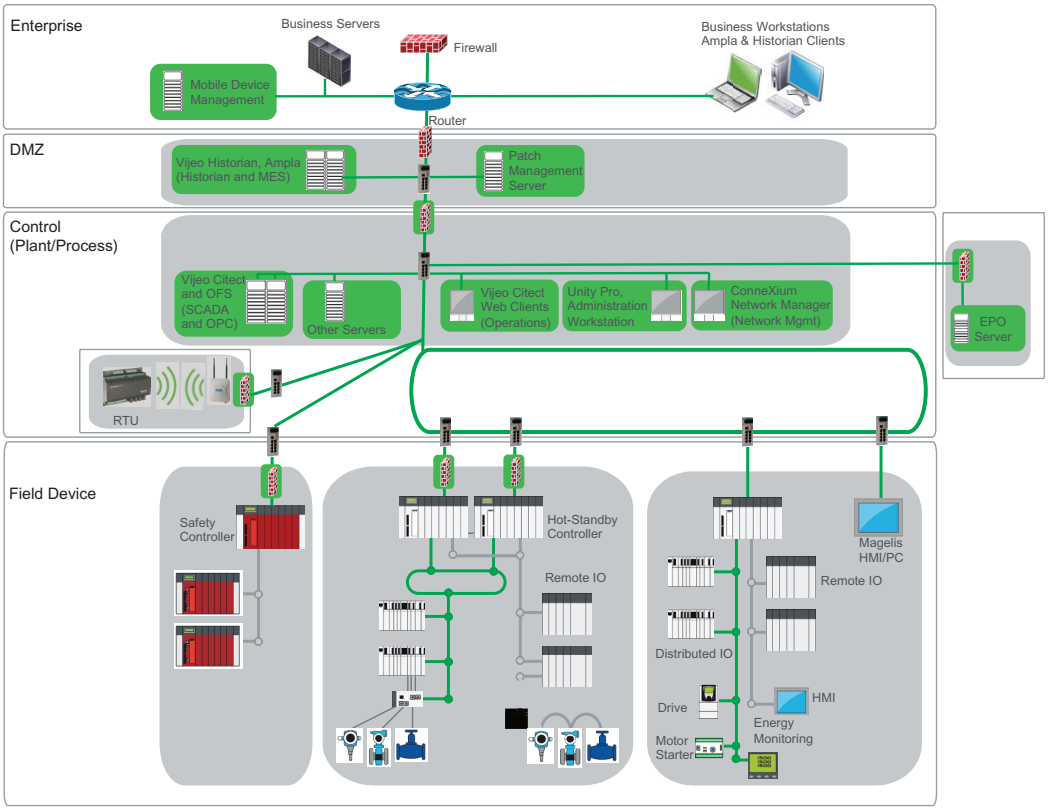
Security assurance level 1 (SL1) is designed to protect against casual or coincidental violations. The IEC 62443-3-3 specifications define a broad list of requirements necessary to obtain compliance to this security level. The table below summarizes key requirements specified in SL1. Note that IEC 62443-3-3 specifies 37 individual requirements. The table below attempts to provide a high-level overview of 14 of the major requirements. Parties interested in details should refer to the IEC standards.

**Table 2**

| Item # | Requirement | Technique to satisfy requirement |
|---|---|---|
| 1 | Control system can authenticate and authorize human users. User accounts can be created and managed. Configurable password strength. Track unsuccessful login attempts. | End user accounts created in devices or centralized authentication server. |
| 2 | Control system can authenticate and authorize wireless users. | Mobile devices and network infrastructure authenticates users. |
| 3 | Control system shall provide the ability to monitor and control access from untrusted networks. | Firewalls monitor traffic from untrusted networks. |
| 4 | Control system shall be able to restrict code embedded in e-mail or on storage media. | EPO server can restrict interactions with mobile devices. |
| 5 | Control systems shall provide the capability to generate audit records. | Audit records/logs generated by equipment. |
| 6 | Control system shall protect the integrity of transmitted information. | Equipment supports encrypted protocols, robust check sums/hashing. |
| 7 | Control system shall detect, prevent, and report the effects of malicious code. | Application whitelisting enabled on end devices. |
| 8 | Control system shall protect the confidentiality of information at rest or in transit. | Equipment supports user names and passwords for authorization |
| 9 | Control system shall segment networks and protect boundaries. | Firewalls segment networks and protect boundaries. |
| 10 | Control system shall be able to prevent messages being received from external users or systems. | Firewall can filter messages from external networks. |
| 11 | The control system shall provide the capability to support partitioning of data, applications, and services based on criticality to implement a zoning model. | Networks should be segmented using zone and conduit modeling. |
| 12 | Control system shall operate in degraded mode during denial of service event. | Network elements (switches, routers, etc.) support rate limiting. |
| 13 | Prohibit unnecessary functions, ports, protocols, and services. | ICS devices have the ability to disable unnecessary capabilities. |
| 14 | Control system shall conduct backup of user and system level information. | Backup files available within individual devices. |

Implementing SL1 requirements impact the network architecture. SL1 requires implementation of defense in depth steps, in particular segmenting networks and protecting zone boundaries. Changes to the sample architecture are highlighted below.

**Figure 3**




In this example, the control zone from the sample network has been broken into seven smaller zones highlighted in grey. New elements are highlighted in green. The zones are:

- *Demilitarized Zone (DMZ)* – A subnetwork that contains and exposes the external facing services of the control zone to the enterprise network. Servers in the enterprise zone should never be directly connected to elements within the control zone. Yet business systems need access to control zone data, and elements in the control zone need access to files originating from untrusted networks (firmware updates for example). The DMZ contains systems that need to access both the control and enterprise equipment.

- *Plant/Process Zone* – Zone hosting products and applications enabling plant and process management.

- *Security Appliance Zone* – Centralized zone hosting a variety of security appliances.

- *Wireless Zone* – Wireless infrastructure is separated into a separate zone.

- *Controller Zones* – In this example the field device area has been broken into three zones. Two are standard control zones, and one is a safety controller zone. Zone segmentation is a product of the security plan and will vary based on the application - this is simply an example.

Industrial grade firewalls (highlighted in green) have been added to segment the network. In addition, an EPO server and Mobile Device Management server have been added along with application whitelisting software for servers hosting ICS software.

## Security Level 2

The security assurance level 2 specification includes requirements specified in security level 1, and adds the following requirements. Note that IEC 62443-3-3 specifies 23 individual requirements, we have simplified the list into 11 major requirements. Parties interested in details should refer to the IEC standards.

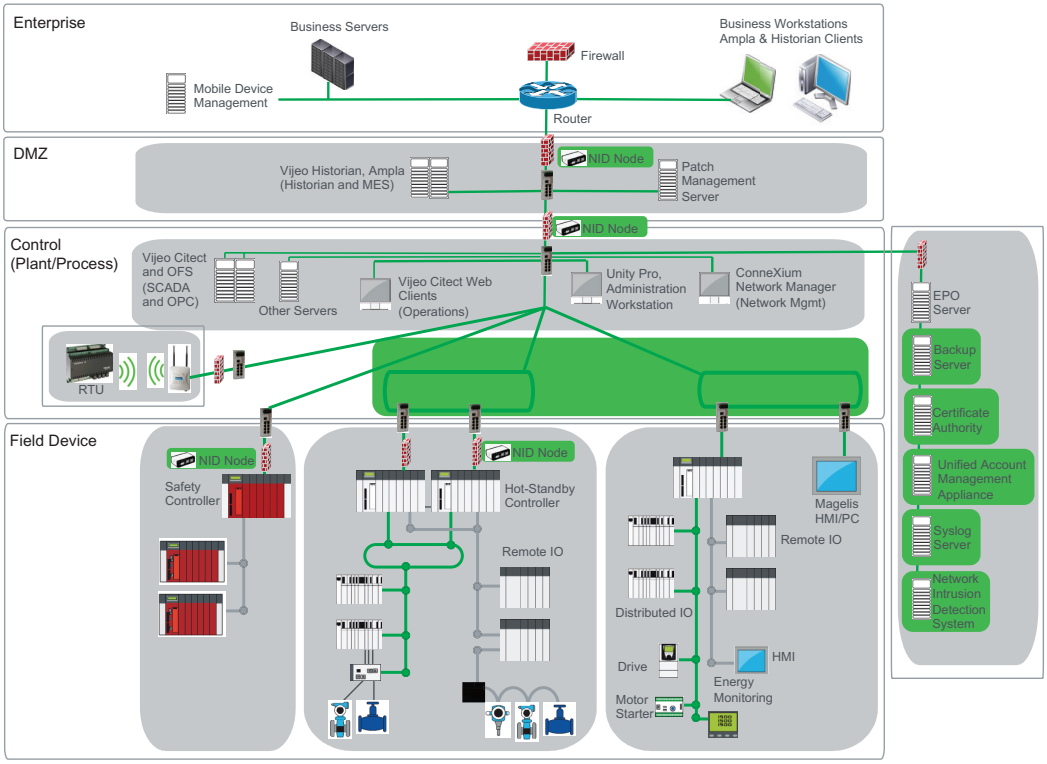
**Table 3**

| Item # | Requirement | Technique to satisfy requirement |
|---|---|---|
| 1 | The control system shall authenticate and authorize software processes and devices. | Software and devices authenticate using certificates. |
| 2 | The control system shall authenticate human and software users engaged in wireless communications. | Mobile devices and network infrastructure authenticates users against centralized authentication server. |
| 3 | The control system shall support standard PKI and certificate-based authentication if used. | Certificate authority added in control network to issues certificates. |
| 4 | The control system shall be able to deny access requests from untrusted networks unless approved by an assigned role. | Feature enabled in end devices. |
| 5 | The control system shall enable authorized users to define and modify mapping of permission to roles. | Roles and permissions enabled in devices or unified account management appliance. |
| 6 | The control system shall employ malicious code protection at all entry and exit points. | Network Intrusion Detection System support provides malicious code protection. Centralized server implemented with remote nodes protect networks. |
| 7 | The control system shall protect the integrity of sessions | Equipment supports encrypted protocols. |
| 8 | The control system shall protect the audit information | Event server employed as centralized repository for equipment records. End devices forward records to event server. |
| 9 | The control system shall protect confidentiality in remote access traversing an untrusted network. | VPN initiated from firewall secures remote access connections. |
| 10 | The control system shall provide the capability to physically segment control system networks from non-control system networks. | Communication from critical systems transported over different networks than non-critical systems. |
| 11 | The control system shall report list of installed components with associated properties. | Data recorded in repository - capability can be provided by Intrusion Detection System. |

It is important to note that some of the requirements are enhancements to requirements specified in security level 1, and some are new requirements. For example, in security level 1, the system must authenticate and authorize human users. In security level 2, the system must also authenticate and authorize software processes and devices. In security level 1, the system must detect, report, and prevent malicious software. In security level 2 the system must detect, report, and prevent malicious software at all zone entry and exit points. In some cases, new requirements are added like the ability to support certificates for authentication.

Some of the specifications require products to be added to the network. A unified account management appliance, Certificate Authority, Back-up Server, Event Server, and Network Intrusion Detection System have been added to the network and highlighted in green below. In addition, the control network has been segmented into two separate networks. Note that the potential ICS device replaced to support new features required in SL2 (having to upgrade to a new PLC that supports secure protocols for example) are not captured in the diagram.

**Figure 4**



## Security Level 3

The security assurance level 3 specification includes requirements specified in security level 2, and adds the following requirements. Note that IEC 62443-3-3 specifies 30 individual requirements, we have simplified the list into 12 major requirements. Parties interested in details should refer to the IEC standards.

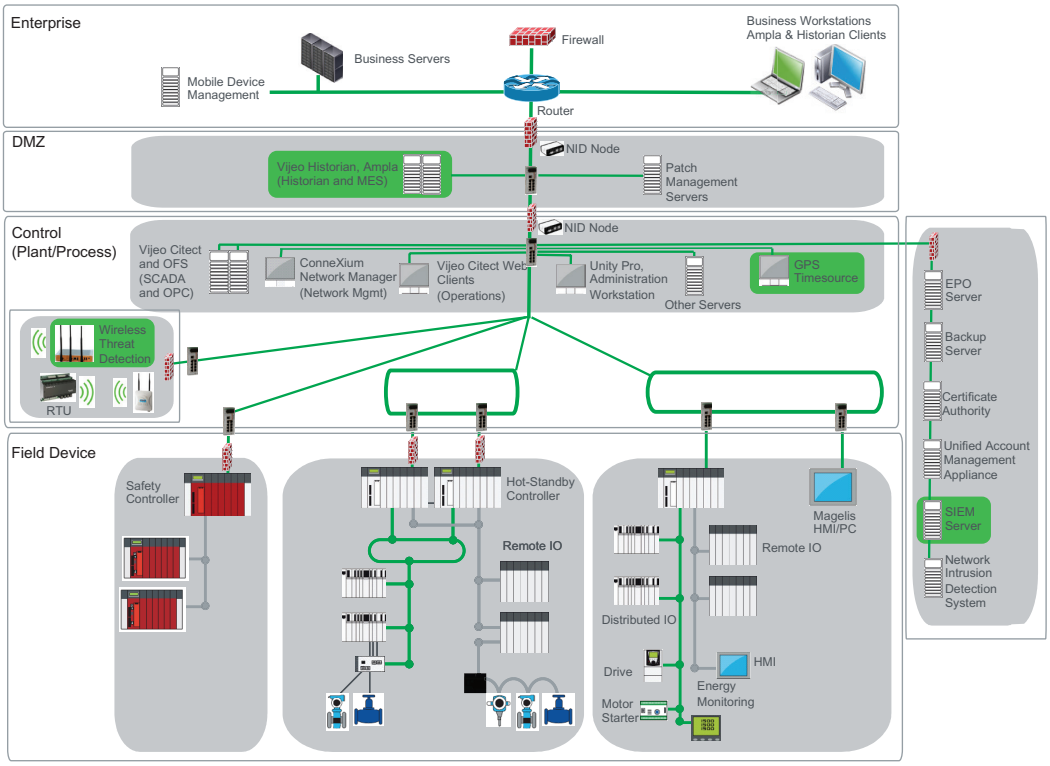
**Table 4**

| Item # | Requirement | Technique to satisfy requirement |
|---|---|---|
| 1 | The control system shall support multi-factor authentication for untrusted interfaces. | Feature enabled through centralized account management and end devices. |
| 2 | The control system shall uniquely identify and authenticate software processes. | Feature supported through certificate authority. Secure protocols can also be utilized. |
| 3 | The control system shall support unified account management. | Unified account management enabled through centralized account management. |
| 4 | The control system shall protect private keys using hardware mechanisms. | Secure element in ICS equipment. |
| 5 | The control system shall identify and report unauthorized wireless devices | Identification of unauthorized wireless devices through the addition of wireless threat detection device. |
| 6 | The control system shall verify the integrity of mobile code before allowing execution. | Mobile code integrity verified from the EPO server and certificate authority. |
| 7 | The control system shall provide a centrally managed system wide audit trail. | End devices forward log files to SIEM server. |
| 8 | The control system shall synchronize internal system clock at configurable frequency. | GPS time source added to network. |
| 9 | The control system shall support cryptographic mechanisms to recognize changes to information during communication. | Enabled through the use of secure protocols. |
| 10 | The control system shall centrally manage malicious code protection mechanisms. | Malicious code is protected via the EPO server and SIEM server. All detected issues are forwarded to the SIEM server. |
| 11 | The control system shall support automated backup based on configurable frequency. | Automated backup function is supported in the backup server. |
| 12 | The control system shall report the current security settings on end devices. | The EPO Server coupled with network management systems report security settings. |

A number of the SL3 requirements are implemented in ICS components. Examples include mandatory secure protocols, and the use of secure elements to protect keys. In security assurance level 2, required features could be implemented via new software. In security assurance level 3, equipment will likely have to be replaced/redesigned.

Some of the specifications require products to be added to the network. For example, the event server that was added at security level 2 will have to be updated to a SIEM server to accommodate security level 3 requirements. In addition, a GPS time source and a wireless threat device have to be added.

**Figure 5**




## Product and System Certification

The IEC 62443 standard defines requirements for product and system security levels. These requirements provide value to both end users and equipment vendors.

- *End Users* – End users traditionally evaluate vendor products based on criteria including feature content, price, and delivery terms. Specifying features can be a complex process. IEC 62443 simplifies the process of defining cybersecurity requirements by allowing end users to specify a target security level vs. defining a cumbersome list of individual features. End users will know the exact features available in equipment based on its compliance with the IEC 62443 standards.

- *Equipment Vendors* – Equipment vendors can differentiate their solutions from competitors via the IEC 62443 standards. Traditionally, it has been difficult to clearly show that one solution is more secure than a competitive solution, as each may have a different set of cybersecurity features. Vendors who design and certify solutions to the security levels as defined in the IEC 62443 standard can clearly differentiate cybersecurity capabilities by marketing a product certified to level 2 standards vs. competitive products that may be at level 1.

Vendors can pursue both certification for end devices (as specified in IEC 62443-4-2) or systems (as specified in IEC 62443-3-3). In both cases, compliance to standards should be validated by an independent third party. End users should adopt cybersecurity certifications to their equipment purchasing requirements.

## Conclusion

The IEC 62443 specification provides essential guidance to end users who seek to secure industrial solutions. The security assurance level framework helps to group cybersecurity requirements to aide implementation. Increasing system security can result in the need to upgrade older ICS equipment, and to purchase new cybersecurity appliances. Required expenditures and implementation complexity will increase with targeted security level.

A detailed security plan is essential before initiating any work to secure an industrial solution. Secure products and architectures are only part of the solution - personnel training coupled with sound corporate security policies are essential to secure industrial control systems.

## About the author

**Daniel DesRuisseaux** possesses over 25 years of diverse experience in engineering, sales, and marketing roles in high tech companies. Mr. DesRuisseaux presently serves as a Cybersecurity Director for Schneider Electric's Industrial Division. In this role, he works to insure the proper and consistent implementation of security features across Schneider Electric's diverse industrial product portfolio.

## Contact Us

For more information, please visit our website at:
https://www.schneider-electric.com/en/work/solutions/cybersecurity/

**Schneider Electric Software**
26561 Rancho Pkwy South, Lake Forest, CA 92630 Telephone: +1 (949) 727-3200 Fax: +1 (949) 727-3270 software.schneider-electric.com


PN SE-998-20186845_GMA-US Rel. 01/18