Effective Implementation of Cybersecurity Countermeasures in Industrial Control Systems

by Daniel DesRuisseaux
Director, Industry Cybersecurity Program
Schneider Electric
# Table of Contents

- **Introduction** ........................................................................................................... 3
- **Security Lifecycle** ................................................................................................. 3
- **Output of Assessment Phase** .................................................................................. 3
- **Implementation Phase** ............................................................................................ 4
- **Security Requirements** ......................................................................................... 4
- **Design Specification** ............................................................................................... 4
- **Creating a Detailed Project Plan** ............................................................................. 4
- **Implementation** ......................................................................................................... 4
  - System Hardening ................................................................................................... 5
  - Software Hardening ................................................................................................. 5
  - Device Hardening .................................................................................................... 5
  - Network Hardening ................................................................................................. 5
  - Deploying Security Appliances ............................................................................. 5
  - Select the Security Appliance .............................................................................. 6
  - Install and Configure Security Appliance ............................................................ 6
  - Test the Security Appliance .................................................................................... 6
  - Deploy the Security Appliance .............................................................................. 6
  - Plan for Ongoing Appliance Management .............................................................. 7
- **Access Control** ......................................................................................................... 7
- **Remote Access** ......................................................................................................... 7
- **Acceptance Testing** ................................................................................................. 7
- **We Can Help** ............................................................................................................. 7
- **Conclusions** .............................................................................................................. 7
Industrial Automation Control System (IACS) operators recognize the need to improve cybersecurity, but many lack the understanding on how to start the process. End users attend cybersecurity conferences, webinars, or read articles in the trade press and learn about specific cybersecurity topics – like threat detection or defense in depth architectures. Many are tempted to start to take concrete steps to improve security – but it is critical to first create a detailed plan prior to acting. Once a plan is created, end users should follow a defined deployment process. In this whitepaper, we will provide a detailed description of the deployment process.

There are several standards that touch on industrial cybersecurity. ISA/IEC 62443 is a major standard for IACS that is backed by both end users and equipment vendors. The standard is written to be applicable across industrial segments and has been accepted by many countries. The ISA/IEC 62443 standard defines the cybersecurity lifecycle - a powerful framework used to secure IACS. The cybersecurity lifecycle is a process consisting of four major phases, and each phase can be broken into multiple steps. The cybersecurity lifecycle is depicted in Figure 1.

**Assessment Phase**—Analyze the IACS. Organize assets into zones and define communications conduits between the zones. Define vulnerabilities, calculate risk, and prioritize based on relative risk.

**Implementation Phase**—Input from the Assessment Phase if utilized to create detailed security requirements. The requirements are in turn utilized to design and implement countermeasures. Countermeasures could be technology, corporate policies, or organizational practices (training, accountability, etc.).

**Maintenance Phase**—The organization actively monitors the IACS, responds to incidents, performs maintenance tasks (back-up, patching, etc.) and manages change.

**Continuous Improvement**—Lessons learned from incidents are analyzed and necessary changes are implemented. Periodic audits are conducted.

In this white paper, we will focus on the Implementation Phase, as it is critical to the successful deployment of countermeasures. A separate paper “Cybersecurity Assessment – The Most Critical Step to Secure an Industrial Control System”, is available that describes the Assessment Phase in detail.

At the conclusion of the Assessment Phase, the team should have created the following documents:

- Architecture Diagrams
- Network Diagrams
- Asset Inventories
- Vulnerability Report
- Zone and Conduit Drawings
- Risk Analysis Report
The documents produced as a result of the Assessment Phase are key to initiating the Implementation Phase of the security lifecycle. For more information on these deliverables, refer to the Schneider Electric white paper “Cybersecurity Assessment – The Most Critical Step to Secure an Industrial Control System”.

The Implement Phase is comprised of a variety of sub-tasks. Each will be detailed below. One of key factors that will influence success of the overall effort is the creation of a strong project team. The design and implementation of security countermeasures is a complex project and should be managed as such. Activities should be planned, documented, and executed throughout the Implementation Phase.

The project team should consist of personnel with knowledge of the process, the OT control network, and the IT network. A strong project manager should be assigned to manage the project team.

Security Requirements
The first step in the implementation phase involves the definition of requirements. Examples of requirements include features tied to the specific countermeasure (firewall, IDS, SIEM, etc.), and requirements that must be supported by all components that comprise the system. Examples of system requirements include regulatory requirements, monitoring requirements, configuration requirements, environmental requirements, and access control requirements. For example, all element in the system must be able to output log data in a specified format. Or all elements must interface to a defined network clock to ground log information.

Requirements are captured in cybersecurity requirements documents. There can be multiple requirements tied to an overall project. The requirements document should capture all requirements, and should also define detailed use cases.

Design Specification
The requirements document specifies features that the system must support, the design specification details how the system addresses the requirements. Multiple design elements can be tied to each requirement. The design document typically contains a variety of sections to clearly define how the system works, including architecture diagrams, network diagrams, and use cases.

Creating a Detailed Project Plan
Once the design is complete, the project team will create a detailed project implementation plan. The plan will fully define the overall project, and should include the following sections:

- Project goal
- System scope
- Project deliverables
- Budget
- Resource requirements
- Dependencies
- Risks
- Schedule

Implementation
Securing a system typically requires the combination of two major efforts – hardening industrial components and deploying security appliances. Both items will be covered in detail in this paper. We will begin by describing system hardening. A system is typically compromised of hardware, software applications, and network devices. Each of these elements will have to independently hardened.
It is important to note that system hardening alone is not enough to protect an IACS. Additional employee training and corporate security policies are additionally required. Examples include policies that restrict employee access to critical locations, and prevent the attachment of memory sticks to IACS equipment. This paper is focused on effective deployment of countermeasures.

System Hardening
Hardening refers to a process utilized to secure a system by reducing its attack surface. Examples of techniques that can be used to reduce attack surface include the removal of unnecessary software, user accounts, unnecessary services, and installing security patches to address known vulnerabilities. The removal of unnecessary items prevents a hacker from using the item to compromise a system. An IACS is composed of a variety of devices including, databases, software applications, networking equipment, PLCs, and drives to name a few. Each of these devices can be individually hardened.

Software Hardening
Software hardening can refer to both OS and software application hardening. Techniques include patching software, removing or disabling unnecessary services/protocols, and configuring proper access controls. One key step involves removing unnecessary software – such as servers. Removing such software significantly reduces the attack surface. Software hardening guidance is available from a variety of sources including National Institute of Standards and Technology (NIST), and security guidelines from automation equipment manufacturers.

Device Hardening
In IACS, devices refer to products with embedded software that is involved in the industrial process. Examples of devices include PLCs, DCS systems, HMIs, drives, sensors, and I/O. Hardening techniques will vary by device. Examples include enabling logs, changing default passwords, installing firmware updates, disabling remote programming changes, and disabling unused services/protocols. Device hardening guidelines are available from NIST and IACS vendors.

Network Hardening
A network is comprised of a variety of elements, including switches, routers, firewalls, and gateways. Network devices can be hardened using many of the same techniques discussed earlier - installing firmware updates, changing passwords, and reviewing logs. There are a few techniques special to networking equipment, including disabling unused physical switch ports, and using protocols to validate that elements can connect to the network. Network hardening guidelines are available from NIST, the National Security Agency (NSA), and network equipment providers.

Deploying Security Appliances
Hardened devices cannot by themselves effectively secure a system. For example, let’s consider a traditional industrial system. The system consists of a PLC, an HMI, a management workstation, and some drives. Each of the devices can be hardened to reduce its attack surface. But additional security appliances may be required to secure the system. Some examples of security appliances are provided below.

- **Firewalls** – Use rules to control incoming and outgoing network traffic. Firewalls can be or hardware or software based.

- **Intrusion Detection Systems** – Can be host or network based. Monitors events occurring in a system and detects possible incidents. Incidents generate alerts that are forwarded to the system administrator.

- **SIEM** - Used to aggregate logs from IACS equipment and generate reports that are valuable for troubleshooting and compliance purposes.
- Data Diode – Enables more stringent network segmentation by restriction traffic flow to a single direction.

- Certificate Authority – An appliance that issues digital certificates. Digital certificates are used to authenticate individuals / equipment and secure protocols.

The process tied to the effective deployment of security appliances is influenced by the appliance in question. For example, the process to deploy a firewall will differ from the process used to deploy a SIEM. The process can be divided into five major phases. To better illustrate concepts, we will walk through each of the steps assuming that we are deploying a firewall.

**Select the Security Appliance**
Device selection is influenced by the risk assessment the and system architecture created as part of the Implementation Phase, as well as the security requirements document discussed earlier. The team uses the information to select the technology, and ensure that the necessary features are supported by the appliance. A secondary task associated with selection involves determining where the appliance will be placed in the network and determining if the existing architecture will change.

As an example, let’s assume the team needs to deploy a firewall. The team would have to determine the locations where the firewalls would be placed to segment the network, and determine the firewall requirements for each placement. There are a variety of firewall types, including stateful inspection firewalls and deep packet inspection firewalls. Each firewall type has different capabilities. The team could determine that a stateful inspection firewall would be required at one location, while a deep packet inspection firewall would be required at a second location. Detailed requirements designed to guide selection would be developed for each prior to selection.

**Install and Configure Security Appliance**
Once the appliance is selected, the team works with organization to have it installed. In this stage key stake holders in the organization are informed and consulted, and an installation schedule is created. The appliance is installed at the agreed upon time. The installation consists of the physical installation coupled with equipment configuration.

We will again utilize a firewall to illustrate the process. The firewall would be installed in the network. The firewall policies would be designed and configured. Configuration include the creation of Access Control Lists which define source and destination addresses, port numbers, and packet flow direction. Additional deep packet inspection rules can be created for specific protocols.

**Test the Security Appliance**
Once the appliance is installed, it should be tested. A test plan should be written and approved by the organization in advance of testing. Test results are documented - any tests that have failed should be reviewed and addressed/waived by the organization.

We will utilize a firewall again to illustrate the test phase. For a firewall, examples of areas that would be tested include device performance, interoperability, and logging. In addition, there may be specific features that should be tested, such as the ability to filter specific protocols.

**Deploy the Security Appliance**
Once the appliance has been tested, it can be formally deployed. During this phase, key departments will be notified that the appliance is operational. Additional monitoring may be required to insure the appliance is not impacting network performance. Device configuration files should also be backed up.
Plan for Ongoing Appliance Management

In the final phase, the team plans for ongoing maintenance of the appliance. The maintenance phase will require the appliance to meet corporate security rules. Key topics addressed in this phase include patching, the ability to track and verify configuration changes, and auditing.

Access Control

Access control refers to policies and technologies implemented to control access to control networks. Properly implemented access control define techniques to create, modify, and remove user accounts. Features typically associated with access control include role based access control, multi-factor authentication, session lock, and concurrent session control.

Remote Access

A critical task to consider when securing an IACS involves effectively managing remote access. Remote access provides significant operational benefits, but it also introduces significant risk as it provides a path for individuals outside of the facility to access the control system. Typical remote users include vendors, system integrator, field technicians, customers, managed service providers, regulatory agencies, and remote operation personnel.

Several variables can impact the design of remote access solutions, including:

- Role of users
- Quantity of users
- IACS nodes accessed
- Security level of accessed elements
- Performance requirements
- Regulatory and policy restrictions
- Services

Some examples of remote access best practices include using two factor authentication for access, encrypting traffic traveling through untrusted networks, enable on-demand session termination, and requiring corporate owned laptops meeting company security policies for access.

There are a variety of technologies available today secure remote access solutions. End users must evaluate security features, potential risk, and cost to select the best alternative for their application. Remote access guidelines are available to assist end users.

Acceptance Testing

Applications may require additional system cybersecurity acceptance testing prior to implementation. Acceptance testing can take place at the factory, a staging site, or both.

Cybersecurity acceptance testing is designed to accomplish two objectives. The first objective verifies that the system meets cybersecurity design requirements. In this phase, the testing verifies that the security settings of IACS devices are properly configured, that security appliances are properly installed and configured, that detection appliances are operational and able to identify and report events, and that access controls are properly configured and effective.

The second objective focuses on proving that the system is robust. In this phase, penetration testing is conducted to ensure that the system can resist attacks. The system will be scanned for vulnerabilities, and the system will be challenged by a variety of attacks.

There are many published accepting test guidelines and best practices that can be used as references to create detailed test plans. Documentation detailing the test plan and results is required prior to the release of the system to operations.
Many industrial customer lack or are trying to build cybersecurity domain expertise. Schneider Electric has created a cybersecurity services practice to help these customers. Schneider security experts can help customers through the Deployment Phase, or any other phase in the Security Lifecycle. Please contact your Schneider Electric sales representative if you are interested in cybersecurity services.

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.

In conclusion, the threat of cyber-attack will continue to be an issue plaguing IACS for the foreseeable future. IEC 62443 standards create a framework that allows operators to strengthen system security. The key first step in the process is the Assessment Phase, which enables end users to analyze their system and understand which threats to address first. Countermeasures are deployed in the Implementation Phase - the process outlined in this paper can assist end users through this process. Schneider Electric has experience with both IACS and cybersecurity, and is available to assist operators attempting to security industrial solutions. The key is to stop waiting and avoid analysis paralysis – it is better to begin to implement counter measures and improve them over time than to wait.

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/