Life Is On | Schneider Electric

# Effectively Maintaining the Security of Industrial Control Systems

by Daniel DesRuisseaux
Director, Industry Cybersecurity Program
Schneider Electric

# Table of Contents

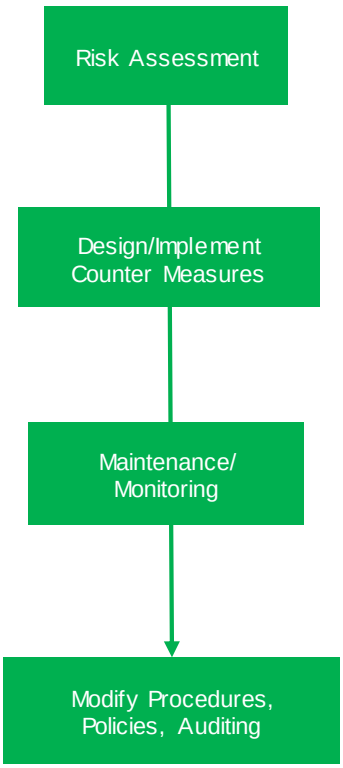
# Introduction

Industrial 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. Once systems have been deployed, a process must be utilized to ensure that systems are effectively managed and monitored. In this whitepaper, we will provide a detailed description of the tasks associated with ongoing maintenance.

# Security Lifecycle

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. The cybersecurity lifecycle is depicted in Figure 1.

**Figure 1: Security Lifecycle**




**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 Maintenance and Continuous Improvement Phases, as they are critical to the ongoing security of industrial control systems. Separate whitepapers are available that cover the Assessment and Implementation Phases:

- "Cybersecurity Assessment – The Most Critical Step to Secure an Industrial Control System" describes the Assessment Phase in detail.
- "Effective Implementation of Cybersecurity Countermeasures" describes the Deployment Phase in detail.

# Maintenance Phase

The Maintenance Phase consists of a variety of independent activities that must be effectively managed on an ongoing basis. Activities can be divided into 2 key types – those that occur on a continual basis, and those that are event driven. Each will be discussed in detail.

## System Monitoring

There are two key activities that undertaken by the organization while the IACS is operational – asset monitoring and security monitoring.

## Asset Monitoring

Ongoing monitoring of the network to track devices connected to the system, and whether elements are using the latest software versions. Any new devices added to the system should be fully investigated. Asset monitoring capabilities are typically provided by internal or third-party tools and applications.

## Security Monitoring

A variety of security appliances could have been added as part of the implementation phase of the security lifecycle, including network intrusion detection systems, host intrusion detection systems, SIEMs, anti-virus applications, and endpoint protection systems. This activity is focused around monitoring the technologies that has been implemented to detect malicious activity. Alarms raised by these systems should be evaluated using the Incident Handling process that will be defined later in this paper.

Security monitoring is typically not as simple as having personnel look at the alarms each morning. Personnel must have in depth knowledge of the monitoring applications, will have to be cognizant of false positives, and may have to tweak configuration rules to optimize accuracy.

## Event Driven Maintenance

In addition to activities that operate in the background, there are a variety of incident driven components of the Maintenance Phase.

## Patch Management

Patches are utilized by equipment vendors to address vulnerabilities, and thus are critical to system security. Patches can also be applied to endpoint protection systems and intrusion detection systems to update malware signatures. Traditionally, companies with IACS have updated software during scheduled system outages. This methodology is not compatible with security requirements. IACS must be able to accommodate security patching between scheduled outages.

Potential patches should be evaluated prior to installation on the system. A patch may address a vulnerability that is not an issue for an IACS, in which case it should not be installed. For example, a patch to address a vulnerability with FTP is not an issue for a device where FTP has been disabled. The new patch should be analyzed to determine if there are any new vulnerabilities that could lead to greater risk than the addressed vulnerability. Patches should also be tested in a sandbox environment prior to deployment in a production network.

The patch management process can be simplified if companies with IACS equipment maintain a list of all patchable devices/applications. A process should be specified requiring employees to regularly review patchable software to monitor disclosed vulnerabilities.

Windows based device patch management can be centralized via the Windows Server Update Services (WSUS). Software patches for other equipment are typically loaded from the enterprise to a patch server that is located within the Demilitarized Zone between that the enterprise and control network.

## System Backup

Companies with IACS typically have policies that defines their system backup process. The policy will define elements requiring backup, backup interval, number of backups, manual vs. automatic backup, backup schedules, file storage locations (must be in secure location), and how to properly dispose of backup systems that have reach end of life. Policies may also require features like code signing to insure the integrity of backed up files. It is important to note that both file backup and restore functionality should be regularly audited to insure the system is functional should the company experience a security related incident.

## Change Management

During the implementation phase, system architecture diagrams, network diagrams, and asset inventories were created. A variety of additional documents were created during the Implementation phase. Changes will occur when the system is operational – new products will be added/removed, networks will change, devices will be replaced. Each change may require changes to system documentation. A formal change management process should be utilized to ensure that changes are effectively requested, decided on, implemented, and documented. Otherwise documentation will not be accurate which could lead to issues when troubleshooting incidents.

## Incident Handling

A critical process in the Maintenance Phase is incident handling. Incident handling creates a plan to deal with unauthorized intrusion, cyber theft, denial of service, malicious code, and other security related events. The key deliverable is the creation and socialization of an incident response plan. The plan can be broken into six major steps.

**Figure 2: Incident Handling Process**


- Preparation - The first and most critical step of the process. Tasks associated with this step are performed prior to an incident. In this step, incident handling policies are created. These policies should be reviewed and approved by management. Key elements of the plan include recovery plans, communications plans, personnel training, and the creation of detailed procedures.

- Identification – In this step, procedures are created to help identify and respond to incidents. Criteria must be created to characterize potential incidents, and personnel must be identified who can make decisions. Once an incident has been identified, key personnel should be identified, including a primary handler, and tracking tickets should be created.

- Containment – In the step, the source of the incident is isolated. The process begins by making a forensically sound backup of all infected systems. One copy should be made for evidence should the company decide to pursue legal action (refer to chain of custody at the end of the section). All passwords should be changed immediately to prevent unauthorized access to compromised accounts.

- Eradication – In this step, the issue is addressed. Reparation is not as simple as loading the latest backup, as the backup could also be infected. It is safer to rebuild the software by starting with a clean initial file and adding updates. Note that rebuilding to the latest state is not enough – there is nothing to prevent the issue from occurring again. The underlying vulnerability must also be addressed. Configuration files must also be studied to identify and remove backdoors.

- Recovery – In this step, the application is restored to a functional state. The application must be validated prior to restoration to service, and performance should be closely monitored during initial hours of operation.

- Lessons Learned – In the final step, the organization identifies areas that could have been improved in the incident handling process, and then initiates steps to implement required changes. Refer to the Continuous Improvement section of the document for more details.

One additional concept that should be touched on involves the legal aspects of incident handling. Companies should be cognizant of concepts like chain of custody and evidence integrity during the incident response process in cases where legal action will be taken. Employees involved in the incident handling process should be trained appropriately.

## Continuous Improvement Phase

The Continuous Improvement Phase is very closely related to the Maintenance Phase. In fact, it's activities typically occur simultaneously with Maintenance Phase activities. The major differences between the two phases are activities in the continuous improvement phase are undertaken specifically to improve the documented processes of the Maintenance Phase. There are two specific activities tied to the Continuous Improvement Phase.

### Lessons Learned

A variety of individual processes can be running at any given time. Each process may conclude with a lessons learned step. It is important to consciously evaluate whether items discussed during the lessons learned step should impact existing processes, procedures, or component configurations. Any changes should be undertaken through the change management process.

### Auditing

Companies should create a comprehensive plan to audit key cybersecurity related policies and procedures on a regular basis. The priority of the policy/procedures drive the audit schedule. Examples of audits include:

- Risk assessment process
- System hardening configuration settings
- Secure appliance implementation process
- Change management process audit
- Asset monitoring audit
- Patch management process audit
- Software backup process audit
- System recovery audit
- Incident response audit
- Physical security policy/procedure audit

Audits will examine both the active process and artifacts generated by the process. Audit results should be presented to executive management. Audit findings can result in changes to existing policies and procedures.

## We Can Help

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 Maintenance and Continuous Improvement Phases, or any other phase in the Security Lifecycle. Please contact your Schneider Electric sales representative if you are interested in cybersecurity services.

# Conclusion

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 overall system is then managed using the processes defined in this whitepaper. 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/

Part Number 998-20304109_GMA-US
© 2018 Schneider Electric. All rights reserved.