Life Is On | Schneider Electric

Cybersecurity Assessment – The Most Critical Step to Secure an Industrial Control System

by Daniel DesRuisseaux
Director, Industry Cybersecurity Program
Schneider Electric

Table of Contents

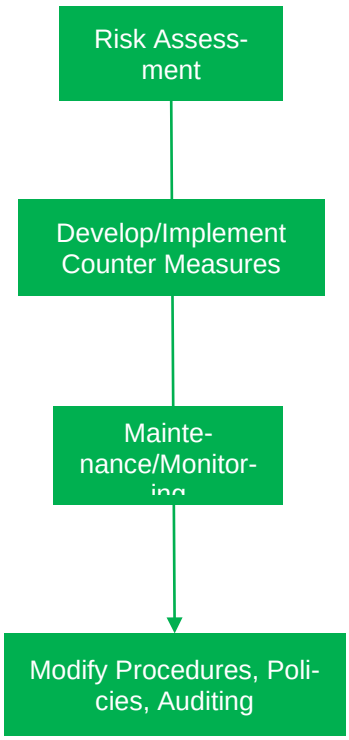
Introduction

Industrial Automation and Control System (IACS) asset owners 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 taking action. In this whitepaper, we will provide a guide to the initial steps that should be taken prior to the deployment of counter measures.

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. ISA/IEC 62443 is written to be applicable across industrial segments and it has been accepted by many countries. The 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



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.

Develop and Implementation Phase – Input from the Assessment Phase is 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.

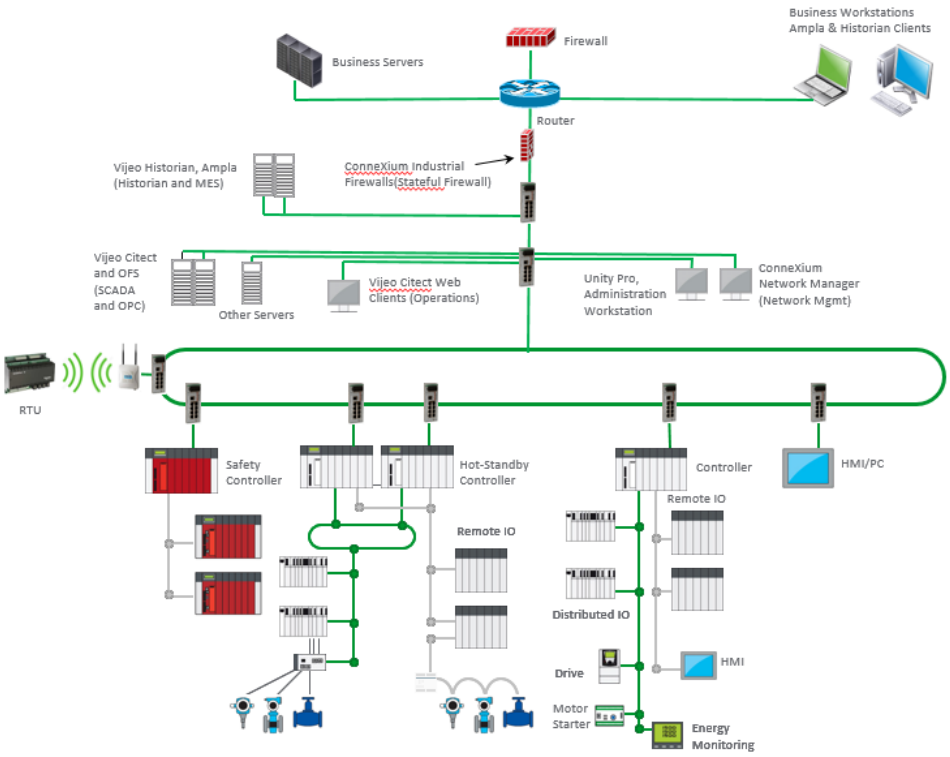
In this white paper, we will focus on the Assessment Phase, as it is the most critical step in the success of the overall process. You may find that you have not addressed key vulnerabilities if you implement countermeasures prior to analyzing your system. The assessment phase consists of a variety of steps, including Documenting the System, Vulnerability Assessment, Creating Zones and Conduits, and creating a Cyber Risk Assessment. Each will be discussed, starting with documenting the system. In this section, concepts will be introduced that are necessary for understanding recommendations presented later in the paper.

Documenting the System

The Assessment Phase begins with the creation of a risk assessment team. The team consists of existing employees who have been tasked to participate in the process. Senior management must support the effort and allocate resources to staff the project. Team membership may change over the course of the Assessment Phase. Initially, the team should consist of a project leader who will spend a majority of their time managing the project. In addition, individuals with knowledge of corporate IT/OT environments and physical security will be needed for the initial phase. The team's first assignment involves defining the scope of the system under assessment. Is the system in question confined to a specific facility, or does it cover multiple facilities? Are there project specific constraints – like regulations or corporate policies? The team should have a clear understanding of the system that will be analyzed, and how the system interfaces to other systems in the company. Once the scope of the system is clearly defined, the team can begin to map the system. Definition of the system scope will lead to the creation of detailed architecture diagrams, network diagrams, and asset inventories (hardware and software). Each deliverable is detailed below.

- Architecture Diagram – The system architecture diagram lists components of the system, defines how they are connected, and captures their physical locations. An example of a system architecture diagram is provided in Figure 2.

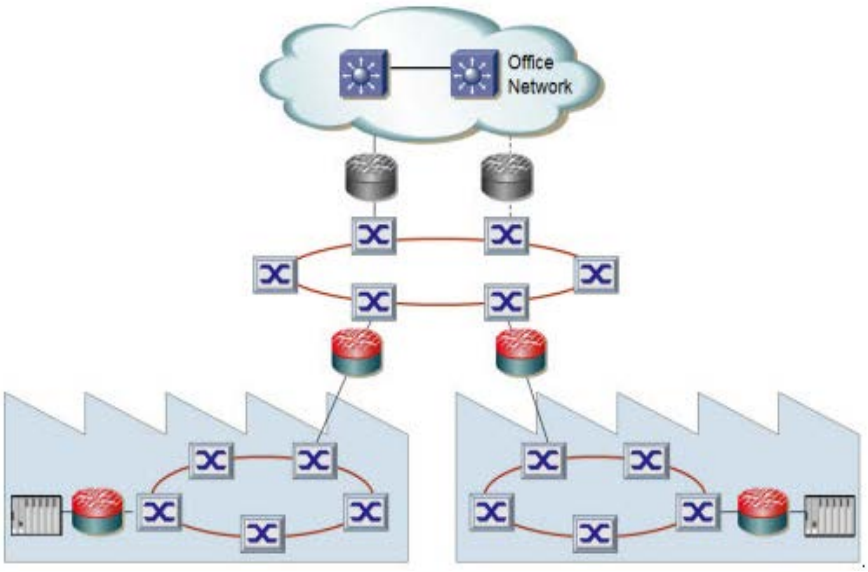
Figure 2: Sample Architecture Diagram



- Network Diagram – The network diagram is a logical representation of the network. It depicts routers, switches, and firewalls. It also identifies how equipment is connected to switch ports. The network diagram may or may

not show the hosts that are connected to the network. A sample network diagram is shown in Figure 3.

Figure 3: Sample Network Diagram



- Asset Inventory – IACS assets consist of hardware (computers, IACS equipment, network equipment), software, and virtual hardware platforms. The asset inventory should track a variety of attributes, including device name, asset ID, function, manufacturer, serial number, model, firmware version, responsible organization, operating system, and network address. Existing documentation, site survey, or automated tools can be used to gather asset information. During this phase, teams typically discover a variety of devices have been connected to the network that have not been documented.

The final important step in mapping the system involves documenting the cybersecurity features and security settings for each piece of equipment in the system. This information will be very important later in the process.

After conclusion of the system documentation step, the team will have a thorough understanding of equipment that comprises the target system, how elements are connected, and security features/settings. The resulting information is critical to the next step in the process, the vulnerability assessment.

Vulnerability Assessment

The vulnerability assessment enables a company to identify and document potential vulnerabilities. Vulnerability assessments can be conducted using 4 different techniques – Gap Assessment, Passive Assessment, Active Assessment, and Penetration Testing. Each technique will be discussed in detail. The membership of the assessment team may change during the vulnerability assessment phase.

- Gap assessment involves reviewing corporate practices utilizing industry accepted best practices, industry regulations, and applicable standards. The gap analysis uses employee interviews, site tours, and comprehensive corporate policy/procedure review. Gap assessments are typically based on accepted frameworks like NERC, NIST, or ISA 624443. It is important to note that assessments involve company processes and personnel in addition to technology. Gap assessments are typically the first step in an overall vulnerability assessment, and can be followed by passive or active assessments.

- Passive assessment involves discovering network devices using passive means, such as site surveys, network/architecture drawings, system logs, equipment configuration files, and network traffic analysis. The team can also review equipment data against vulnerability databases.

- Active assessment involves using tools to scan the network. Active assessment will discover devices on the network, device software/firmware versions, and potential vulnerabilities. Examples of tools used during active assessment include Nmap,
Shodan, and Nessus. It is important to note that active assessment places traffic on the IACS network which could introduce risk.

- Penetration testing is the follow-on step to the preceding steps. In penetration testing, attempts are made to exploit known and unknown security vulnerabilities discovered by the earlier steps using exploit tools and techniques. Penetration testing can be used to validate vulnerabilities, and test the effectiveness of countermeasures.

A vulnerability assessment report should be written after conclusion of activity. The report should document the scope of the system under assessment, a description of the system, and a summary of findings including details of specific vulnerabilities.

Creating Zones and Conduits

The next step involves segmenting the network into zones and conduits. Equipment grouping can be based on their location, function, and importance of the assets to process. Special attention should be given to the following:

- 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 control and enterprise equipment.

- Safety Systems – Safety systems typically have different security requirements than basic control systems and should be grouped into zones that are separate from non-safety assets.

- Wireless Devices – Wireless communications should be placed into zones that are separated from wired communications as they can be exposed to a wider variety of security issues.

- Device Connected to Insecure Networks – Remote access can be provided to employees, suppliers, and partners for maintenance or reporting. Remote access relies on connections through untrusted networks that lie outside of the physical network boundaries, and should be separated and protected.

- Zones and conduits are built on the defense in depth concept. 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 three steps. A summary is each step is provided below.

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

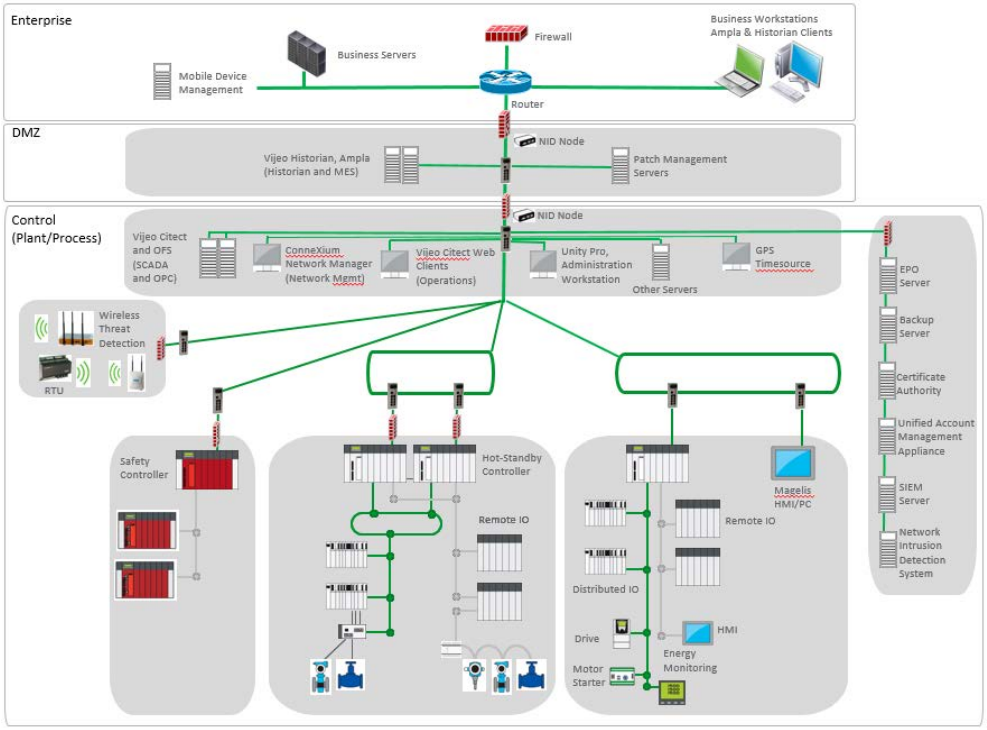
- Perimeter Protection – In this step, conduits between zones are properly protected.

- Network Segmentation – In this step, zones created previously 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 at a lower security level than a zone where safety equipment is located. The level of each segmented zone does not have to be the same as it neighbors.

A zone and conduit drawing is completed at the end of the exercise. Figure 4 illustrates a network that has been divided into zones. In this case, the overall network was divided into the DMZ, Control, and Enterprise zones. The perimeters of each was protected with a firewall. The control zone was segmented into 5 smaller zones (Factory Control, Wireless, Safety, Process Control 1, Process Control 2, and a security appliance zone). The perimeters of critical zones were protected.

Figure 4:
Sample Network Divided into Zones



Cyber Risk Assessment

The final part of the Assessment Phase is Risk Assessment. Risk assessment enables the organization prioritize activities to secure a system. Cybersecurity is an exercise in risk management. Organizations have limited resources, and can rarely afford to implement all counter measures to fully protect system. Thus, cybersecurity expenditures must be balanced based on potential impact.

During risk assessment, the team should be expanded to include control engineers, network engineering, cybersecurity experts, and equipment operators. It is important to note that not all risk has to be addressed – an operator can recommend choosing to live with the risk or designing the risk out of the process (remove element). Risk assessment is comprised of multiple steps:

- Criticality assessment – The team analyzes the relative importance of system assets and information. The criticality assessment measures the negative impact of the loss/corruption of components or data. This step illustrates the components/data in the system that should be protected.
- Identify threats – The team reviews potential threat sources (internal personnel, hacker, malware, etc.), and threat vectors (denial of service attack, identity spoofing, etc.) that each threat source could use to compromise a system.

- Identify vulnerabilities – The team identifies potential vulnerabilities. The work done as part of the vulnerability assessment is leveraged during this step.

- Determine impact and likelihood – The team now understands potential threats, and the vulnerabilities that the threats can leverage to compromise a system. Now the team must determine the consequences of an incident. Will the incident result in process shutdown, or the temporary loss of remote monitoring? The likelihood of compromise is also calculated. Risk is calculated using the formula: Risk = Impact x Likelihood. The formula is simple, but it takes significant effort and understanding to assign likelihood and impact to each potential vulnerability, and to combine findings to prioritize countermeasures. Results can be compared in a risk matrix as shown in Figure 5.

  The risk matrix can be used to prioritize which potential threats the company should prioritize to address. In Figure 5, threats with a risk greater than 11 are prioritized, and threats with risks less than 6 are tolerated.

Figure 5: Risk Matrix

Cybersecurity Risk Matrix		Impact Effect				
		1 *Insignificant*	2 *Minor*	3 *Moderate*	4 *Major*	5 *Catastrophic*
Occurrence Likelihood	5 *Expected*	5	10	15	20	25
	4 *Likely*	4	8	12	16	20
	3 *Reasonably Possible*	3	6	9	12	15
	2 *Unlikely*	2	4	6	8	10
	1 *Improbable*	1	2	3	4	5

- Select countermeasures – The team now has a list of targeted threats/vulnerabilities. Only now should the team begin to select countermeasures. At the beginning of the paper, we discussed how personnel could attend a webinar on threat management and leave wanting to purchase a threat management system. What if the threat management system did not address the prioritized vulnerabilities – that capital would have been wasted. This illustrates why a company should go through the Assessment Phase prior to implementing countermeasures.

  It is important to note that countermeasures do not always involve incorporation of new technology – corporate policies can also be impacted. Examples of corporate policies might include changing the organization to assign an individual responsibility for security, implementation of awareness training programs, or creation on policies detailing restrictions on items that can be connected to the network.

  It is also very important to ensure that the expenditure tied to the countermeasures does not exceed the value of the what is protected. For example, let's assume the team calculates that a specific threat could cost the company $250,000, and a compromise is likely to occur once every 5 years. Thus, the annual loss expectancy is $50,000. Let's assume that implementation of a countermeasure to address the threat costs $75,000 per year. In that case, the company may choose not to implement the counter measure as the counter measure cost exceeds the loss expectancy.

- The final step of the risk assessment involves reassessing risk after countermeasures have been incorporated. The team determines if the selected countermeasures have reduced risk to a tolerable level. If not, additional countermeasures may have to be implemented or the company may decide to tolerate the risk.

Process Documentation

After the conclusion of the Assessment Phase, customers are in a position to create a cybersecurity requirements specification document that will define the countermeasures that should be implemented by the organization. This is the first step of the Develop & Implementation Phase of the security lifecycle. Documentation is critical to capture information throughout the Assessment Phase. By the end 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

It is critical to document findings, and maintain the documents. These documents will be used later in the cybersecurity lifecycle

Help is Available

ISA offers IACS Lifecycle Cybersecurity training based on IEC62443. More specifically, ISA's Assessing the Cybersecurity of New or Existing IACS Systems (IC33) can be found at: https://www.isa.org/training-certifications/isa-training/instructor-led/course-descriptions/ic33/

Many asset owners 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 Assessment Phase, or any other phase in the security lifecycle. Please contact your Schneider Electric sales representative if you are interested in cybersecurity services.

Conclusions

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, following the steps detailed in this paper will enable operators to improve system security. Schneider Electric has experience in both ICS 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 policies and counter measures and improve them over time than to wait. But it is critical to analyze your system and understand which threats to address first.

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 998-2018xxxx_GMA-US