Core Principles of an ICS Cybersecurity Program

Krish Sridhar, P.E, GSEC, MBA

Business Manager – Industrial Cybersecurity

aeSolutions

krish.sridhar@aesolns.com

Abstract

The design and implementation of Industrial Control Systems (ICS) cybersecurity program poses significant challenges due to the stringent requirements of a manufacturing plant and how control systems and their networks are engineered, operated and maintained. While industry has made significant strides in gaining awareness and applying resources to address these requirements, many organizations have also come to realize that implementing cybersecurity measures in the ICS environment – also referred to as Operations Technology or OT, is challenging and quite different from implementing cybersecurity in the enterprise IT environment. Many of the concepts proven and accepted in enterprise IT are either too difficult and/or complex to execute or simply not relevant to the operating environment. Guidance provide by the NIST framework and other publications are helpful to getting started, and experience also dictates that there are a core set of cybersecurity elements for the ICS environment that must be done right. This paper highlights the uniqueness of the ICS environment and offers core principles for a successful development and launch of an ICS cybersecurity program.

Introduction

Organizations responsible for critical industrial operations are focusing on protecting their industrial control system (ICS) networks and assets against cybersecurity threats and potential attacks. Consider the situation at a large multinational company, gearing up to developing a cybersecurity program for their manufacturing plants. The installed base of various control system platforms at different versions of firmware and software including legacy systems poses a daunting task of inventorying and identifying assets that need to be protected. Add to this the complexity and cost of determining a strategy to harden and patch systems and keeping them up to date while ensuring uninterrupted plant operations. The cybersecurity team typically is challenged with several questions; How to prioritize the control measures to be applied and guarantee smooth operations? How much security is good enough? What are our competitors and peers in the industry doing? Are we on the right track and setting ourselves up for a scalable program? Then there is the typical arms-length relationship between operations and corporate IT to overcome for a chance that the cybersecurity program succeeds. From experience there have been numerous occasions where ICS cybersecurity programs start off with ambitious goals, but falter along the way and struggle to execute and sustain.

While industry has made significant strides in gaining awareness and applying resources to address these issues, many organizations have also come to realize that implementing cybersecurity measures in the ICS environment – also referred to as Operations Technology or OT, is challenging and quite different from implementing cybersecurity in the enterprise IT environment. Many of the concepts proven and accepted in enterprise IT are either too difficult and/or complex to execute or simply not relevant to the operating environment. In order to establish a successful program, a delicate balance is required between IT, operations, engineering and maintenance.

This paper highlights the uniqueness of the ICS environment and offers core principles for a successful development and launch of an ICS cybersecurity program.

Core Principles of an ICS Cybersecurity Program

The National Institute of Standards and Testing (NIST) Cybersecurity Framework published in 2014 identified 5 key functions of a holistic cybersecurity program - Identify, Protect, Detect, Respond and Recover. The NIST Framework is one of several guidance documents available for the user to help get started http://csrc.nist.gov/publications/PubsSPs.html). There are also publications from International Society of Automation or ISA (https://www.isa.org/standards-publications/), Center for the Protection of National Infrastructure or CPNI (https://www.cpni.gov.uk/scada/), Center for Internet Security (https://www.cisecurity.org/) and others.

While these documents can help with the details it is critical for the organization to identify and establish the core principles of its program. In our experience, the following basic principles form the foundation of any successful ICS cybersecurity program:

- Take a risk based approach to design the program
- Know what you are protecting
- Understand your baseline
- Segmentation, Segmentation, Segmentation!
- Design User Access management that is non-intrusive
- Ensure managed switches are "managed"
- Pay attention to remote access and all its use cases
- Develop ICS relevant policies and procedures
- Develop a phased approach to roll out the program
- Develop sustainability measures for the cybersecurity program

Take a risk based approach to design the program

ICS are the bread and butter of industrial organizations which rely on the control system to operate safely, efficiently and reliably. Therefore availability and reliability of control systems is paramount. Designing cybersecurity for the ICS environment must therefore balance availability, reliability and cybersecurity. Risk based analysis use a Consequence-Likelihood matrix to help identify risk tolerance for the organization. Each threat is associated with threat sources, vulnerabilities to be exploited, consequences and likelihood to determine the risk exposure. Following the industry proven process of Process Hazards Analysis (PHA), a “cyber PHA” format is recommended. Based on this approach, unmitigated risks are identified and scored. Then potential countermeasures are identified to further reduce the risk to tolerable levels. Such an approach provides a rational basis for deriving a set of prioritized recommendations, short-term/long-term mitigation strategies, and develop a cybersecurity road map for the organization to follow through and execute.

Know what you are protecting

Managing assets in terms of updated software and patches is critical to protect against known vulnerabilities. Enterprise asset management deploys popular asset management tools to automatically discover, alert and manage asset inventory. However ICS devices use proprietary firmware that often cannot be interrogated using common enterprise tools. Vendor specific tools must be used to manage these devices. Realistically, the cybersecurity program must provision for multiple tools and different personnel skill sets to manage ICS asset inventory. Personnel proficient with ICS tools may not be familiar with enterprise tools and vice versa. In order to consolidate data from different sources, popular enterprise asset management tools (Solarwinds, WhatsUP Gold) provide an API interface to customize and integrate external data sources. Such an approach would centralize the inventory management and tracking for the ICS environment.

Understanding your Baseline

The relatively static nature of ICSs, offers the defender a leg up in terms of protecting the systems. Unlike the enterprise end points, ICS assets are typically configured with static IP addresses. DHCP is non-existent in a typical ICS network. In addition the hosts that are responsible for running control system application software are actively managed to ensure that no new software or configuration changes are applied to these systems. This is primarily driven by the control system vendors who provide life cycle support for the systems. Therefore a strong case exists to develop a baseline of the configuration of end points and data flows between the various end points on the network. Such a baseline fingerprint helps identify misconfigured systems – for example a DCOM data flow path from an ICS console to the business network that should not be present. It also helps design anomaly detection systems for monitoring and analysis and to issue alerts based on predetermined rule sets for intrusion detection. The result is a holistic cybersecurity program based not only on the Identify and Protect functions of the NIST framework but also Detect, Respond and Recover.

Segmentation, Segmentation, Segmentation!

A popular reference for segmenting industrial networks is the Purdue Model for Control Hierarchy (https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327). A simplified version is presented in Figure 1. It states that devices on a network segment can only communicate to a segment directly below or above it. This is a simple yet powerful model to help design well segmented network architectures.

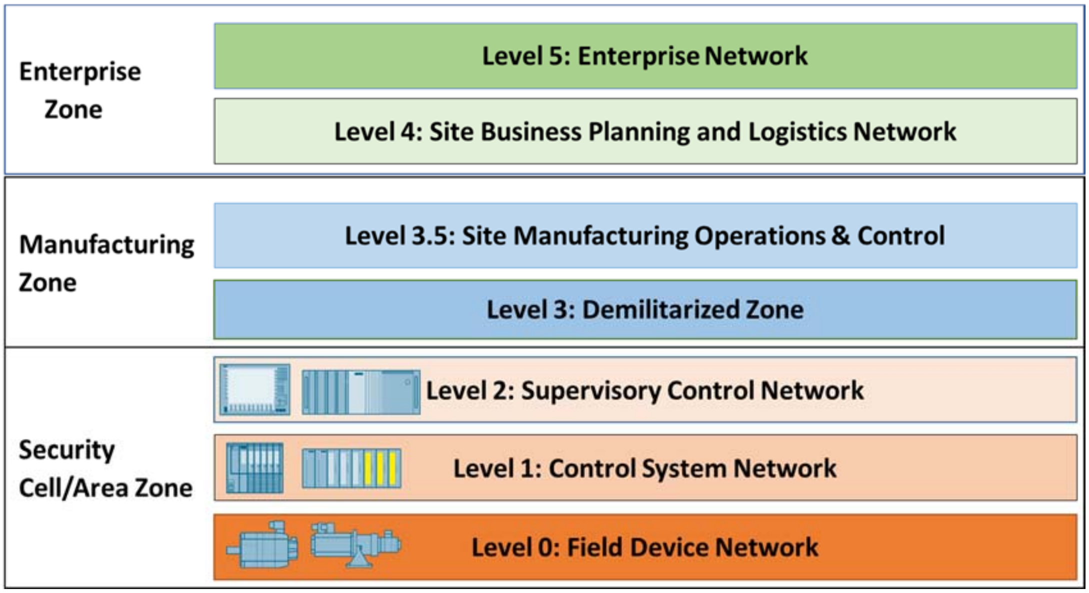
Enterprise Zone
Level 5: Enterprise Network
Level 4: Site Business Planning and Logistics Network
Manufacturing Zone
Level 3.5: Site Manufacturing Operations & Control
Level 3: Demilitarized Zone
Security Cell/Area Zone
Level 2: Supervisory Control Network
Level 1: Control System Network
Level 0: Field Device Network

Figure 1: Purdue Model for Control Hierarchy

ICS networks consist of assets with different functionalities such as a PLC for basic process control (BPCS), Safety Instrumented Systems (SIS) for safety critical functions, Gateway PLC for managing network protocol conversions, and so on. In a typical control system architecture there is very little if any segmentation between these control system assets (Level 1 in Figure 1). It is very common to see a BPCS PLC, a SIS PLC and Gateway PLC all on the same network segment. Very often plant – plant or area – area communications occur across one contiguous network segment (Level 2 in Figure 1).

It is best practice to segment networks with similar functionality/criticality into their own zones, commonly referred to as the zone and conduit model. For illustration purposes a conceptual zone and conduit model applied to a control system network is shown in Figure 2.

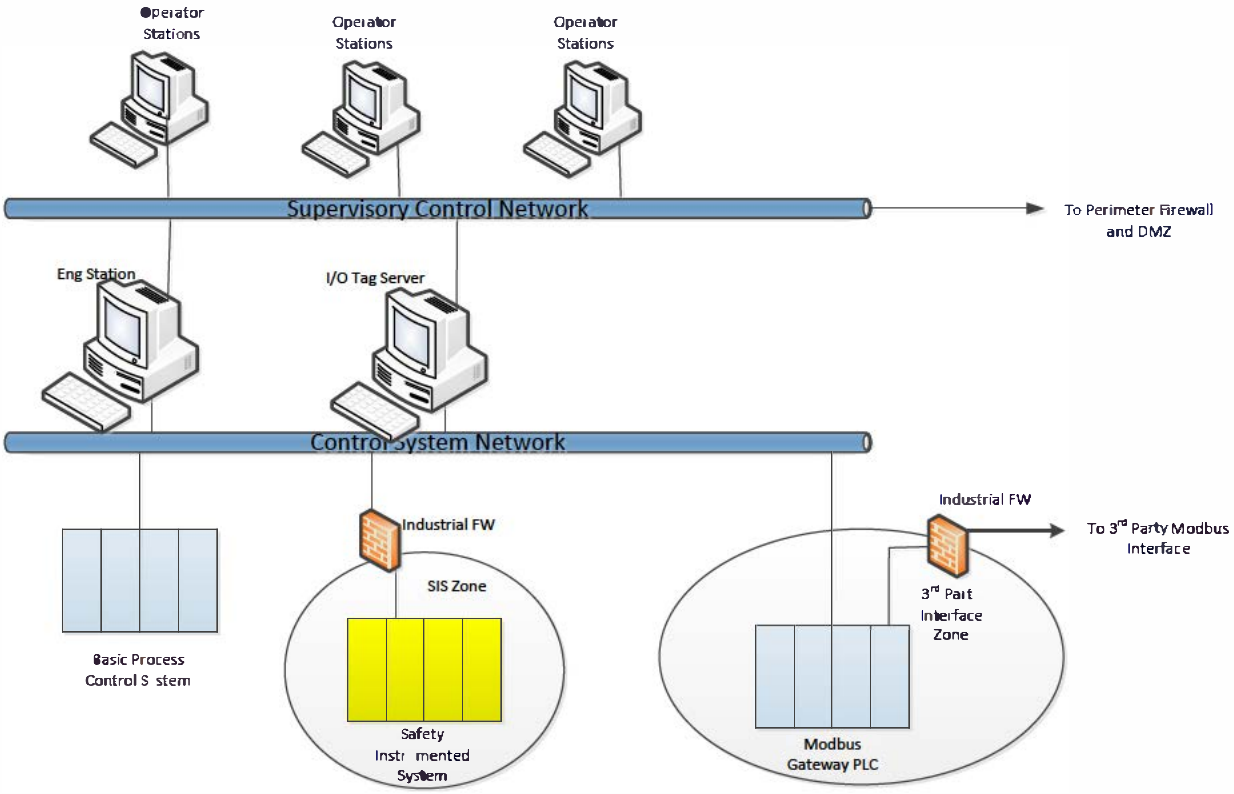

Figure 2: Example of zone based segmentation

All communications within the zone is trusted while any communication that enters or leaves the zone is monitored and filtered. A zone-based industrial firewall can be deployed here. These are appliances with deep packet inspection capabilities to examine the incoming and outgoing traffic and make rule based decisions on what data is allowed to flow across. Common zones in the ICS networks are basic process control (BPCS), safety instrumented systems (SIS) , gateway controllers, tank farm system, skid mounted systems, loading/unloading railcar systems, to name a few. This concept aligns with defense-in-depth strategy, by preventing un-fettered access to all the resources on a network if one or more access points within the network is compromised.

Design User Access management that is non-intrusive

User management within the ICS is very challenging to say the least. This is primarily due to the fact that operator consoles need to be logged in and available all the time for the operators to react and respond quickly to critical alarms and events. Individual user logins are not the norm due to a couple of reasons – multiple operators work in a shift on the same system/console and in some facilities individual user logins are not allowed by union law which prohibits companies monitoring operator actions (audit trail). Therefore it is common practice to deploy group logins. Within this construct, it is recommended to implement multiple groups such as one for Operators, Engineers, Maintenance, etc. There is also effort within some companies to enforce policies to lock the console screen when the operator is away. Limiting physical access to the control room through badged access keys or similar mechanism is recommended. Many control system platforms have built-in tracking of logged-in user actions at the application level. Make sure this feature is configured and monitored via reports. It is still necessary to track the group logins (e.g., via Active Directory) at the operating system level in order to track system level access. Combined with the application level tracking, this approach is valuable for incident response and forensic analysis.

Ensure managed Switches are "managed"

Managed switches within the process control network are seldom "managed" and are typically configured with vendor delivered default configuration settings. Vendor default user credentials (which are public information thanks to Google and other search engines), open port access with no access control, clear text protocols such as telnet enabled, Simple Network Management Protocol (snmp v1) based community strings are just the tip of the iceberg. Hardening these switches and managing them must be an integral part of the cybersecurity program. Configuring snmp traps to alert on user logins and connections to open switch ports are fairly easy to set up and configure. Such measures increase the resiliency of the overall system from unauthorized access to critical ICS assets.

Pay attention to remote access and all its use cases

Remote access to ICS networks has become all too common because it enhances productivity by allowing faster troubleshooting, remote maintenance and engage subject matter experts regardless of their location. However remote access interface increases the attack surface of the ICS networks by providing external entry points into the system. Organizations must design remote access solutions without violating the Purdue Model. This means all access must flow through the DMZ and perimeter devices. Several options are available and most common approach is to terminate external connections to a jump server in the DMZ e.g., VPN Server to manage access to the underlying ICS network. Paying attention to all the different users and their roles is essential in the design. The concept of least privilege must be at the core of the design philosophy. Limit access to engineering stations and safety systems from remote users. Another powerful technique that is employed to control remote access at plants that are manned 24x7 is to use ushered access as the last step in the authentication process. Monitoring and recording remote access sessions is also a powerful tool that can serve forensic analysis during incident response and handling.

Develop ICS relevant policies and procedures

Even though most organizations have IT related policies and procedures, they have come to realize that they are not actionable in their current form for the ICS environment. This is primarily due to the differences in the ICS networks mentioned earlier and how they are operated and maintained. Hence ICS specific policies and procedures must be developed. It is recommended to have personnel with expertise in IT security concepts as well as ICS engineering and operations experience lead the effort and have a document review process in place to elicit feedback from key stakeholders (e.g. IT, Operations, Engineering, etc.). The result is a collection of documents that are actionable and successful for plant/company-wide adoption.

Develop a phased approach to roll out the program

Implementation of the cybersecurity program should be performed in phases. This is because of the following reasons:

- Continuous operation plants cannot be interrupted unless there is a compelling reason
- Maintenance turnarounds are the perfect window of opportunity to implement cybersecurity control measures. These occur once or twice a year depending on the plant.
- Lessons learned from a phased approach will help improve the implementation process

Develop sustainability measures for the cybersecurity program

- Establish a set of KPIs to measure the progress of the cybersecurity program.
- Take a forward looking and practical approach to the program by factoring resource allocations necessary (in-house or out-sourced), political climate at different plants/regions, criticality of plants, and other considerations. Start with plants/regions that you believe are more supportive or less complex to implement. Remember, success breeds success.
- Provide guidance for plants to implement the cybersecurity program starting with basic, less complex measures and gradually transition towards a more advanced, mature state of the program.
- Establish a culture of compliance by incentivizing plants/regions to be at the forefront of the cybersecurity program. Plan internal communications and success stories.

Conclusions

ICS networks differ from enterprise networks in how they are engineered, operated and maintained. Recognizing these differences is at the core of a successful ICS cybersecurity program. Some of the core principles highlighted in this paper have shown from experience to be very important to get it right. Designing these elements with a practical approach will ensure that both IT and OT are able to collaborate and bring best in class expertise to sustain the lifecycle of the ICS cybersecurity program.