NAVIGATING INDUSTRIAL CYBERSECURITY

A Field Guide

Presented by

FORTRA

TABLE of CONTENTS

CHAPTER 1 • PAGE 4

KNOW YOUR TERRAIN

Industrial Control System Basics

CHAPTER 2 • PAGE 14

CLAWS, FANGS & VENOM

The Industrial Cyberthreat Landscape

CHAPTER 3 • PAGE 18

DON'T GO IN WITHOUT A MAP

The Value of Industrial Frameworks

CHAPTER 4 • PAGE 25

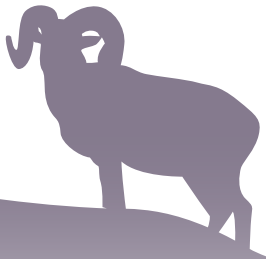
PERFECT YOUR SURVIVAL SKILLS

Best Practices for ICS Decision-Makers

CHAPTER 5 • PAGE 33

START THE EXPEDITION

Your ICS Cybersecurity Action Plan



NAVIGATING INDUSTRIAL CYBERSECURITY · A FIELD GUIDE ·

© Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners.

INTRODUCTION

Nearly every aspect of modern life depends upon the uninterrupted function of industrial control systems (ICS). ICSs keep the lights on, ensure clean drinking water, and provide other critical infrastructure processes. Beyond power, energy, and other utilities, ICSs are also responsible for the manufacturing of your computer, your car, and countless other physical items we rely on every day.

It's imperative that ICSs are protected against all cyber events—accidental or malicious—because the physical ramifications of such events pose major threats to both public safety and to any industrial entity's ability to stay operational and competitive.

But it's not realistic to apply cybersecurity best practices from the informational technology (IT) side of your organization to the operational technology (OT) side. IT and OT environments consist of completely different types of devices and network structures. OT environments also experience wildly different risks and threats than IT environments.

WHAT IS AN INDUSTRIAL CONTROL SYSTEM?

Industrial control system (ICS) is a generic term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control systems like programmable logic controllers (PLC). These control systems are found in discrete manufacturing, process automation, energy and transportation verticals, many of which operate critical infrastructure. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to operate and control a physical process (e.g., found in the automotive, manufacturing, petrochemical, oil & gas, food & beverage, pharmaceutical, water/wastewater, transportation, and power generation/transmission/distribution industries).

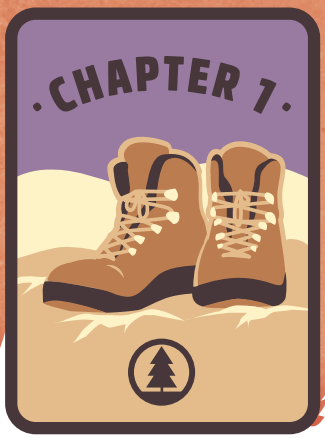
As ICS devices become increasingly Ethernet-connected, they also become increasingly vulnerable. By and large, industrial organizations are underprepared for the digital convergence of their IT and OT environments; the rate of new connected devices is outpacing the rate of device security.

Physical equipment that was once only mechanical is now entering the fast-growing world of the industrial internet of things (IIoT). Having smart machinery improves efficiency, but—without the proper precautions—it also offers cybercriminals remote access and attack opportunities they didn't have before.

These are just a few of the topics we'll explore, starting with ICS cybersecurity basics and eventually guiding you through step-by-step actions you can take to secure your ICSs against today's biggest emerging cyberthreats. This guide is simply a high-level primer, but it will give you a foundational lay of the land about the biggest issues in industrial cybersecurity.

"IT technologies will continue to permeate industrial control systems, thus opening OT assets up to threats that the IT side of the shop is familiar with. Organizations need to shift focus and put a bigger emphasis to protect the OT environment from these threats. Today's mindset at different levels of the organization is that 'IT is in charge of security.' The controls engineer or maintenance technician doesn't think that security is part of their role. But that's not necessarily the case. Training and education focused on industrial cybersecurity needs to improve within these organizations."

— Nick Shaw, Senior Systems Engineer



KNOW YOUR TERRAIN

Industrial Control System Basics

While OT and IT both need to protect their systems and data from compromise, OT cybersecurity professionals tend to approach their systems differently than traditional IT because they have varying priorities.

For example, ICS control engineers can be reticent to upgrade their equipment even when it would enhance their cybersecurity outlook. This is because their focus on maintaining constant uptime and measuring performance characteristics such as overall equipment effectiveness (OEE) rivals other priorities like making sure they are running the latest and greatest firmware. These three imperatives tend to dominate the OT cybersecurity conversation:

1. **Safety** *Cyberattacks or human errors in an ICS context can have real-world physical consequences. Whereas a customer data breach could cost a retail company millions in fines and damage their reputation, the physical safety of human beings isn't a central factor. In industrial environments, however, safety is paramount. This includes the safety of the workers on the plant floor as well as the customers served by the output of a particular ICS. This could look like shipping uncontaminated ingredients from a food processing plant or delivering a functioning car airbag within a vehicle built in an automotive assembly plant.*

2. **Quality** *In an industrial environment, consistency is everything. Regardless of your end product, any threat to its quality could be financially impactful. Cyber events that don't risk the physical safety of workers or customers can still take a toll on industrial organizations in the form of lost product due to quality inconsistencies in the forms of recalls or scrap. The ability to detect and correct anomalies affecting quality is crucial to ICS process integrity.*

3 **Uptime** *Cyber events can financially impact industrial organizations in a number of ways, from the theft of intellectual property to a denial of service (DoS) attack that renders parts of the control system unusable for a period of time. To put the significance of uptime in perspective, the manufacturing industry sees annual losses of $50 billion due to unplanned downtime*[1].

Many industrial devices are running older, highly-vulnerable versions of Windows that have not been hardened or patched. Operators often feel that they can't take these systems down for routine maintenance to improve security because they are critical for the overall operation of the plant or service.

There's also the concern that an upgrade/update might interrupt operations. In some cases, security vulnerability scans typical in IT environments are too disruptive to use in OT environments. In fact, many ICS environments may still have specialized industrial protocols and equipment that don't use TCP/IP (the most common communication protocol for IT networks and security tools).

Even when organizations can overcome these obstacles, cybersecurity is a relatively new discipline for operations teams running an ICS environment, and they may choose to delay acting on security issues because of real concerns about safety, quality and uptime. While such concerns are understandable, cyberattacks against critical infrastructure are escalating.

CRITICAL INFRASTRUCTURE

Not every ICS supports its nation's critical infrastructure, but many do. Critical infrastructure pretty much does what it says on the tin, meaning it keeps the world running by providing basic services like water treatment and electricity.

The U.S. Department of Homeland Security's National Infrastructure

CRITICAL INFRASTRUCTURE SECTORS

1. Chemical
2. Commercial facilities
3. Communications
4. Critical manufacturing
5. Dams
6. Defense industrial base
7. Emergency services
8. Energy
9. Financial services
10. Government facilities
11. Food & agriculture
12. Healthcare & public health
13. Information technology
14. Nuclear reactors, materials, & waste
15. Transportation systems
16. Water & wastewater systems

"In an increasingly interconnected world, where critical infrastructure crosses national borders and global supply chains, the potential impacts increase with these interdependencies and the ability of a diverse set of threats to exploit them."

— U.S. Department of Homeland Security

Protection Plan[3] breaks critical infrastructure into distinct sectors: "There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."

However, many ICS-based organizations aren't serving as the backbone of public safety—but they nonetheless need to be secured. Common verticals include automotive manufacturing, power generation, transmission and distribution, oil and gas, pharmaceutical manufacturing and water/wastewater.

THE IT/OT DIVIDE

Until recently, disparate network types like Ethernet and Fieldbus didn't mix. ICSs are now increasingly enmeshed with IT devices and business processes, multiplying the risk of compromise to their command and control functions.

The need for IT/OT convergence also raises several questions for business unit owners: namely, whose responsibility is ICS cybersecurity—the plant floor operator or the IT security operations center (SOC)?

The answer, of course, is that the responsibility is shared. But many organizations lack the internal organizational structures to delegate and enforce roles and responsibilities across both sides of the business.

Once you define roles and responsibilities within your overarching IT/OT cybersecurity program, you can run into several technical hurdles in bringing these two sides together as well. This is due to the fact that legacy ICS equipment, now increasingly Ethernet-connected thanks to the IIoT, wasn't made to handle data transmission in a secure manner. Here is the U.S. Department of Homeland Security's[2] breakdown of the differences between various security controls on the "shop floor" versus the "top floor."

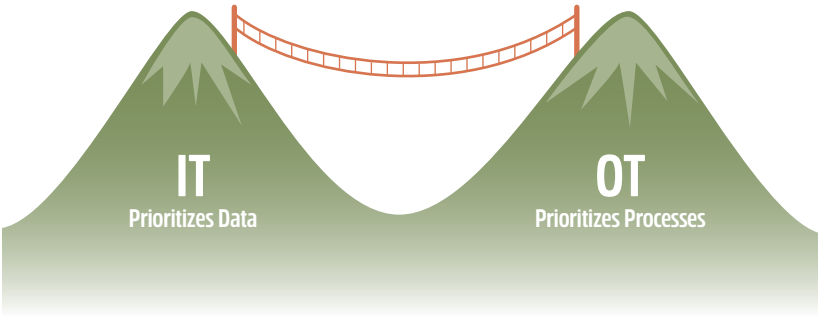
Differences in IT and OT Cybersecurity Challenges

Security Topic	Information Technology (IT)	Operational Technology (OT)
Antivirus and Mobile Code	Very common; easily deployed and updated. Users have control over customization and can be asset-based or enterprise-based	Memory requirements can impact ICSs; organizations can only protect legacy systems with after-market solutions; usually requires "exclusion" folders to avoid programs quarantining critical files
Patch Management	Easily defined; enterprise-wide; remote and automated	Long timeline to successful patch installation; OEM-specific; may "break" ICS functionality; asset owners required to define acceptable risk
Technology Support Lifetime	2–3 years; multiple vendors; ubiquitous upgrades	10–20 years; usually same vendor over time; product end-of-life creates new security concerns
Testing and Audit Methods	Use modern methods; systems usually resilient and robust to handle assessment methods	Tune testing to the system; modern methods can be inappropriate; equipment may be susceptible to failure during testing
Change Management	Regular and scheduled; aligned with minimum-use periods	Strategic scheduling; nontrivial process due to impact on production
Asset Classification	Common and performed annually; results drive expenditure	Only performed when obligated; accurate inventories uncommon for non-vital assets; disconnect between asset value and appropriate countermeasures
Incident Response and Forensics	Easily developed and deployed; some regulatory requirements; embedded in technology	Focused on system resumption activities; forensics procedures immature (beyond event re-creation); requires good IT/ICS relationships
Physical and Environmental Security	Can range from poor (office systems to excellent (critical IT operations systems)	Usually excellent for critical areas, maturity varies for site facilities based on criticality/culture
Secure Systems Development	Integral part of development process	Historically not an integral part of development process; vendors are maturing but at a slower rate than IT; core/flagship ICS solutions difficult to retrofit with security
Security Compliance	Definitive regulatory oversight depending on sector (and not all sectors)	Specific regulatory guidance depending on sector (and not all sectors)

"IT tends to eagerly embrace the latest technology, while OT tends to delay upgrades as long as possible to avoid interruptions. Sometimes it seems that they are even speaking a different language altogether. For example, tell a group verbally to make sure that the new network management software is compatible with "sip" and the professionals with the OT background will hear "Common Industrial Protocol" while the IT professionals will hear "Session Initiation Protocol"—with both equally certain that they are looking to spec the correct product!"

– Jeremy Friedmar, Industrial Business & Channel Development Manager

The IT/OT Gap



THE THREE CLASSES OF ICS

Industrial organizations have options when it comes to automation equipment. For instance, some systems must be distributed to be able to manipulate instruments that are physically distant from one another. Others are localized, with oversight of multiple subsystems for a large number of control points managed within close proximity. Most ICSs run on one of the following types of systems:

1. **Distributed control systems:** *Distributed control systems (DCS) manage and automate thousands of control points within a process. These are typically found in large localized facilities such as oil and gas refineries, chemical, pharmaceutical and power generation plants. DCSs are often made up of a number of different components, like controllers, I/O devices and servers.*

2 **Programmable logic controllers:** *A programmable logic controller (PLC) is a type of industrial computer that is the brains of the operation. It makes decisions through input received by sensors and then through logic programming, makes a decision of what to do, e.g., turn on a motor or release pressure. PLCs are found within any industrial automation process and can also be part of a larger system, such as a DCS.*

3 **Supervisory control and data acquisition:** *A supervisory control and data acquisition (SCADA) system centrally manages and monitors remote field devices that are often spread over thousands of square miles, and can control remote field devices to perform certain operations based upon specific alarm or notification conditions, such as opening a valve or closing a breaker. For geographically-dispersed control environments, like those of a natural gas pipeline or remote electrical substations, a SCADA system is used to control and manage these applications.*

> ***TIP:*** Regardless of what type of ICS you oversee, your cybersecurity best practices (like achieving and adhering to IEC 62443) are more or less constant. Ensuring the integrity of your industrial environment is largely a matter of asset discovery/inventory, management, and monitoring—those processes will just look different depending on the specific hardware and software within your ICS.

THE PURDUE MODEL

During the early days of IT/OT convergence, it was clear that a reference architecture needed to be created to articulate the specific roles and functions of the machines that control the physical processes as well as the other relevant ancillary devices and operations. In 1990, The Purdue Enterprise Reference Model was born to do just this. Today, it is simply referred to as the Purdue Model.

The Purdue Model has evolved over the years, but its purpose of classifying different domains of management for physical processes remains the same. Over its evolution, the Purdue Model has become the gold standard for network segmentation (this refers to segmenting networks supporting the different levels of the model through the use of firewalls, where all traffic is denied traversing the Purdue Model levels unless it's explicitly permitted).

As more and more connectivity was occurring between the shop floor and business IT networks, the Purdue Model evolved to outline a new line of demarcation between industrial control networks and enterprise networks through the use of a demilitarized zone (DMZ). Today, the Purdue Model consists of seven levels, including the DMZ at Level 3.5.

Levels of the Purdue Model

» *LEVEL 0* I/O Field devices

» *LEVEL 1* Control: PLCs and RTUs

» *LEVEL 2* Process: HMIs, operator stations and supervisory control

» *LEVEL 3* Operations: Historians, network services and advanced control

» *LEVEL 3.5* DMZ

» *LEVEL 4* Business network

» *LEVEL 5* Enterprise IT

Industrial-specific equipment and devices are found as you get closer to the physical process at Level 0. As such, Level 0 and Level 1 are where devices such as sensors, actuators, drives, PLCs and DCSs reside. As you get further from Level 0 and Level 1, more standardized, traditional IT systems (such as engineering workstations, human-machine interfaces (HMIs), data historians, and SCADA) will be found—all of which are running on common operating systems, such as Linux and Microsoft Windows.

As automation systems continue to evolve, the different levels of the Purdue Model will still be needed, but they will probably not look as physically identifiable as they are today. The future of automation systems will be on the same trajectory as IT systems that will eventually be abstracted from physical qualities through the use of virtualization, service-driven networking, application containers and cloud environments.

As cybersecurity solutions were first created, they set out to address one—if not the greatest—challenge for industrial cybersecurity: the inability to secure something that is unknown or invisible. These solutions did not gain much credibility until they were able to identify devices that operate at Level 0 and 1 of the Purdue Model, as devices at these levels communicate not with traditional IT protocols, but with industrial protocols such as Ethernet/IP, Modbus and Profinet.

WHY SOME ICSs ARE STUCK IN THE PAST

Cybersecurity was not even close to being on the radar when modern-day ICSs were initially developed over 30 years ago. In addition to IT/OT convergence, there are a few other challenges industrial organizations face if they want to enact the cybersecurity programs they'll need in order to stay protected from errors and attacks.

The shift to new network technologies improves data collection, new levels of automation, operational efficiencies and time-to-market, but it also produces new cybersecurity risks due to factors:

- **Unintegrated technologies:** *Many ICSs are purpose-built and proprietary, and were created when cybersecurity impacts were not a concern.*
- **Flat networks:** *Many ICS networks are flat, meaning each device has access to the rest. In a flat, non-segmented network architecture, a malware attack against one device gives the malware free reign to propagate through the control environment with impunity.*
- **Workforce challenges:** *Through the combination of an aging workforce and more and more IT technologies being adopted within ICS at a faster rate than ever, a skills gap for securing ICS has emerged. With an estimated 3.5 million unfilled cybersecurity jobs by 2021[4], the skills gap is another challenge to overcome.*

> ***TIP:*** To bridge the IT/OT divide, a recommendation for industrial organizations would be to create an ADX role (ADX stands for automation and data exchange). The primary function of this role is to interface with both IT and OT control engineers to ensure the operational process functions and the data about the process is exchanged with IT to drive business decisions.

"In the next 5–10 years, industrial systems are going to become increasingly connected to the internet as the IoT becomes more and more essential to industrial operations, and as those systems are also hooked into 5G cellular networks—which are promising much lower communication delays between devices. IoT device security is usually terribly weak right out of the box, so this will be a serious challenge for industrial systems to manage when IoT devices are deployed at scale."

— Justin Sherman, Cybersecurity Policy Fellow, New America

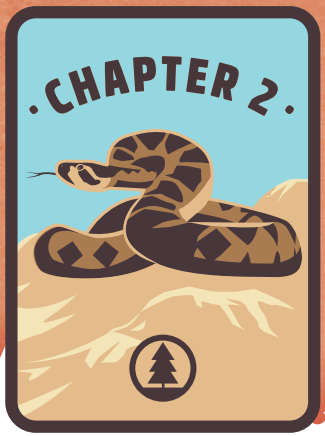
KEY TERMS & DEFINITIONS

Let's go over some of the language commonly used in the industrial cybersecurity field that you'll want a basic understanding of as you continue reading.

Physical Systems	
ICS (industrial control system)	A term that encompasses several types of control systems, and consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy), ICSs are critical to the operation of critical infrastructures that are often highly interconnected and mutually dependent systems
SCADA (supervisory control and data acquisition)	The control system used in distribution systems to centrally manage and monitor remote field devices that are often geographically dispersed. They collect field data and transfer it to be displayed at a central facility
Fieldbus	Fieldbus is a means of communicating with input and output devices without the need to connect each individual device back to a controller
DCS (distributed control system)	DCSs manage and automate thousands of control points within a process, often made up of a number of different components like controllers, I/O devices and servers
PLC (programmable logic controller)	The PLC is a type of industrial computer that is the brains of the operation, making decisions through input received by sensors and then through logic programming, making a decision of what to do, e.g. turn on a motor, release pressure, etc.
HMI (human-machine interface)	Hardware or software, ranging from physical control panels to an industrial PC running dedicated software, that allows human operators to monitor the state of a process under control, modify control settings, change the control objective, and manually override automatic control operations
Industrial Cybersecurity Terms	
Critical infrastructure	Physical and cyber systems and assets that are vital to the nation—any interruption or destruction would have a debilitating impact on a nation's economic security or public health and safety
Critical asset	A specific entity of such importance that its incapacitation or destruction would have a serious effect on the ability of a nation to continue to function effectively
IIoT (industrial internet of things)	A term for all of the various sets of hardware pieces that work together through connectivity to help enhance manufacturing and industrial processes

Some definitions provided by *NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security.*

Zone	A collection of entities that represents partitioning of a system under consideration on the basis of their functional, logical and physical (including location) relationship
Conduit	A logical grouping of communication channels, connecting two or more zones that share common security requirements
Cyber incident	A security event that compromises the integrity, confidentiality or availability of an information asset
Breach	An incident that results in the confirmed disclosure— not just potential exposure—of data to an unauthorized party
Defense in Depth	A multiple-layer technique that involves two or more overlapping security mechanisms to minimize the impact of a failure in any one mechanism, often including firewalls, demilitarized zones, training programs, incident response mechanisms and physical security
Phishing	The strategy of tricking individuals into disclosing sensitive personal information by claiming to be a trustworthy entity in an electronic communication
Social engineering	Psychological manipulation of people to reveal information (like a password) or perform actions (like sending money)—these tactics can be used to attack systems or networks
Malware	Software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity or availability of an information system
Zero-day attack	A breach leveraging a previously-unknown security vulnerability when either the patch has not been released or the application developers were unaware
SCM (security configuration management)	The management and control of configurations for an information system with the goal of enabling security and managing risk
FIM (file integrity monitoring)	Also known as change monitoring, FIM is the process of examining files to see if and when they change, how they change, who changed them, and what can be done to restore them when modifications are unauthorized
VM (vulnerability management)	The process of scanning networks for known vulnerabilities or CVEs (common vulnerabilities and exposures), then prioritizing and remediating those vulnerabilities in order based on risk severity
ICS Security Roles	
CISO (chief information security officer)	An executive who is typically responsible for directing strategy and establishing and maintaining protection programs for an organization to secure information assets and technologies
ADX (automation and data exchange) engineer	The emerging role title used for cybersecurity professionals whose primary concern is bridging the IT/OT gap



CLAWS, FANGS & VENOM

The Industrial Cyberthreat Landscape

Industrial operators have to be knowledgeable about common adversarial tactics like phishing and malware, but they also need to understand emerging tactics designed specifically to compromise ICSs. Even though many ICSs use proprietary devices and software, custom-built malware designed to penetrate ICS environments—like Stuxnet—is becoming more common.

Verizon's *2019 Data Breach Investigations Report*[5] found that "(m)anufacturing has been experiencing an increase in financially motivated breaches in the past couple of years, but espionage is still a strong motivator. Most breaches involve phishing and the use of stolen credentials." Of the 352 incidents and 87 confirmed data breaches cited in the report, Financial (68 percent) and Espionage (27 percent) were the two primary actor motives.

So how exactly are threat actors managing to make their way into vulnerable ICSs? That depends on how mature your cybersecurity program is. For example, if an industrial organization doesn't have basic change monitoring as part of its cybersecurity program, attackers have much more low-hanging fruit to pursue. Attackers can linger within the industrial network undetected, exfiltrating data and gaining access to privileged accounts. On the other hand, a similar organization with a highly-mature program that monitors their devices and networks raises the stakes for adversaries, where the initial access and reconnaissance activities will be detected before damage can be done.

"If your business has an industrial control system footprint, now is the time to evaluate how you're securing that environment. Industrial companies have accepted the reality that digital threats can have tangible consequences. This perception is perhaps heightened by recent attacks that were specifically designed to affect physical operations and have proven capable of doing so."

– Tim Erlin, VP of Strategy

INTENTIONAL vs ACCIDENTAL & INSIDER vs OUTSIDER THREATS

If you read a headline about a critical infrastructure cyberattack, a coordinated nation-state attack might be what first comes to mind. While intentional outsider threats do pose serious risks to public safety, not all cyberattacks carried out within an ICS are the stuff of action movies.

According to the *2019 DBIR*, 30 percent of cybersecurity incidents were the result of internal threats. Internal threats can come from insiders being paid to engage in espionage, or disgruntled employees aiming to inflict financial losses or operational damage. And in many cases, cyber events are the result of simple human error. Accidental insider threats can look like an employee configuring the incorrect switch resulting in downtime, or even leaking confidential information by way of a password absentmindedly left in the open.

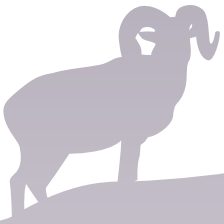
COMMON TYPES OF ICS CYBER EVENTS

1. Destruction of data
2. Manipulation of data
3. Theft of data
4. Denial of service
5. Masquerading of identity
6. Escalation of privilege
7. Human error
8. Equipment failure

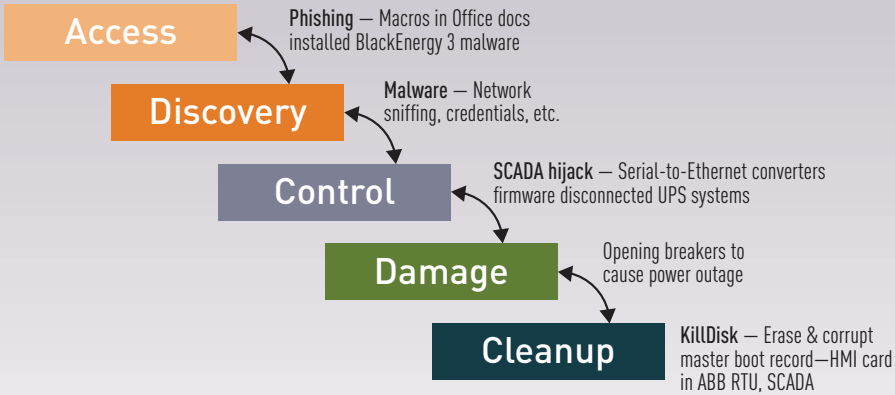
WHAT A REAL-WORLD ICS BREACH LOOKS LIKE

In December 2015, more than 230,000 Ukrainians in three different regions suddenly found themselves without electricity on a cold winter evening. A single, coordinated attack had taken down 30 public power substations.

The attack may have seemed sudden to the utility company, but it was the result of careful plotting over the course of six months on the part of the cybercriminals. They used a combination of phishing, keylogging, VPN hijacking, denial of service, firmware modification and more.



Anatomy of Ukraine Power Grid Attack



Major Industrial Cybersecurity Events

Year	Entity Breached	Tactic	Outcome
2010	Iranian nuclear plant	The Stuxnet worm initially infiltrated the plant via a USB stick, which then targeted control software used to program the operation of the uranium centrifuges.	Stuxnet successfully impeded the operation of Iran's nuclear program by introducing failures to approximately 20% of their uranium enrichment centrifuges.
2011	Energy sector operations in the U.S., Switzerland and Turkey	The group DragonFly was established in 2011 but became increasingly active in 2017, using remote access tool (RAT) malware by way of spear phishing, trojanized software and watering hole attacks.	Dragonfly gained unauthorized remote access that allowed them to exfiltrate sensitive information, such as passwords, from ICS systems.
2013	Multiple ICS targets in energy and pharmaceuticals	The group Energetic Bear used watering hole and phishing attacks for espionage and reconnaissance.	Energetic Bear compromised PLCs by backdooring them with Havex malware.
2015	Ukraine's electrical grid	Industroyer is a type of malware that was used to control electricity substations and circuit breakers.	Industroyer attacks have succeeded in stopping power service, a blackout that impacted more than 230,000 people.
2017	Saudi-Arabian petrochemical plant	Adversaries used TRITON malware to bypass physical safety systems. They moved laterally through the network for over a year, renaming files and mimicking regular processes until they accessed the ICS' safety instrumented system (SIS).	The attackers' mission appears to have been an explosion in the plant, but ultimately they were only able to wipe a number of company hard drives.
2018	Over 200,000 entities in energy, manufacturing, oil & gas, petrochemical and others in over 150 nations	Attackers used WannaCry in a ransomware attack to exploit a Windows vulnerability and encrypt data.	An attack with significant global impact, WannaCry resulted in some major automakers temporarily halting plant operations.

DON'T GO IN WITHOUT A MAP

The Value of Industrial Frameworks

Verticals such as healthcare, financial services and retail are tightly regulated by cybersecurity frameworks like HIPAA, PCI and SOX to help them secure their environments. Mandatory frameworks are enforced by rigorous audits, and organizations can face crippling fines for non-compliance. By and large, the industrial sector is yet to acquire this same level of regulation—though some verticals publish frameworks for guidance, not regulatory compliance.

WHY YOU SHOULD USE A FRAMEWORK

Why would you choose a framework if you're not legally mandated to? The reason is simple: Leveraging a non-mandatory framework is one of the best ways to start a cybersecurity program, build a defensible network and ensure your industrial process stays operational. These frameworks give organizations a clear-cut, step-by-step path for mitigating risk and keeping their names out of breach headlines.

It's also appropriate to think of aligning with a framework as an investment in your organization's future stability and profitability. The rise of the IIoT is only projected to drive increased connectivity, bringing increased cyber risk along with it. When you apply the basic foundational cybersecurity controls provided by compliance frameworks, you're future-proofing your ICS.

Frameworks like IEC 62443, NIST SP 800-82 and NERC CIP are a few that give industrial organizations actionable methodologies for safeguarding their industrial processes through leveraging a wealth of industry knowledge to take the guesswork out of their cybersecurity programs.

TIP: When something goes wrong, how quickly can you detect and correct the issue? Maintaining the integrity of your process is a byproduct of a good cybersecurity program. Cybersecurity monitoring solutions give you visibility into cyber events that threaten process integrity—like having a video recorder where you can rewind the video to see what caused the problem. The goal for cybersecurity monitoring is to keep the process stable, where the variation of the output from the process is within acceptable bounds. Cybersecurity monitoring solutions give you the ability to rewind so that you can quickly detect and correct.

IEC 62443

IEC 62443, originally known as ISA-99, was created by the International Society for Automation (ISA) and adopted by the International Electrotechnical Commission (IEC). It is a cybersecurity framework for industrial organizations to provide guidance on implementing security solutions.

IEC 62443 was created to ensure flexible methods for secure processes with an emphasis on the safety of personnel and production, availability, efficiency and quality. As a consensus-based standard, it's a leading framework in industrial verticals such as discrete manufacturing, oil and gas, electricity and water/wastewater.

One major concept introduced by IEC 62443 is the zone and conduit structure which can be used to segment the different levels of the Purdue Model—also a key component for the Defense in Depth methodology, covered in Chapter 4.

"The ISA/IEC 62443 series of standards, developed by the ISA99 committee and adopted by the International Electrotechnical Commission (IEC), provides a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs). The committee draws on the input and knowledge of IACS security experts from across the globe to develop consensus standards that are applicable to all industry sectors and critical infrastructure."

– International Society for Automation

CIS CONTROLS

Many of the cybersecurity industry's most trusted organizations recommend the Center for Internet Security's CIS Controls for securing enterprise systems. As the CIS states, the 18 controls are a *"prescriptive, prioritized, highly focused set of actions that have a community support network to make them implementable, usable, scalable, and in alignment with all industry or government security requirements."*

The CIS Controls

1. Inventory and Control of Enterprise Assets
2. Inventory and Control of Software Assets
3. Data Protection
4. Secure Configuration of Enterprise Assets and Software
5. Account Management
6. Access Control Management
7. Continuous Vulnerability Management
8. Audit Log Management
9. Email and Web Browser Protections
10. Malware Defenses
11. Data Recovery
12. Network Infrastructure Management
13. Network Monitoring and Defense
14. Security Awareness and Skills Training
15. Service Provider Management
16. Application Software Security
17. Incident Response Management
18. Penetration Testing

"Many organizations facing the current cybersecurity environment are overwhelmed by what we call the "Fog of More"—a constant stream of new information and problems. ... The CIS Controls are designed to bring priority and focus to this daunting task, to harness the power of a large expert community to identify and support high-value practices and foundational steps, and to stop "admiring the problem."

– Center for Internet Security

CIS CONTROLS ICS COMPANION GUIDE

In addition to their popular Controls, the CIS has published the *CIS Controls Implementation Guide for Industrial Control Systems,* a companion document intended specifically for industrial organizations. This publication provides detailed guidance around each of the Controls, geared specifically toward the unique needs of ICS environments.

"The security challenges facing Industrial Controls Systems (ICS) are one such example where additional attention is required. While many of the core security concerns of enterprise IT systems are shared by ICS operators, the main challenge in applying best practices to ICS is tied to the fact that these systems typically operate software and hardware that directly control physical equipment or processes."

– CIS Controls Implementation Guide for Industrial Control Systems

MITRE ATT&CK FOR ICS

Whereas CIS offers a prioritized list of actions you can take to harden your systems against cyberattacks, MITRE approaches its frameworks from the point of view of the attackers themselves.

MITRE is a not-for-profit organization operating federally-funded research and development centers, including cybersecurity research to help strengthen national defenses. They've so far developed two ATT&CK (adversarial tactics, techniques, and common knowledge) frameworks listing widespread cyberattack methods from real-world scenarios—one to address enterprise IT environments, the other, ICS.

Their aim is to help you see how adversaries compromise and exploit cyber infrastructure so that you can create effective cyber defenses. By leveraging the ATT&CK for ICS framework, you can begin simulating how an attacker may target your ICS and implement the appropriate cybersecurity controls to prevent or minimize the potential impact.

> *"Logic executing in ICS has a direct effect on the physical world. The consequences associated with this logic executing in an improper way include significant risk to the health and safety of human lives and serious damage to the environment, as well as serious financial consequences such as production losses, negative impact to a nation's economy, and compromise of proprietary information. ATT&CK for ICS seeks to characterize and describe the actions of an adversary who seeks to cause such consequences."*
>
> **– MITRE**

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

The National Institute of Standards and Technology (NIST), publishes a framework called the *Framework for Improving Critical Infrastructure Cybersecurity*. This framework is invaluable to critical infrastructure organizations that wouldn't otherwise have a clear set of best practices to follow within the particular challenges of their OT environments.

While the NIST framework is managed by the federal government, it wasn't made with only federal agencies in mind. *NIST Special Publication (SP) 800-82* is of particular importance to industrial organizations. It gives clear instructions on how to secure SCADA systems, DCSs, and PLCs. It outlines concrete steps for restricting unauthorized access to your ICS, protecting individual components from exploitation, and maintaining functionality during adverse conditions.

"Cybersecurity is critical for national and economic security. The voluntary NIST Cybersecurity Framework should be every company's first line of defense. Adopting version 1.1 is a must-do for all CEOs."

– U.S. Secretary of Commerce Wilbur Ross

AMERICAN WATER WORKS ASSOCIATION

The American Water Works Association published the *Process Control System Security Guidance for the Water Sector* in 2013 as this vertical was in need of a framework to provide step-by-step guidance to secure process control networks from cyberattacks. The creation of this guidance also helped address the U.S. Presidential Executive Order 13636—*Improving Critical Infrastructure*, which was also issued in 2013. This executive order directed NIST to lead the development of a framework to reduce cyber risks to critical infrastructure.

"The goal of the AWWA guidance is to provide water sector utility owners/operators with a consistent and repeatable recommended course of action to reduce vulnerabilities to cyberattacks as recommended in ANSI/AWWA G430: Security Practices for Operations and Management and EO 13636. The project is also expected to communicate a "call to action" for utility executives acknowledging the significance of securing PCS."

– American Water Works Association

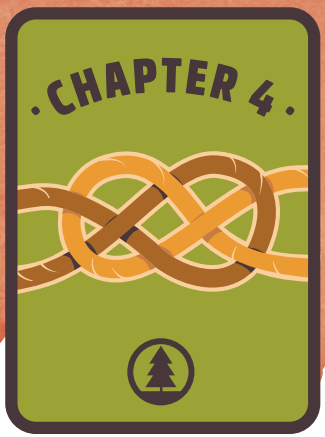
NERC CIP

The North American Electric Reliability Corporation (NERC) is an international regulatory organization that works to reduce risks to power grid infrastructure. They do this through the continual development of a set of regulatory standards in addition to education, training and certifications for industry personnel.

Unlike the other compliance frameworks listed here, cybersecurity professionals who work within the electrical grid and other critical infrastructure supply industries are mandated to comply with NERC CIP (critical infrastructure protection) requirements. NERC CIP is enforced by audit, so energy organizations are required to spend substantial time, resources and budget making sure that their systems are in compliance.

> *"The vision for the Electric Reliability Organization Enterprise, which is comprised of NERC and the six Regional Entities, is a highly reliable and secure North American bulk power system. Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid."*
>
> **— NERC**

Want to learn more about NERC CIP compliance? Download the white paper ***Achieving Resilience While Fulfilling NERC CIP Requirements*** from **tripwire.me/NERCwp**



PERFECTING YOUR SURVIVAL SKILLS

Best Practices for ICS Decision-Makers

Once you understand the industrial cyber threat landscape and the frameworks you can use to secure your ICS against cyber events and breaches, you're ready to take action using proven methods leveraging a Defense in Depth strategy with foundational controls.

DEFENSE IN DEPTH

Defense in Depth is a concept borrowed from medieval European castles, where multiple levels of defense were used to defend the castle from adversaries. Such layers included the moat, bridges, gates, inner and outer walls armed with cannons and soldiers, and tower keeps.

The same strategy can be used to secure your networks. It's a layered strategy to defend networks where multiple levels would need to be breached before a cyberattack could reach its full damage potential. This strategy makes it more difficult to achieve the desired end goal, and also adds the capability of detecting and preventing the spread of an attack based upon the layered defense approach. Built-in redundancies are put in place in order detect and then stop intruders from laterally moving from one part of your ICS to another or lingering on your network undetected.

What does Defense in Depth look like in an ICS context? Imagine this: Your cloud network feeds through edge network firewalls, which lead to your plants, substations or field facilities. Your plants and field facilities then connect to another deep packet inspection device firewall, which leads to your final PLCs. That's one example of network segmentation, a concept we'll continue to explore in this chapter, achieved through Defense in Depth; the attacker would need to overcome several layers of security controls in order to carry out their goals.

Elements of a Defense in Depth Strategy[6]

Risk Management Program	» Identify threats » Characterize risk » Maintain asset inventory
Cybersecurity Architecture	» Standards/Recommendations » Policy » Procedures
Physical Security	» Field electronics locked down » Control center access controls » Remote site video, access controls, barriers
ICS Network Architecture	» Common architectural zone » Demilitarized zones (DMZ) » Virtual LANs
ICS Network Perimeter Security	» Firewall/One-way diodes » Remote access and authentication » Jump servers/Hosts
Host Security	» Patch and vulnerability management » Field devices » Virtual machines
Security Monitoring	» Intrusion detection services » Security audit logging » Security incident and event monitoring
Vendor Management	» Supply chain management » Managed services/Outsourcing » Leveraging Cloud services
The Human Element	» Policies » Procedures » Training and awareness

"Defense in Depth as a concept originated in military strategy to provide barriers to impede the progress of intruders from attaining their goals while monitoring their progress and developing and implementing responses to the incident in order to repel them. In the cybersecurity paradigm, defense in depth correlates to detective and protective measures designed to impede the progress of a cyber intruder while enabling an organization to detect and respond to the intrusion with the goal of reducing and mitigating the consequences of a breach."

– U.S. Department of Homeland Security

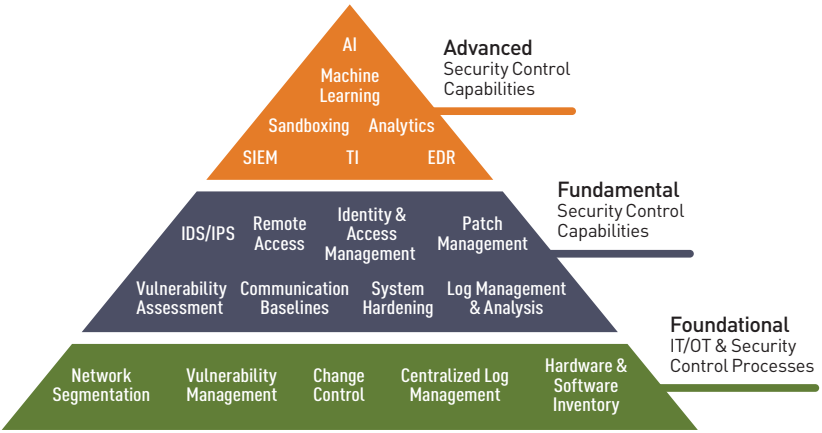
FOUNDATIONAL CONTROLS: THE BEST FRIEND OF ICS

In Chapter 3, you may have noticed a common theme among the industry-recognized frameworks provided by organizations such as IEC, NIST and CIS. Following these frameworks takes the guesswork out of what can be referred to as "foundational controls."

WHAT ARE FOUNDATIONAL CONTROLS?

Foundational controls are the basic cybersecurity practices—such as network segmentation, vulnerability management, configuration management, and change control—that serve as the core of a successful cybersecurity program.

After you have the basic controls firmly in place, you can move on to the more advanced security ones. To eliminate the most risk and get the biggest bang for your security buck, you first need to make sure foundational controls are implemented and the supporting processes around them are being followed.



The Pyramid of Foundational Controls

THE FIVE FOUNDATIONAL CONTROLS YOU NEED TO KNOW

These foundational controls are the ICS cybersecurity best practices on which you should build your industrial cybersecurity program. These controls are called out by all the industrial cybersecurity frameworks listed above.

1 Hardware & Software Inventory

It goes without saying, but one of the most basic steps to securing any environment is knowing what's in it. How can you secure something unknown? If you don't already have one, an accurate asset inventory, including both hardware and software, should be your first objective. Maintaining this inventory over time is critical for your cybersecurity program. The technology capabilities in your automation systems will continue to evolve—as well the threats targeted against them. This inventory is a cornerstone of your cybersecurity program so you can then effectively implement the other foundational controls for those assets.

One quick way to achieve a high-fidelity level of inventory is to use a tool that passively collects data on every connected device within your ICS. This same tool not only can tell you what's on your network, but can also baseline normal network communication, inclusive of the industrial protocol, so you can determine if there are any deviations in the baseline and pinpoint changes from normal operations. It's from this baseline monitoring you have a change control process, as you can start to watch for and manage changes in your process configuration.

For example, someone overseeing an oil refinery may know that their most sensitive asset is the system that maintains oil temperatures. A hacker enters an email server by way of an internet-connected device. How do they get from the email server to their target? The hacker needs to follow a path to their target from IT to OT using crackable, vulnerable devices as stepping stones. That's why ICS operators need to have an accurate network map that details each device's configuration and vulnerabilities. You can use that information to make sure there is a conduit in place to block the hacker's path to your most sensitive zones and assets.

2 Change Control

How do you maintain a high level of integrity over your industrial process if you don't have a change management process? Your process should not only outline how to document, approve, test and deploy changes, but also map every change from a configuration of a firewall or switch to a new control program being uploaded to a PLC. A change management process will be most effective when it is enforced with a detective control that highlights all

changes—as all control engineers will know their activity is tracked against authorized work orders or change management requests.

Unauthorized configuration changes or authorized changes made to the wrong devices, whether accidental or intentional, can cripple plant operations systems. These scenarios create unplanned work to remediate outages and can cost a lot of money in production downtime or quality recalls.

Configuration changes can also affect the hardened configuration of a device against a framework like IEC 62443 that can leave it vulnerable to malware and malicious behavior that can quickly negatively impact your ICS. An example of this is the enabling of a USB port when the framework calls for all USB ports to be disabled. Understanding whether configuration changes impact the secure configuration state of a device is critical for reducing the attack surface for malicious behavior.

3 Centralized Log Management

Log management solutions are synonymous with the way a data historian captures and replays process events and sensor measurements for industrial processes. Log management is the act of aggregating log information across all devices in your ICS into a centralized log repository.

These logs provide evidence about the ICS' cybersecurity state and operation. Logs are produced from network devices (switches, routers, firewalls, etc.), operating systems such as Windows and Linux, applications such as SCADA and HMI, and controllers and DCS. Remote access solutions, VPNs and authentication systems such as Active Directory also provide log information.

This raw log data contains a wealth of information that tells how the system or device is operating, like providing an indication that a power supply has failed or highlighting cybersecurity events such as unsuccessful login attempts. It's critical not to ignore this data, as it can be a form of predictive maintenance outlining situations that could create downtime and unplanned work.

4 Vulnerability Management

Vulnerability Management (VM) is the process of understanding what publicly-known vulnerabilities or weaknesses are present on your network, referred to as common vulnerabilities and exposures (CVEs). Most attacks from ransomware and malware are the result of unpatched CVEs that have been known and go unpatched or unremediated before the attacker strikes.

One challenge of implementing VM in OT environments is that most legacy ICS equipment can't handle the interrogation of vulnerability checks from traditional VM scanning technologies. As you get closer to Levels 0 and 1 from

the business networks at Levels 4 and 5, there will be assets that are likely not suitable for active scanning techniques. Devices such as HMIs, data historians and engineering workstations in Levels 2, 3, and 3.5 (DMZ) are probably better candidates for active scanning as these devices are based on traditional IT technology.

As long as you know where they are, ICS assets will benefit from an in-depth vulnerability scan from a VM tool. VM tools score vulnerabilities based on risk in order to help you know which ones to remediate first.

5 Network Zones & Segmentation

Network segmentation is achieved by dividing your network into zones that are organized by groups of systems that are serving a similar operational function and risk profile. A conduit creates the boundaries between zones, where all communication in and out of the zone is denied unless it is explicitly permitted through the use of firewalls or access control lists.

If one device, such as an HMI, gets compromised by ransomware, it can only affect other devices of similar function within the same zone, as the conduit would limit the spread of the ransomware by denying communication between zones. This is a key part of establishing your Defense in Depth strategy.

The IEC 62443 ICS security standard recommends the concept of network segmentation using the zones and conduits strategy.

Zone: *A grouping of logical or physical assets that share common security requirements based on factors like criticality and consequence.*

Conduit: *Creates the boundaries of the zones and denies all communication in and out of the zone unless it's permitted—effectively a network pathway between zones, in which applied controls can resist network-based attacks, shield other network systems, and protect the integrity and confidentiality of network traffic.*

> ***TIP:*** Focusing on monitoring and the configuration of conduits is typically far more cost-effective than having to upgrade every device or computer in a zone to meet a requirement.

PASSIVE vs ACTIVE SCANS & AGENT vs AGENTLESS MONITORING

Some areas of your network require passive scanning to avoid disrupting sensitive legacy systems. Passive scanning is the technique of listening to network traffic and fingerprinting devices as they're found. This aids in

creating an asset inventory, determining communication patterns, mapping networks and detecting vulnerabilities.

On the other hand, active scanning or querying/polling can directly interact with a particular device to glean additional information. Using both active and passive techniques gives you the most robust data. However, there could be limitations with passive monitoring, e.g. network switches may not have the available port capacity to be the aggregator port for mirroring.

Another limitation could be performance capacity of the switch, as it may not have the processing power to perform mirroring as it requires additional processing overhead. Due diligence must be performed to make sure that the switch fabric can support mirroring to meet the needs of data collection for cybersecurity and asset inventory.

> ***TIP:*** **When actively querying a device, you should make sure your scanning solution speaks the asset's native language (such as Modbus TCP or Ethernet/IP CIP). Otherwise, your scans run the risk of halting production by taking a device offline.**

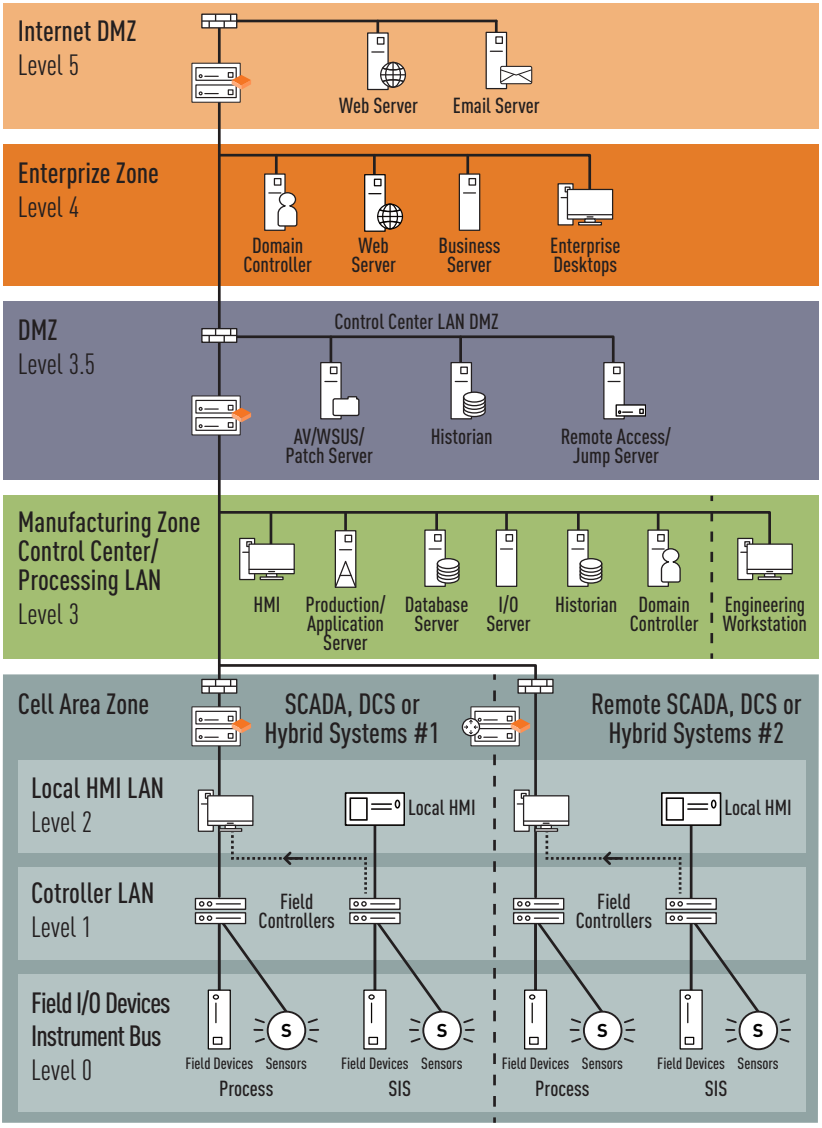
Beyond passive versus active scanning, you also need to understand when and when not to use agents for data collection. While agents provide rich information, as they are installed locally on the device, first make sure that your automation vendor allows for third-party agents to be installed on their HMIs or engineering workstations before attempting.

Agentless scanning also allows you to harvest data from devices—as long as you can get credentialed access. There are countless ways to harvest data agentlessly, so find a solution that provides the most flexibility through both OT and IT protocols. Your best bet is a strategic combination of agentless and agent-based scanning.

THINK IN TERMS OF RISK MANAGEMENT

Don't be overwhelmed by the amount of work it will take to implement all five of these foundational controls in your network. Everyone needs to start somewhere, and that somewhere is generally starting with gaining visibility into what devices you have on your network and their communication patterns, vulnerability posture, configuration state and log information.

Standard Purdue Model Industrial Network Architecture



TIP:

Levels 0–2: Passive scans, and active and passive agentless precise protocol scans

Levels 3–5: Active agentless scans

START THE EXPEDITION

Your ICS Cybersecurity Action Plan

It's one thing to understand the frameworks and foundational controls you need to apply to your ICS in order to keep it secure, but getting organizational buy-in to actually implement those controls is an entirely different undertaking.

HOW TO SPREAD CYBERSECURITY AWARENESS

Sixty-eight percent of ICS professionals believe it would actually take a breach to convince their leadership to make the proper investments. However, taking a proactive approach and having the right conversations with the right stakeholders can save you from having to get serious about security only as a response to a successful attack.

> ***TIP:*** Talk to your CISO and/or CTO about ICS security in terms of the concept of risk management as discussed in Chapter 4.

TIPS FOR GAINING EXECUTIVE LEADERSHIP SUPPORT

1 Create a Security Program Timeline

One way to get the ball rolling on improving your industrial cybersecurity posture is to create a developmental timeline to share with key stakeholders. An ideal high-level timeline will include all of the programs you'll need to initiate or optimize in order to implement all five of the foundational controls.

ICS SURVEY FINDINGS

Tripwire surveyed 263 IT and OT security professionals. All participants had direct responsibility for the security of ICS systems at an energy, manufacturing, chemical, dam, nuclear, water, food, automotive or transportation company with more than 100 employees.

» Eighty-eight percent are worried about the threat of ICS cybersecurity attacks, with the highest rate of concern in the energy and oil & gas industries.

» Industrial organizations have emphasized concern on the physical consequences of a cyberattack. Operational shutdowns and downtime are the biggest concern. Two-thirds (66 percent) believe an ICS attack could be catastrophic.

» Almost two-thirds (61percent) think they could be hit by a successful ICS attack in the next 10 years.

» Only 12 percent have a high level of confidence in their ability to avoid business impact from a cyber event.

» Over the past two years, 77 percent said they have made cybersecurity investments in their industrial environment.

» Fifty percent do not believe their company is investing sufficiently in ICS cybersecurity.

» Of those, 68 percent think they'd need to experience a significant attack in order to invest more.

» Only half (52 percent) have more than 70 percent of their assets tracked in an asset inventory.

» About a third of organizations don't have a baseline of normal behavior for their OT devices, nor a centralized log management solution.

» Only a third (34 percent) have an industrial security assessment, but more than half (55 percent) are thinking about it.

» Most (79 percent) reported the need to better train their teams on OT security.

2 Get an ICS Cybersecurity Assessment

When presenting leadership with the logistics of time and costs of investing in security, a good first step is often an ICS security assessment. Use a trusted third party to conduct a cybersecurity assessment you can then present to your CISO to clearly illustrate the current risk profile the current state brings to safety, productivity and quality. As part of the assessment, it's also good to outline risk with a threat analysis that takes into account the probability alongside the potential impact on the business of a cybersecurity event.

3 Proactively Foster IT/OT Collaboration

Encouraging internal organizational collaboration by creating cross-functional teams with representation from both the IT and OT sides of your organization. Explicitly define roles and scope for security initiatives and understand that IT and OT professionals often have different ways of looking at security. Well-honed communication skills are a must here, and internal workshops are often a great way to get everyone on the same page.

4 Adopt a Framework to Use as a Guideline

An industrial framework such as IEC 62443 is a useful tool for illustrating industry consensus around the importance of ICS security controls to your organization's leadership. Since it outlines recommendations on network architecture, configuration and monitoring, it's a helpful resource in getting key stakeholders in your organization on the same page about security priorities.

BUYER'S GUIDE: ICS SOLUTIONS FOR FOUNDATIONAL CONTROLS

Once you know how to use foundational controls to secure your ICS, it's time to select the right tools for the job. Some solutions will cover multiple foundational controls at once. Some will be built specifically for industrial environments, while others will be able to move with ease across the IT/OT gap. Here are the basic capabilities you'll want to look for when addressing each of the five foundational controls discussed in Chapter 4:

» For Hardware & Software Inventory

Look for a solution that will passively create a real-time map of your entire ICS network, including an inventory of all connected devices. In ICS environments,

"I can't stress enough that IT and OT network engineers need to both understand their respective needs, requirements and philosophies for network security differ from one another quite drastically ... Understanding the critical differences between both sides and having regular communication before security policies are rolled out can help make the IT/OT convergence much easier to manage."

– Scott Kornblue, Industrial Field Application Engineer

it's important to be able to gather this information without disrupting operations—so make sure you select a solution that can not only harvest data passively, but can also actively communicate via native industrial protocols (e.g. Modbus TCP, Profinet, Ethernet/IP, etc.) for asset discovery as well as inventory.

» For Change Control

The basis of effective change control is rigorous file integrity monitoring (FIM) and secure configuration management (SCM). Tools with these capabilities will capture a complete picture of the state of your systems and track any deviations from a known, secure baseline. These basic processes are your best defense against intruders lurking on your network. SCM is also invaluable in tracking compliance drift from policies and frameworks.

» For Centralized Log Management

Look for a log management tool that preprocesses log data before filtering it through your SIEM. Log management tools will also help with asset inventory, as they can passively discover devices as they become connected to your ICS environment. Your centralized log repository needs to be able to help you understand what information devices are producing so you can optimize their performance and ensure the control system stays operational. Think of a log management tool as a cyber historian for your ICS.

» For Vulnerability Management

When it comes to VM, selecting the right tool for an industrial environment takes extra care. In most cases, you'll want a tool that conducts vulnerability scans via a combination of both agentless and agent-based techniques. This is especially useful in circumstances where your environment contains occasionally-connected endpoints. Also, keep in mind that risk scores need to be prioritized in a granular enough manner to help you understand how to remediate the biggest risks first. If you get a flood of high-severity vulnerability alerts without prioritization guidance, you're not using an adequately sophisticated VM tool.

» For Network Zones & Segmentation

The main guidance here from ISA 99/IEC 62443 is to create distinct zones and conduits. For example, you should use a firewall that is industrial protocol-aware to be a conduit for communication between zones. Zones are the organization of specific devices that perform process functions to mitigate the impact of cyber events throughout your industrial network.

TIP: Holistic visibility to control networks will most likely require multiple ways to connect raw data. Focus on solutions that not only have active and passive data collection capabilities but also have hybrid and integrated methods. "Hybrid" means the solution can interact with third-party applications that already have the data, and "integrated" is where network hardware can be used to collect data through embedded sensors or virtualization.

FOUNDATIONAL CONTROLS WITH FORTRA'S TRIPWIRE

Attackers look for the easiest way into your system, which usually means exploiting well-known vectors such as unmonitored systems, unpatched vulnerabilities, flat networks and misconfigured assets. That means the vast majority of common ICS threats can be prevented by focusing on foundational controls and their corresponding processes. Tripwire's industrial solutions are purpose-built to establish the five key foundational controls discussed in this chapter:

Tripwire® Enterprise detects configuration changes across a wide spectrum of devices and can assess the configuration for adherence to cybersecurity frameworks.

Tripwire Industrial Visibility provides ICS operators with total visibility into the devices and activity on their network. It uses change management, event logging and threat modeling to protect your most sensitive assets.

Tripwire LogCenter® collects, analyzes and correlates log data from network devices, controllers, SCADA, servers and applications.

Tripwire ExpertOps℠ Industrial is a managed services version of Tripwire Industrial Visibility that gives busy security teams personalized consulting from trained experts and hands-on tool management.

GAINING VISIBILITY IS KEY

ICS operators need visibility into all network communications between the industrial control network and the corporate enterprise IT network, including remote access through VPNs and cellular activity. It is also important to capture and maintain asset inventory information and understand what industrial protocols communicate between assets (such as HMIs to PLCs) and how they are configured. This information will allow you to maintain an accurate network topology diagram and understand what the baseline should look like and identify vulnerabilities when they arise.

TRIPWIRE'S APPROACH TO ICS SECURITY

Tripwire turns raw ICS data into actionable information. Our holistic tools span the IT/OT landscape, and our large ecosystem of technology integrations and vendor-agnostic solutions give ICS operators plenty of freedom of choice in the selection of automation systems that are best for their business.

Tripwire provides deep visibility through a comprehensive suite of highly-integrated products to detect ICS cyber threats and breaches, prevent future incidents by discovering and prioritizing risks, and continuous monitoring to help keep your security program on track.

Many industrial organizations also lack the personnel necessary to implement and maintain rigid ICS security controls. Tripwire also offers a range of professional services customized for industrial environments, such as security assessments, penetration testing and even on-site resident engineers.

Trusted by thousands of companies worldwide, Tripwire offers over 25 years of experience in leading global cybersecurity solutions.

TAKEAWAY: VISIBILITY, PROTECTIVE CONTROLS, CONTINUOUS MONITORING

Keep these three activities top-of-mind in order to stay out of the weeds when selecting your investments as you build and optimize your cybersecurity program:

1. **Visibility** *Know exactly what's on your network via a complete inventory of hardware and software assets. Know what these devices are communicating with, know if their configurations are changing, know what vulnerabilities are applicable, and know what their logs are telling you. Visibility starts with holistic asset inventory, but also has many other lenses to understand the risk posture of the industrial network.*

2. **Protective Controls** *After visibility is achieved, the right level of protective controls can be implemented based upon which level (per the Purdue Model) the controls are appropriate. Two protective controls that are not optional are 1) network segmentation, and 2) device hardening.*

3. **Continuous Monitoring** *Once you know what you have, monitor it. This takes place across several parallel processes: vulnerability management, security configuration management, log management and file integrity monitoring.*

INDUSTRIAL CYBERSECURITY FAQs

Q: Which devices within my ICS could pose a potential cyberthreat?

A: In the past, an adversary would have to socially engineer themselves onto the plant floor to physically manipulate the instruments within a control system. That, or do something like place a malware-infected USB in the parking lot and hope curiosity gets the best of someone. But in the IIoT age, any connected device that isn't secured poses a threat.

Q: How do we provide a secure method of remote access to our ICS?

A: Controlling remote access is an important part of securing your ICS. Understand and document all remote access connections (like vendor access with dial-up modems, VPN and cellular connectivity) into the industrial control network. Industrial organizations can also use secure authentication solutions to set up multi-factor authentication for remote users, then log all of their activity.

Q: What is the best way to determine what we should do first to mitigate risk of a cyber attack impacting our physical process?

A: Understanding and maintaining an accurate asset inventory of all the components on your industrial network is a great first step. How do you secure something you don't even know you have? Don't stop, however, with visibility to asset inventory. Gain visibility into other critical things (such as configuration changes, device communication pattern baselines, network topology changes, and diagnostic log information) as all of these will assist with the ability to detect and quickly correct from anything that negatively impacts your industrial process.

Q: Do we need to worry about phishing to secure our ICS?

A: Yes. Phishing is a common technique to gain access via email, telephone or text message into the corporate IT network or a control engineer's laptop, which is then used to pivot into the industrial network. Understanding and educating employees for identifying phishing techniques is a critical piece of a Defense in Depth strategy.

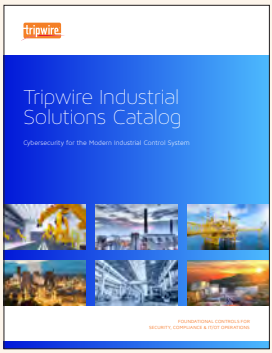
Q: If my ICS isn't regulated by a mandate, do I still need to adopt a cybersecurity framework?

A: While this is not mandatory, these frameworks can help you create and sustain a cybersecurity program to mitigate risk from the impact of cyber events. It's also important to understand that adhering to such a framework is going to take time and investments in people and technology, all of which does

not happen overnight. Leverage these frameworks for guidance and have a plan to implement them over time. Slow and steady wins the race.

Q: Do we need to be concerned about the cloud?

A: Absolutely! The cloud is coming, and in some industrial applications it's already here. Concern, however, is still warranted, and adoption of cloud-based solutions into industrial networks is only a matter of time. And they'll continue to use and adopt more and more IT-related technology and solutions at a faster pace than in the past. SCADA solutions, as well as some monitoring solutions from major automation vendors, have already moved to the cloud. Cost benefits will continue to drive further adoption. Don't assume that cloud solutions are secure, and don't forget to apply foundational controls to the cloud just as you do for any other technology landscape in your environment.



Ready to learn more?

Download Tripwire's Industrial Solutions Catalog

tripwire.me/TISC

SOURCES

[1] Aberdeen Group, Asset Performance Management: Blazing a Better Path to Operational Excellence, November 2017.

[2] Department of Homeland Security National Cybersecurity and Communications Integration Center (NCCIC) and Industrial Control Systems Cyber Emergency Response Team (ICS–CERT), Recommended Practice: Improving Industrial Cyber Security with Defense In-Depth Strategies, 2016.

[3] Department of Homeland Security. (2019). Critical Infrastructure Sectors. [online] Available at: https://www.dhs.gov/cisa/critical-infrastructure-sectors.

[4] Morgan, S. (2019). Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021. [online] CSO Online. Available at: https://www.csoonline.com/article/3200024/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html.

[5] Verizon Data Breach Investigations Report. (2019). Manufacturing Data Breaches & Cybersecurity. [online] Available at: https://enterprise.verizon.com/resources/reports/DBIR/2019/manufacturing/.

[6] Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. (2016). U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team.

NAVIGATING INDUSTRIAL CYBERSECURITY

Nearly every aspect of modern life depends on industrial control systems (ICS) operating as expected. As ICS devices become increasingly connected, they also become increasingly vulnerable. By and large, industrial organizations are underprepared for the digital convergence of their IT and OT environments. ICS operators need to get a robust cybersecurity program in place—and fast. This book covers how to do just that, with clear instructions on implementing industrial frameworks and foundational security controls, aligning IT/OT, gaining executive buy-in and selecting the right tools for the job.

fta-tw-gd-1122-r2-hm