SANS

Analyst Program

Survey

Threat-Informed Operational Technology Defense: Securing Data vs. Enabling Physics

Written by **Dean Parsons**

January 2022

ABS Group

Executive Summary

Cyber attackers have skills well beyond that of traditional intrusion and data-exfiltration techniques, and they have set their sights on industrial control system (ICS) and operational technology (OT) environments. They have illustrated an understanding of control system engineering and demonstrated ICS-capable attacks with tools to gain access and negatively impact operations and safety. In fact, 45% of participants in our survey estimate the current threats to their control systems at high risk today.

The survey results and content herein directly apply across multiple control system sectors and cover many areas, including (but not limited to) realized and evolving threats in the OT/ICS cyber threat landscape and organizations' greatest challenges and effective initiatives in managing an OT/ICS security program. A comparison of cybersecurity between traditional IT and OT/ICS appears front and center. Other points include insight into the ICS risk at different levels in an organization. For example, 61% of survey participants indicate that a gap exists in the perception of cybersecurity risk to their ICS facilities between OT/ICS cybersecurity front-line teams and other parts of the organization. Of these, 35% indicate the gap is between senior management and the OT/ICS cybersecurity front-line teams. Further points cover the investments organizations are making in ICS cyber defense and who's responsible in the organization for OT/ICS cyber defense (and whether that includes the safety of people).

The Certainty of Modern Adversary Capabilities

Attacks targeting critical infrastructure are becoming more prevalent. While incidents in IT are commonly digital data breaches exposing sensitive information, or data deletion causing application downtime, incidents from an ICS cyberattack affect physical conditions or render unexpected physical output that can have serious consequences to the health and safety of people and the environment. Consider a compromised active safety system that pumps crude oil from an offshore tanker to an onshore marine terminal, or compromised engineering sensors that are unable to shut down a gas leak in a pipeline or refinery under emergency conditions.

The Norsk Hydro Incident

OT and industrial engineering control system assets are often compared to traditional IT assets. Recent case studies include the Norsk Hydro incident.

> *"All of that damage had been set in motion three months earlier when one employee unknowingly opened an infected email from a trusted customer. That allowed hackers to invade the IT infrastructure and covertly plant their virus... The financial impact would eventually approach $71 million.*

"'Transparency is core to the Norsk Hydro culture,' says Halvor Molland, senior vice president of media relations. By issuing frequent, candid communications about the events, the company also sought to expose the shadowy tactics of cyber criminals and maybe curb similar threats."[1]

Of the main takeaways, the Norsk Hydro incident highlights the importance of OT/ICS network architecture, with IT and external environments being well segmented from the industrial control system networks. It also highlights several critical steps of OT/ICS network visibility and communications when an incident response plan is executed.

IT Security Is Not OT/ICS Security

Organizations often incorrectly believe they can directly apply IT security practices to ICS environments. While a wealth of knowledge is available from IT security, a "copy and paste" of IT security tools, processes, and best practices into an ICS could have problematic or devastating impacts on production and safety. The Department of Homeland Security makes an accurate statement regarding ICS incident response: "Standard cyber incident remediation actions deployed in IT business systems may result in ineffective and even disastrous results when applied to ICS cyber incidents, if prior thought and planning specific to operational ICS is not done."[2] While cyber incidents in IT environments can lead to undesirable data impacts—such as the unavailability of critical business applications, data corruption, and data loss—the impacts to physical processes are much different. Impacts in ICS environments range from the loss of visibility or control of a physical process to the manipulation of the physical process by unauthorized users, which can ultimately lead to serious personnel safety risks, injury, or even death.

In fact, the principles of traditional incident response—detection and identification, containment, eradication, recovery, lessons learned—are still at play in ICS. For each step of the process, however, organizations need to consider the safety and reliability of operations to prioritize human life and the protection of physical assets. Therefore, steps are expanded, other steps are added, and processes are different to support the differences in missions of IT and OT/ICS.

IT and OT/ICS Security Differences

Traditional IT assets focus on data at rest or data in transit. OT and industrial systems monitor and manage data that drives real-time systems changes in the real world with physical inputs and physically controlled output actions. Simply put, IT focuses on the digital data world, whereas OT/ICS focuses on the physical and safety world.

---

[1] "Hackers hit Norsk Hydro with ransomware. The company responded with transparency," news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/

[2] "RECOMMENDED PRACTICE: Developing an Industrial Control Systems Cybersecurity Incident Response Capability," www.cisa.gov/uscert/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf

Primary differences between IT and OT/ICS industrial systems require that a different approach be taken with control systems environments for OT/ICS. The differences include security incident response, environment and safety, cybersecurity controls, engineering, support, system design, threat detection, and network architecture. Traditional IT security practices directly applied to ICS environments commonly have problematic or devastating impacts. Organizations must adapt security for ICS.

The Business of OT Security

Security teams are commonly resource-challenged in IT, but perhaps even more so in ICS, where additional security and engineering knowledge is required to perform effective ICS active cyber defense. Survey results exemplify this, as 47% of ICS organizations do not have internal dedicated 24/7 ICS security response resources to manage OT/ICS incidents, and just a slightly lower percentage (46%) of ICS organizations do have this function, leaving 7% unsure of their current state.

Main Differences in IT and ICS/OT Security

IT and ICS have completely *different missions.* IT secures digital data at rest and in transit, aligned with data confidentiality, integrity, and availability of business systems. OT/ICS focuses on the physical and safety world by monitoring and managing real-time engineering systems for physical inputs and making changes in the real world with physically controlled output and actions. See Figure 1.

Figure 1. IT and ICS Distinguished Differences[3]

The top roles responding to the survey are the security manager or director at 11%, security architect (12%), and security administrator/security analyst (18%). A full 61% of participants observe a gap in the perception of cybersecurity risk to their ICS facilities, with 35% of those indicating a gap is between senior management and the OT/ICS cybersecurity front-line teams.

The corporate-level CIO/CISO and information technology manager roles, 42% and 38% respectively, are the leading roles responsible for implementing security controls for OT/ICS systems, followed by the ICS owner/operator (33%) and the engineering manager (31%). See Figure 2.

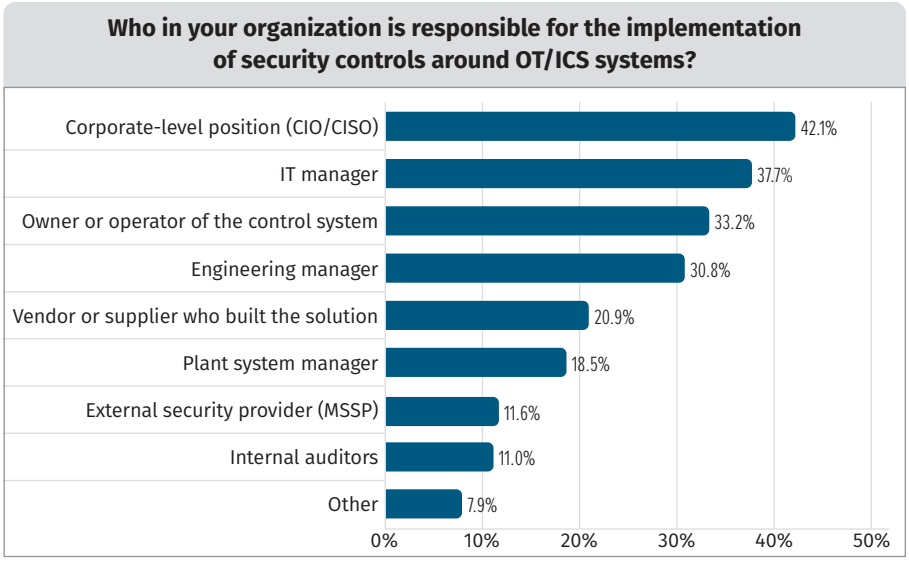


Figure 2. OT/ICS Security Control Responsibility

Safety could be at risk if information or traditional business systems are prioritized over control systems, if the reporting structure fails to fully embrace the differences and prioritization between IT and ICS. Consider, for instance, if an email security incident (IT business) and a SCADA controls communication incident (ICS/OT or engineering) occurs at the same time. Which incident gets the prioritization to focus efforts, tools, and teams to investigate, respond, and defend? What pace and rigor will the organization give to the incident selected as a primary focus? Did the organization select their focus based on the most important for the safety of the people, the environment, and the organization overall? Today's ICS incident response teams must understand the control system processes, the engineering, industrial protocols, safety factors, and ICS-specific cyber threats and tailor incident response playbooks accordingly.

[3] "ICS418: ICS Security Essentials for Managers," www.sans.org/cyber-security-courses/ics-security-essentials-managers/

IT Attacks Impacting ICS and Living Off the OT Land

The community is seeing more ransomware with more sophisticated variants that have the capability to cause more disruption to system assets and process flows. In fact, when asked about the threat categories of most concern, 50% of respondents place ransomware at the top.

Targeting ICS operations using ransomware is a goal of the adversary of late. Adversaries have learned that targeting ICS operations can lead to higher and quicker payouts. However, ransomware in the ICS does not translate to "the power grid goes dark" or "the pipeline explodes." To date, most ransomware variants target and impact assets running traditional operating systems in Purdue Model *Level 4* – Enterprise IT Business Systems, *Level 3* – ICS Plant Site, SCADA Controls, or *Level 2* – HMI, Engineering Workstations.

The community has not yet observed prevalent ransomware threats or impacts directly targeting or impacting the engineering devices in Purdue Model *Level 1* – Process Control, Field Devices or in *Level 0* – Sensors, Hardware Actuators. In some cases, control systems and the industrial process may be able to continue operating safely if traditional operating systems are not available or in manual mode.

However, furthering the need for ICS network visibility and control system–specific network security monitoring (NSM), research does show that adversaries cold weaponize a programmable logic controller (PLC) type of ransomware attack under certain conditions.[4]

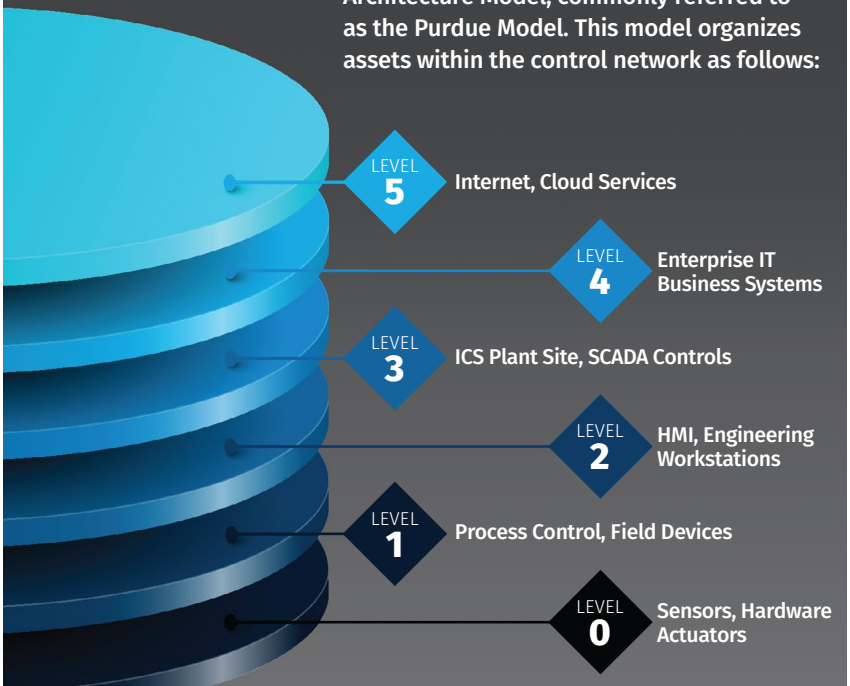
IMPLEMENTATION TIP

ICS-specific incident response tabletop exercises are high-value exercises that help validate ICS-specific incident response plans, while providing awareness of existing defense and adversary threat capabilities and highlighting practical actions for ICS facility defenses (both tactical and strategic). Most respondents (43%) reported that their organization had completed a specific OT/ICS cybersecurity incident response tabletop or other exercise in the past 18 months, with another 17% planning to do so in 2022. This still leaves slightly more than 40% who have not completed such an exercise or who simply don't know the status.

IMPLEMENTATION TIP

Understanding the Purdue Model

Control networks are typically implemented following the Purdue Enterprise Reference Architecture Model, commonly referred to as the Purdue Model. This model organizes assets within the control network as follows:



Organizations can add affordable security by segmenting the control network into these levels and by following the SANS ICS410 SCADA Architecture Reference Model.[5]

[4] en.wikipedia.org/wiki/LogicLocker

[5] "Control Systems are a Target," October 1, 2021, www.sans.org/posters/control-systems-are-a-target/

The Colonial Pipeline Attack

On May 7, 2021, potential dependence on IT applications by controls systems was identified during a cyberattack on the Colonial Pipeline. The US oil pipeline system, which originates in Houston, Texas, and carries gasoline and jet fuel mainly to the southeastern United States, suffered a cyberattack from DarkSide ransomware[6] directly targeting its IT business network. The attack impacted billing, shipping, and logistics systems for the control system that runs part of the pipeline operations.

This attack highlighted the criticality of industrial control systems we rely on for daily life. The Colonial Pipeline transfers huge amounts of fuel across its 5,500-mile infrastructure in a region where the shutdown caused panic buying among individual consumers and a massive fuel shortage for large industrial customers. Fully understanding dependencies of OT/ICS systems on IT applications or networks should be known and part of an organization's incident response plan.

Organizations can discover and test whether their ICS facility can work in isolation or in a manual mode by using embedded engineering HMIs or other means by performing dedicated ICS IR tabletop exercises.[7] The results could be surprising and help identify dependences on systems, processes, and other external networks such as the IT network or external services.

Access and Living Off the ICS Land

More and more ICS adversaries are using IT malware for access to an environment, often compromising IT business networks first and then gaining access to the ICS networks from there. In many cases, adversaries learn about the ICS network from the business network. Organizations may store engineering project files (ladder logic), control network architecture diagrams, as-build documentation, and control system configuration files on the business network. Attackers target this sensitive ICS data, which can then assist attackers in an ICS Cyber Kill Chain Stage 2 attack with impact.

Once in the control environment, attackers often use engineering software and a system against itself, known as *living off the land*, rather than using additional malware. Consider human adversaries causing negative impacts on processes or safety ramifications by directly interacting with the control environment using legitimate operational software with malicious intent. We witnessed this human machine interface (HMI) in 2015 in the Ukraine power grid attack and outages.

Why would adversaries waste time finding, testing, and deploying exploit attack code if they don't have to? Many identified vulnerabilities provide capabilities to the adversaries that could be similar in nature to features already inherent to control systems themselves. The ability to adjust engineering and process control settings can affect the real world (for example, shutting down, enabling, isolating, and manipulating the industrial process components).

Security analysts have observed ICS attack groups living off the land (that is, abusing systems, features, and even industry protocols themselves that are native in industrial environments and thus turning the systems against themselves). The community witnessed living off the land as far back as HAVEX[8] in 2014, and more recently we witnessed it with the tailored CRASHOVERRIDE[9] ICS-specific framework, which targeted electric power grids with significant impact—loss of power to a large region in the Ukraine.

---

[6] en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack

[7] "Top 5 ICS Incident Response Tabletops and How to Run Them," June 16, 2021, www.sans.org/blog/top-5-ics-incident-response-tabletops-and-how-to-run-them/

[8] https://us-cert.cisa.gov/ics/alerts/ICS-ALERT-14-176-02A/

[9] "CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations," www.dragos.com/wp-content/uploads/CrashOverride-01.pdf

Attacks Impacting Safety

In 2021, an attack used the legitimate HMI application that runs the Oldsmar water treatment facility to manipulate water treatment operations, which could have resulted in *severe health and safety consequences* to human life. The attacker gained unauthorized access directly to HMI from the internet. Using HMI, the attacker increased the level of sodium hydroxide: "the main ingredient in drain cleaner … from 100 parts per million to 11,100 parts per million, dangerous levels that could have badly sickened residents if it had reached their homes."[10] Engineering and operations staff noticed the incident at the plant and restored the industrial processes to normal operations by readjusting the chemicals to a trusted engineering setting for normal non-toxic levels.

The Oldsmar event draws attention to the importance of vulnerability management and protection of ICS, starting with external services and internet-facing access. Organizations should prioritize common open source intelligence (OSINT) exercises trialed for ICSs and use them to uncover vulnerabilities from an attacker's perspective on the internet.[11]

Organizations can detect (and, better yet, proactively defended against) these types of attacks, even in their range of sophistication, before impact by deploying and maintaining the ICS Active Cyber Defense Cycle (ACDC) discussed later in this paper.

ROI on OT Asset Inventory and OT Network Visibility

Having an established and managed (regularly updated, assessed, and monitored) ICS asset inventory of OT devices and engineering assets will drastically improve industrial control system security functions. Updated asset inventories and network visibility align with best practices for ICS active defense needed to protect against the current and evolving threats our facilities face. Both aid in identifying the ICS risk surface by combining it with threat intelligence, and both assist in ICS IR scenarios, making for real-time visibility into an unfolding attack. Facilities can leverage and expand any existing engineering asset inventory, or build one, which then adds immense value as a step toward a proactive ICS cybersecurity program.

The majority of respondent organizations (60%) have a formal process to inventory OT/ICS assets. However, SANS would like to sound the alert of increased risk for the 30% of respondents who currently do not have a program and the 10% who remain unsure of the status of their inventory.

[10] "'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town," www.nytimes.com/2021/02/08/us/oldsmar-florida-water-supply-hack.html

[11] "SANS ICS Site Visit Plan," May 10, 2021, www.sans.org/blog/sans-ics-site-visit-plan/

Four main methodologies enable us to establish the inventory, which we can also combine for improved accuracy. For example, physical inspection will take advantage of face-to-face security awareness and educational discussion, as it is on-site with engineering and operational teams. Physical inspection augmented with passive network captures can create and verify an inventory while providing network traffic to sift through for threat detection. See Figure 3.

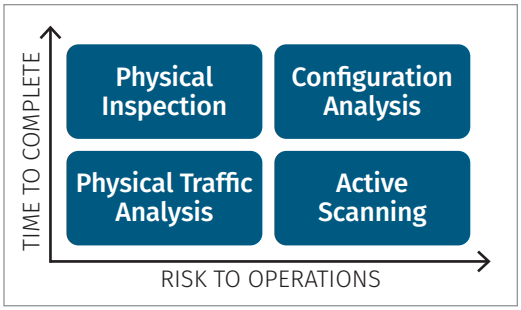


Figure 3. Four Methods of ICS Asset Identification, Time vs. Risk

1. **Physical inspection—**Getting physically to industrial facilities, documenting the hardware seen in racks, cabinets, on the plant floor, software and protocols used, etc. Time-consuming, accurate, and expensive if traveling to remote sites. Some potential physical risk exists, so personal protective equipment (PPE) is required on sites.
2. **Passive network packet capture—**Non-intrusive to ICS operations, accurate representation of natural network comms. Can be quick. Can output a visual network diagram that organizations can print and use for engineering troubleshooting and ICS incident response. But this is a point in time and may not get all assets if not communicating at the time of capture.
3. **Active scanning—**Intrusive to ICS operations, unnatural representation of network comms, but very fast and very detailed information about devices, services, etc. Should be tested in a development environment prior to scanning any production environment.
4. **Configuration analysis—**Many control system and network devices may have to be accessed to review configuration settings. Switch and firewall configurations can reveal IP address and MAC address pairings through Address Resolution Protocol (ARP) tables to indicate devices allowed or denied access on the network. Traffic and port information at a 5-tuple level could reveal general protocols in use. However, it may not reveal details needed for risk assessments and to leverage threat intelligence.

IMPLEMENTATION TIP

Leveraging ICS Asset Inventory and Threat Intel

Start by reviewing any previously created network diagrams. Even with a very low budget, use an encrypted laptop with at least a basic spreadsheet application to start cataloging and storing ICS asset information during a physical site walkthrough. At a minimum, record the following attributes from the commonly targeted critical assets, such as data historians, HMI, PLCs, engineering workstations, core network devices, and active safety instrumented systems (SIS) being used:

- **Model/manufacturer**
- **Serial number**
- **Firmware version**
- **Applications installed**
- **Industrial protocols used**
- **Purpose of assets in the ICS**
- **IP address**
- **MAC address**

Identify your risk surface by searching across your established formal ICS asset inventory for known vulnerabilities and attack methods by leveraging sector-specific threat intelligence. Organizations can add additional real-time vulnerability assessment processes and technology (passive preferred) to provide a real-time view into the risk surface of an environment.

ICS Security ROI: ICS/OT Controls

Of the controls currently in use inside OT/ICS environments, the top three are antivirus solutions (57%), ICS asset inventory (53%), and backup and recovery (49%). See Figure 4.

A control such as endpoint antivirus agents for OT/ICS are limited to installation and protection of traditional Windows or Linux operating systems, only—a small portion of all of the engineering devices used in control system environments. Because no prominent antivirus solution exists for engineering assets such as PLCs, remote terminal units (RTUs), meters, or embedded HMIs, organizations can leverage control system network visibility (also known as *network security monitoring* or *NSM*). While not specific to ICS, NSM does excel in control systems due to the static nature of control networks compared with IT networks. NSM applied to ICS is a human-powered process using technology that must understand the many industrial network protocols to proactively and passively (without disrupting operations) detect cybersecurity threats to control environments. The benefits of NSM in ICS go beyond security, however, and they support engineering troubleshooting and safety as well. ICS NSM is especially important in the case of adversaries living of the land, where it is unlikely endpoint antivirus agents would detect the abuse of legitimate control system functions either on endpoints or on a network.

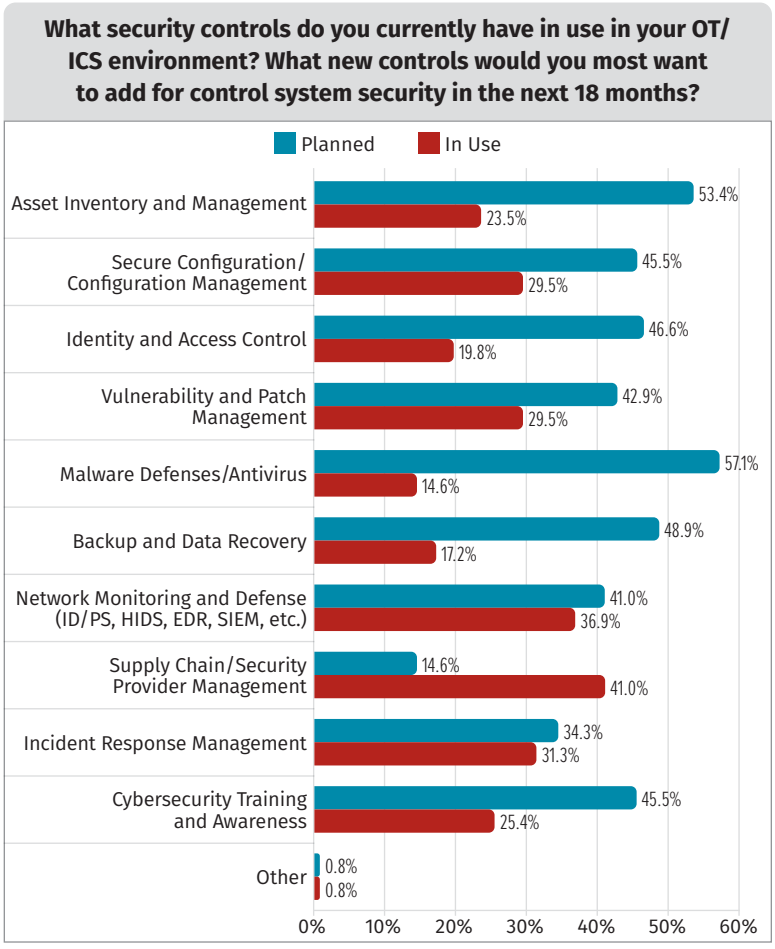


Figure 4. Current and Planned OT/ICS Security Controls

ICS asset inventory management follows antivirus solutions at 53%. This is a known critical phase of proactive ICS/OT defense that really positions facilities for modern defense. A formal inventory can ultimately lead to ICS-specific threat hunting, making for a very strong, mature, and safer state.

Backup and recovery processes rank among the top three controls, which is unsurprising given the recent influx of ransomware, to which recovery from such a cyber incident usually entails restoring infected systems from backup. For ICS operational resilience, all ICS backup/recovery plans must go beyond the traditional operating systems and essential engineering software. They must also include backing up the configuration settings of engineering hardware devices at the lower levels of the Purdue Model (protection and control relay settings in the electric utility sector, for example, or safety instrumented system settings in PLCs that operate the ballast control system in an offshore oil rig).

Backup and recovery features for engineering systems and settings may vary from vendor to vendor. In some cases, facilities may rely on vendor contracts to support their production systems, which may include backup and recovery services. Facility owners should include the available capabilities and vendors services in their regular backup and recovery exercises for verification or improvement of this control.

Several ICS facilities fell victim to the EKANS ICS-tailored ransomware, including Honda[12] and multinational energy company Enel Group,[13] where the adversary group demanded $14 million in ransom for the decryption key and to prevent the attackers from releasing terabytes of stolen data.

"2020 saw the first ICS-tailored ransomware families. This began with EKANS (aka SNAKE), which was responsible for multiple ransomware cases in the community, including the forced shutdown of some of Honda's factories as well as Enel group and numerous undisclosed compromises. ...EKANS featured additional functionality to forcibly stop a number of processes, including multiple items related to ICS operations. For ICS operations in particular, backups must include last known-good configuration data, project files, and related items to enable rapid recovery should a disruptive event occur."[14]

Control System Components at Risk

Computer assets on business networks differ from critical assets and components in a control system environment. Adversaries in targeted attacks on OT/ICS have illustrated their knowledge of engineering components, industrial protocols, and which assets are critical to the engineering process. Targeted OT/ICS attacks go well beyond targeting a traditional operating system commonly found in a business network or office setting. In many cases, adversaries may scale these attacks to impact a wide variety of ICS facilities, including maritime operations, critical manufacturing, and power grid systems, as well as pharmaceutical, chemical, and wastewater management facilities.

When asked about which control system components are considered at greatest risk for compromise, we are seeing expected results, but some outliers are worth noting.

Fifty-six percent of respondents see the HMI as having the greatest risk for compromise, followed by engineering assets (workstations, as observed with TRISIS,[15] instrumentation laptops, ICS calibration assets) at 51%. Curiously, although identified in several ICS-targeted attacks rendering major operational impacts the past several years, only 8% believe the data historian is at risk of compromise. An example of data historian compromise, allowing adversary access from IT into OT/ICS, is the use of CRASHOVERRIDE leveraged by the activity group Electrum: "The group used Microsoft SQL database servers as the gateway that bridges both the business and industrial control networks, to successfully compromise industrial control systems where they used stolen credentials to execute code."[16] See Figure 5.

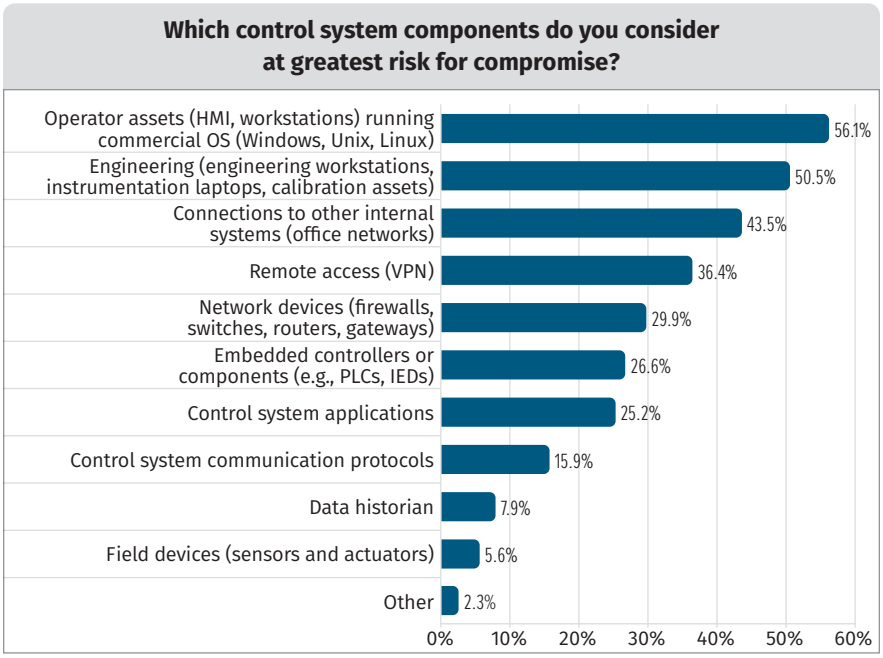


Figure 5. System Components Considered at Risk of Compromise

[12] "Honda Shuts Down Factories After Cyberattack," www.popularmechanics.com/technology/security/a32825656/honda-cybersecurity-attack/

[13] "European Giant Enel Hit by Ransomware Gang Netwalker," techgenix.com/enel-hit-by-ransomware/

[14] "EKANS Ransomware and ICS Operations," www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/

[15] www.cisa.gov/uscert/ics/MAR-17-352-01-HatMan-Safety-System-Targeted-Malware-Update-B

[16] "ELECTRUM," www.dragos.com/threat/electrum/

ICS threat intelligence reminds us of common attack tactics, techniques, and procedures where adversaries have time and time again initially compromised IT business networks and from there compromised data historians to abuse the trusted relationship of this critical OT/ICS asset to pivot from IT business networks into ICS control networks. The IT business network remains a common initial intrusion point for adversaries as mapped using the ICS Cyber Kill Chain[17] Stage 1 attack. A Stage 1 attack helps adversaries prepare for a potential pivot into the ICS environment for an ICS Cyber Kill Chain Stage 2 attack, with direct impact to engineering operations.

ICS System and Network Visibility

We cannot detect or respond to threats unless we have OT/ICS visibility and we look for them. It's too late when safety and operational impacts are seen from a cyberattack. Survey results show that visibility is an area that warrants improvement. When asked about ICS visibility, 65% indicate their visibility is limited for their control systems, while only 22% have visibility needed to defend against modern threats, and 7% have no visibility into their control systems. See Figure 6.

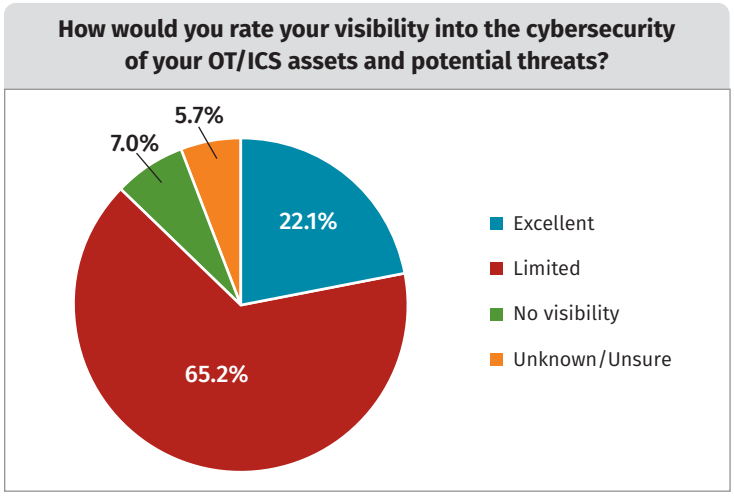


Figure 6. OT/ICS Asset and Threat Visibility

ICS system and network visibility is critical for any ICS defense program for all ICS sectors. We think this is recognized in the community and will likely continue to improve in the short term and provide long-term benefits. As a start, organizations will benefit by rectifying the identified shortcoming of suboptimal visibility to gain significant value with ICS network visibility.

IMPLEMENTATION TIP

A formal ICS asset inventory is a prerequisite and best practice in preparing for an effective cyber defense against today's modern threats. As an inventory initiative is kicked-off, OT/ICS teams can start with the critical assets outlined below. Adversaries often target these critical industrial assets with malware, but human adversaries can also cause negative impacts by directly interacting or abusing them—using legitimate operational software with malicious intent. At a minimum, organizations should protect and regularly monitor access control, control system network traffic, and system integrity for these industrial assets with ICS-specific solutions and processes:

Data historian—This is a database that stores operational process records. Data historians are usually positioned in a network segment that may be accessible by IT and ICS. This critical ICS asset could allow trusted network connections and data channels between the business network and control system networks. Adversaries may use it to act as a pivot point from a compromised asset in IT to an asset in the ICS network. Usually seen in Level 3 of the Purdue Model.

Engineering workstation—The engineering workstation has software to program and change PLC and other field device settings/configurations. Usually seen in Level 2 or 3 of the Purdue Model.

Human machine interface—HMI is a visual interface between the physical process and operators that is used to monitor, control, and change almost any part of the industrial process. Usually seen in Level 3 of the Purdue Model.

Programmable logic controllers—PLCs connect the physical hardware, run logic code to read or change the state or a process, and interface with devices that make physical changes in the real world. Usually seen in Level 1 of the Purdue Model.

[17] "The Industrial Control System Cyber Kill Chain," October 5, 2015, www.sans.org/white-papers/36297/

Increased visibility into control system assets (52%) and implementing ICS-specific network security monitoring (NSM) for control systems (51%) rank as the top two budgeted initiatives for organizations within the next 18 months. See Figure 7.

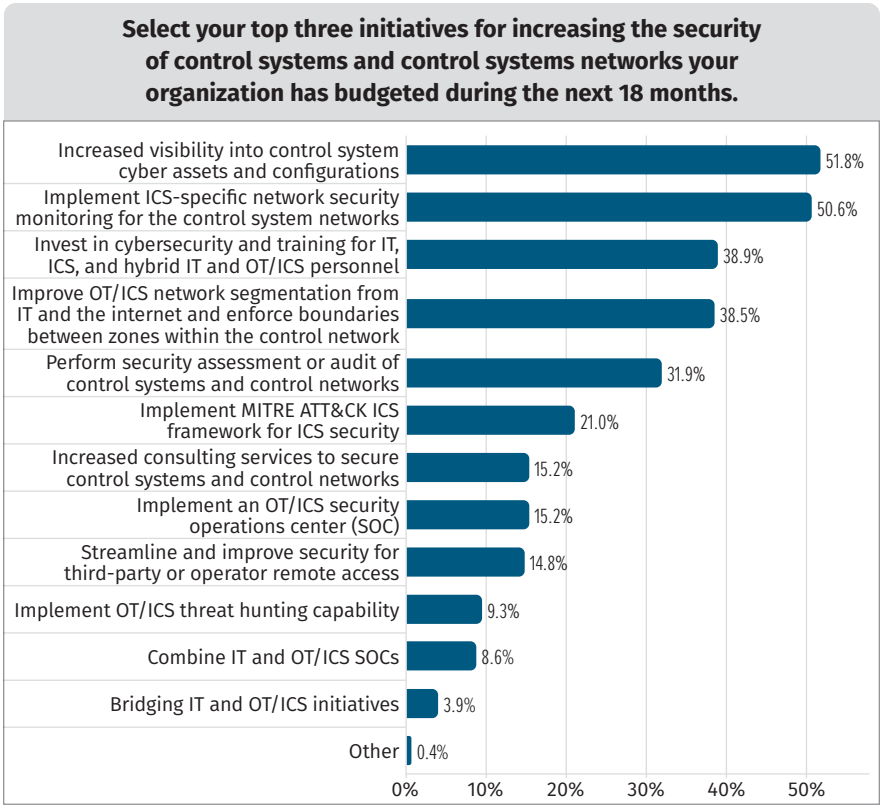


Figure 7. Planned Initiatives for Increasing ICS Security

Threat-Informed OT Active Cyber Defense

How can OT/ICS security managers improve their security program and lead their teams to success? By first allocating resources through new hires, or changing internal roles to focus exclusively on ICS security, and then positioning ICS security team members and technologies in an active defense position within the Sliding Scale of Cyber Security. The active cyber defense is that process of dedicated trained ICS human analysts leveraging technology to monitor, respond to, and learn from threats internal to the control network. Active defense proves most effective when built on top of ICS network architecture, followed by passive defenses, and a documented asset inventory.

Organizations also have the option of outsourcing ICS/OT-specific cyber defense but doing so has its own set of pros and cons OT cybersecurity managers will need to consider. One benefit could be reduced cost for outsourcing OT security resources (such as external ICS/OT incident response retainers to augment any exiting internal security staff).

Threats, Monitoring, and Detection

Organizations are leveraging cyber threat intelligence (CTI) for advantages to drive proactive tactical and strategic security changes. Actionable threat intelligence should provide specifics on adversary attacks and illustrate ways to identify and mitigate such threats, and it's best if the intelligence is sector specific.

For example, technical threat intel would include indicators of compromise (IoCs) in the form of malicious IP addresses, hashes of malicious files, and other technical signatures associated with evolving and ongoing attack campaigns. Security analysts commonly use IoCs to scope how a compromise has spread and to identify the affected devices, engineering systems, and parts of the control system process. They may also be ingested into security controls to alert security teams when they are detected on an endpoint or network security solution, with the best being ICS-specific solutions.

IoCs are not without their limitations, however. They prove useful for only a limited time and are easy for adversaries to change. For example, malware file hashes and IP addresses used as part of an adversary's campaign can change quickly, thus decreasing the usefulness of IoCs over time.

Proactive ICS security teams should leverage threat intelligence tactics, techniques, and procedures (TTPs) in their defense strategy for longer-lasting defense measures. TTPs are adversary attack behaviors or tradecraft that organizations can use to prevent attacks. Examples of tradecraft include how the adversary executes an attack; which devices are commonly targeted, abused, or exploited; and which technical attack tools have been observed in previous attacks for adversary persistence, network lateral movement, data exfiltration, and remote access.

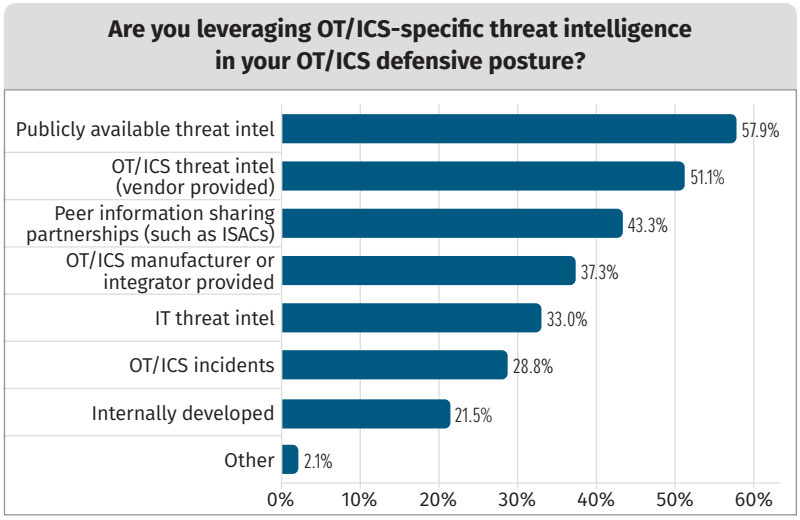


Figure 8. OT/ICS-Specific Threat Intelligence

Threat intelligence by nature relies on sharing information insights into current and evolving threats. Most respondents (45%) indicate the current threats to their control systems are high, with another 15% rating the threats as severe/critical. Another 29% consider threat levels moderate. Yet we are seeing more facilities use publicly available threat intelligence rather than ICS-specific threat intelligence to become more aware of attacks, defenses, and risk-mitigation strategies. See Figure 8.

Cyber threat intelligence can come in many forms: hardware or software vulnerability advisories, technical indicator feeds via the STIX/TAXII protocol, strategic cyber threat reports, malware analysis reports, and open source technical maps of tactics and techniques observed in the wild. They can also come in the in the form of security advisories from common ICS vendors such as Siemens, ABB, Rockwell, Emerson, SEL GE, and so on. Threat intel sources or products can be evaluated for applicability and quality by using the CART methodology as described by Dragos.[18]

While ISACs and publicly available threat intelligence reporting can come at low or no cost, commercial OT/ICS CTI services excel in providing timely reporting and specific control system detail needed to proactively defend against emerging threats. This is the case because many OT/ICS-specific vendors conduct their own in-depth cybersecurity incident response across multiple sectors and are likely in the best position to have the most detail on recent events. The observations from their work in the field feed their CTI report generation directly. By having security teams leverage ICS-specific threat intelligence, facilities can prioritize their team members on the most relevant or severe cyber threats first.

Open source or freely available threat intel sources include the following:

- **SANS: Internet Storm Center[19]**
- **Cybersecurity & Infrastructure Security Agency Industrial Control Systems Advisories[20]**
- **Department of Homeland Security: Automated Indicator Sharing[21]**
- **National Council of ISACs[22]**
- **The U.S. FBI InfraGard Portal[23]**
- **UK National Cyber Security Center CNI[24]**
- **Electric Sector ISAC[25]**
- **Oil and Natural Gas ISAC[26]**
- **Canadian Centre for Cyber Security[27]**
- **MITRE ATT&CK for ICS[28]**
- **MITRE ATT&CK for Enterprise[29]**

[18] "Industrial Control Threat Intelligence," www.dragos.com/wp-content/uploads/Industrial-Control-Threat-Intelligence-Whitepaper.pdf
[19] isc.sans.edu/threatfeed.html
[20] https://us-cert.cisa.gov/ics/advisories
[21] www.cisa.gov/ais
[22] www.nationalisacs.org
[23] www.infragard.org
[24] www.ncsc.gov.uk/section/advice-guidance/all-topics
[25] www.eisac.com
[26] ongisac.org
[27] cyber.gc.ca/en/alerts-advisories
[28] collaborate.mitre.org/attackics/index.php/Main_Page
[29] attack.mitre.org/matrices/enterprise/

Future OT/ICS Investments

When asked about the top three initiatives for improving ICS security and defense budgeted for the next 18 months, a positive trend shows investments in ICS security training for security staff, implementing ICS-specific NSM, and increasing visibility into cyber asset configuration and inventories. See Figure 9.

Figure 9. Planned OT/ICS Investments

The bar for best practices for ICS security is set at deploying and maintaining the ICS Active Cyber Defense Cycle (ACDC). It is a repeatable process driven by human cyber defenders, (trained in both cybersecurity defense and engineering knowledge about your process), who secure, maintain, monitor for, and respond to threats in control system environments.

The Active Cyber Defense Cycle

ACDC guides a team to active defense through these five continuous phases, once a strong ICS asset inventory is established (see Figure 10):

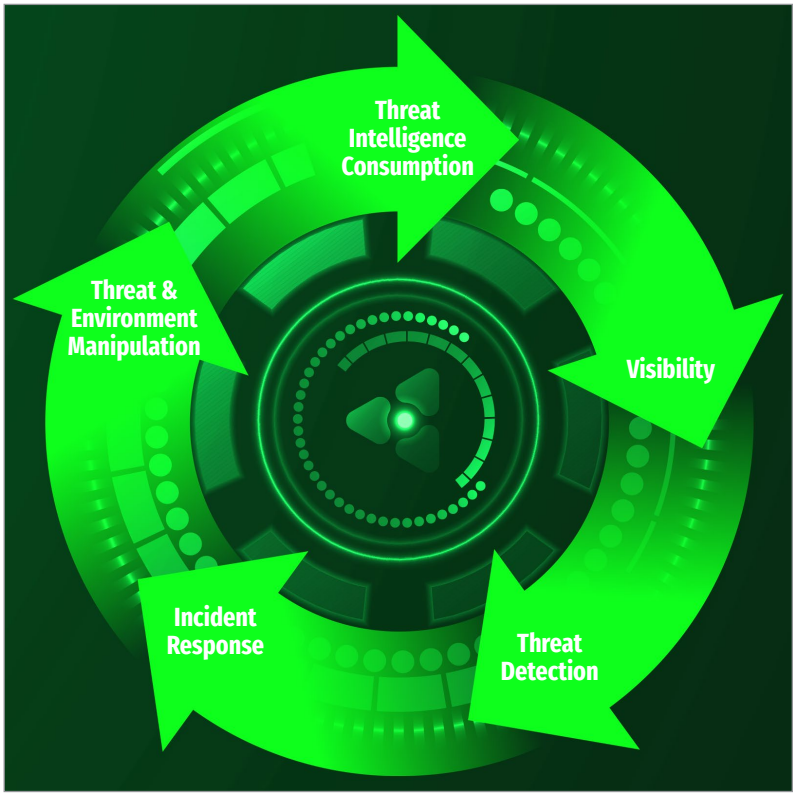


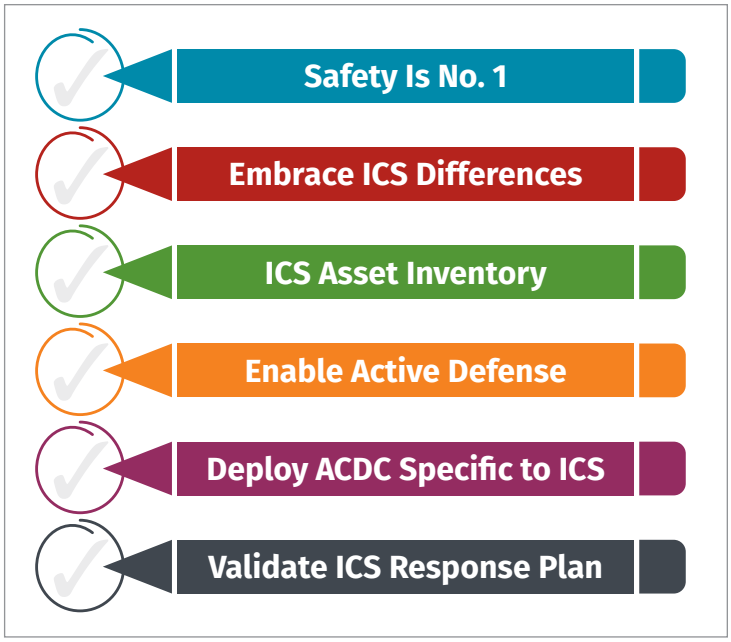
Figure 10. Active Cyber Defense Cycle[30]

1. **Threat intelligence consumption—**Cyber threat intel is refined information with context on cyber threats and threat groups, which defenders can leverage to detect, scope, or prevent the same or similar attacks previously observed.
2. **Visibility—**Take control of your OT cybersecurity by increasing visibility. This means having a formal asset inventory, having at least a passive view of the ICS network, utilizing technology that can dissect and properly interpret specific industrial protocols in network traffic streams.
3. **Threat detection—**Detecting threats requires the capability to leverage technology that sifts through data for malicious signs of attack attempts or intruder entry.
4. **Incident response—**Successful incident response requires being prepared to execute quick triage and adapting steps of incident response specific to control systems while maintaining and considering safety.
5. **Threat and environment manipulation—**To make the environment less habitable for threat actors, defenders need to know how to change the threat during the attack or change the control system. A threat is defined as a malware capability introduced by a threat actor or as human threat actors using legitimate operational software or legitimate protocols with malicious intent to cause negative impacts.

[30] "ICS515: ICS Visibility, Detection, and Response," www.sans.org/cyber-security-courses/ics-visibility-detection-response/

Call to Action: A Prioritized List

Ideally, ICS facilities should consider these top takeaways to kick-start or mature their ICS cybersecurity program:



1. **Safety Is No. 1.** In control system environments, safety is the top priority, and cybersecurity and other functions support the safety and reliability of operations. For example, tools like intrusion *detection* are preferred due to side effects of false positives in intrusion prevention systems, which render an unsafe condition that could hurt or kill people.
2. **Embrace IT and OT differences.** Fully understand and embrace the differences between IT and OT by prioritizing the OT mission—secure and enable physics that monitor for and make physical changes in the real world that are safe for people and the environment.
3. **OT/ICS asset inventory.** A prerequisite for active defense that also streamlines risk analysis and a facility's risk surface is a formal ICS/OT asset inventory. The four main methodologies of creating an ICS asset inventory can be combined for increased accuracy.
4. **Enable active defense.** Ensure the ACDC has a strong foundation by implementing ICS/OT-specific architecture (align with the Purdue Model to start) and passive defense first, to prepare for active defense on the Sliding Scale of Cyber Security.[31]
5. **Deploy ACDC specific to ICS.** Empower technical ICS security staff to maintain the human-driven ICS/OT ACDC. Leverage sector-specific ICS/OT threat intelligence, dedicated and ICS/OT specifically trained security resources who understand the engineering process at the facility to determine if control network traffic is anomalous or malicious in nature.
6. **Validate the ICS/OT incident response plan.** Validate and gain the many benefits of regularly executing a specific ICS/OT incident response plan tabletop exercise, and then apply the lessons learned.

Sponsor

SANS would like to thank this paper's sponsor:

ABS Group

[31] "The Sliding Scale of Cyber Security," September 1, 2015, www.sans.org/white-papers/36240/