Analyst Program

Survey

The State of ICS/OT Cybersecurity in 2022 and Beyond

Written by **Dean Parsons**

October 2022

Executive Summary

The industrial control system (ICS)/operational technology (OT) security community is seeing attacks that go beyond traditional attacks on enterprise networks. Given the impacts to ICS/OT, fighting these attacks requires a different set of security skills, technologies, processes, and methods to manage the different risks and risk surfaces, setting ICS apart from traditional IT enterprise networks.

Adversaries in critical infrastructure networks have illustrated knowledge of control system components, industrial protocols, and engineering operations. From the previously observed impactful attacks, such as CRASHOVERRIDE[1] in the electric sector, human machine interface hijacking through remote access[2] in water management, and ICS-specific ransomware[3] in the manufacturing and energy sectors, to the more recent Incontroller/PIPEDREAM[4] advanced scalable attack framework targeting multiple ICS sectors, ICS/OT attacks are more disruptive with the possibility of physically destructive capabilities. Threat intelligence supports the fact that industrial security defenders across all sectors must address new challenges and face serious threats.

The 2022 SANS ICS/OT Cybersecurity survey results reveal several changes and significant focus on ICS operational improvements; however, progress in key areas needs more emphasis to defend our critical infrastructure into the future. Industrywide insights from this survey include:

- Significant change in who is being called to perform ICS incident response
- A shift in the responsibility for implementing security controls in ICS/OT
- Continued value and investment in ICS-specific training and skillset development
- Steady increase in obtaining the benefits of an ICS asset inventory
- A more dedicated focus on ICS operations
- A significant uptake in ICS-specific threat intelligence for active threat-hunt defense
- Industry struggles on actions related to threat detection coverage
- Continued adoption of MITRE ATT&CK for ICS framework

IT and ICS/OT Security Differences Defined[5]

ICS/OT assets are often compared to traditional IT assets; however, traditional IT assets focus on data at rest or data in transit. ICS/OT systems monitor and manage data that makes real-time changes in the real world with physical inputs and controlled physical actions. Some of the technical differences that set ICS apart from IT are: the prioritization of passive asset discovery and passive threat detection, low-bandwidth sites, critical yet legacy devices, proprietary engineering protocols, engineering systems not running traditional endpoint operating systems, and requirements for engineering hardware to be ruggedized and operate extremely reliably in harsh and even hazardous environments, to name a few.

[1] "Alert (TA17-163A), CrashOverride Malware," www.cisa.gov/uscert/ncas/alerts/TA17-163A

[2] "Alert (AA21-042A), Compromise of U.S. Water Treatment Facility," www.cisa.gov/uscert/ncas/alerts/aa21-042a

[3] "Ekans/Snake NJCCIC Threat Profile," www.cyber.nj.gov/threat-center/threat-profiles/ransomware-variants/ekans-snake

[4] "Alert (AA22-103A), APT Cyber Tools Targeting ICS/SCADA Devices," www.cisa.gov/uscert/ncas/alerts/aa22-103a

[5] "The Differences Between ICS/OT and IT Security," February 1, 2022, www.sans.org/posters/the-differences-between-ics-ot-and-it-security

It's these primary differences between IT and ICS/OT industrial systems that drive differing requirements for incident response, environment and safety concerns, cybersecurity controls, engineering, support, system design, threat detection, and network architecture. This is because IT focuses on the digital data world, whereas ICS/OT focuses on the physical and safety world.

The 2022 SANS ICS/OT survey received 332 responses representing a wide range of industrial verticals from the energy, chemical, critical manufacturing, nuclear, water management, and other industries. See Figure 1. Of the 63 subcategories across these verticals, many respondents are subclassified in electricity, oil and gas, equipment manufacturing, specialty chemicals, transportation equipment manufacturing, drinking water, and engineering services.

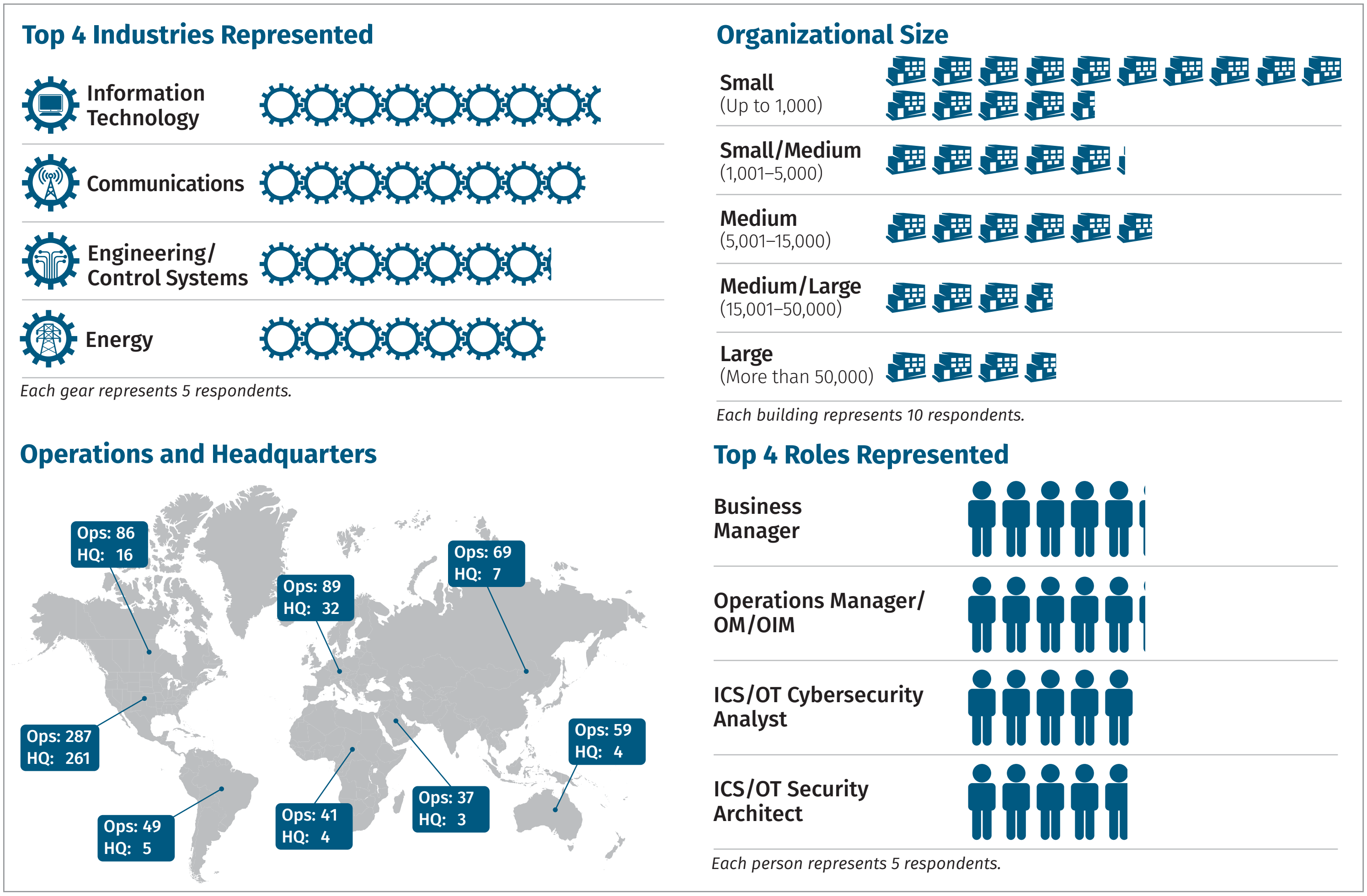


Figure 1. Demographics of the Survey Respondents

Twenty-two percent of survey respondents consider the current cybersecurity threats toward ICS as severe/critical, whereas 41% consider them to be high. This represents a slight but steady increase year over year across 2019 (38%), 2021 (40%), and 2022 (41%).

Nearly 80% of respondents have roles that emphasize ICS operations, compared with 2021 when only about 50% did. Those indicating their roles emphasize both ICS and business-related activities suggest there is still a convergence in responsibilities even though the areas have different missions, skillsets needed, and impacts during a security incident. Overall, respondents are spending most of their time on ICS operations. See Figure 2.

Across the verticals, the data continues to reveal industrial control system security training and certification is sought after. Slightly more than 80% of respondents hold certifications relevant to control systems security. This is a significant jump from 54% in 2021, and shows continued industry investment in the value of certification. SANS certifications account for the top two categories: Global Industrial Cyber Security Professional (GICSP) (49%) and Global Response and Industrial Defense (GRID) (27%).

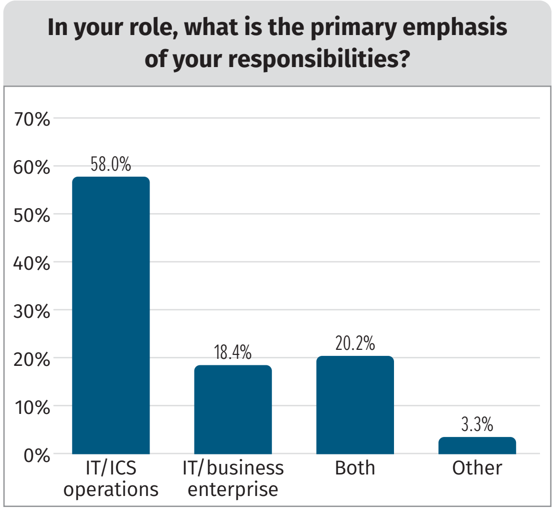


Figure 2. Primary Responsibilities

People in the ICS security workforce are in high demand. Hiring managers may be looking for specific ICS certifications. Existing employees may look to options to increase their knowledge or solidify their career path by obtaining accreditation in ICS security specifically, for example, in ICS active defense and incident response.[6]

Convergence: Where Are We?

Traditional off-the-shelf operating systems, commonly seen in office environments, have been used in the upper levels of control networks for decades to help automate engineering operations. Given they have a mission of engineering and safety, they should be maintained and secured differently than traditional IT assets; that is, they should be treated, managed, maintained, and secured as ICS/OT assets.

ICS/OT Is the Business

Facilities recognize the business is the control systems running critical engineering assets, and they must be protected for business survival. With the evolution of new attack frameworks, legacy devices, evolving technology options, and resource constraints, the biggest challenge with securing control systems technologies and processes is the technical integration of legacy and aging ICS/OT technology with modern IT systems. Facilities are confronted with the fact that traditional IT security technologies are not designed for control systems and cause disruption in ICS/OT environments, and they need direction on prioritizing ICS-specific controls to protect their priority assets.

[6] "Protect Control Systems and Critical Infrastructure with GRID," September 3, 2021, www.sans.org/blog/protect-control-systems-and-critical-infrastructure-with-grid

See Figure 3 for the biggest challenges faced in securing ICS/OT technologies and processes. These are ranked as:

1. Legacy and aging OT technology must be technically integrated with modern IT systems.
2. Traditional IT security technologies are not designed for control systems and cause disruption in OT environments.
3. IT staff does not understand OT operational requirements.
4. There are insufficient labor resources to implement existing security plans.

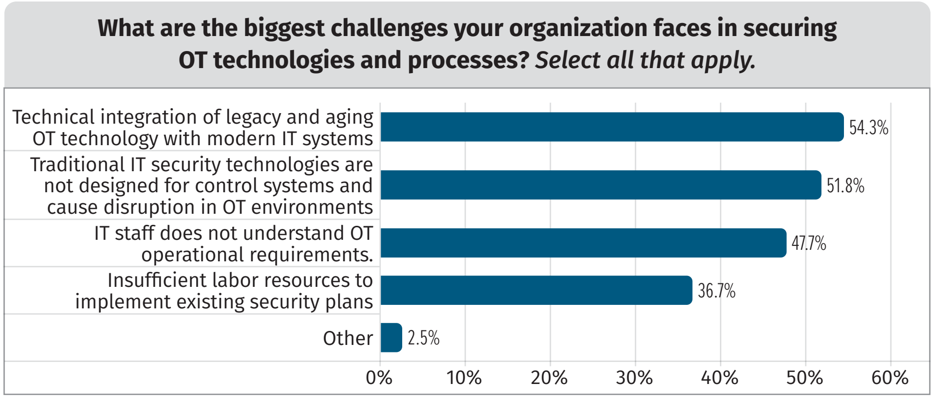


Figure 3. Biggest Challenges in Securing OT Technologies and Processes

We can deal with these challenges with guidance in the people, process, and technology categories as follows:

- **People—**The support for training in the ICS area is clear. Organizations recognize its value and will do well to obtain and retain ICS-specific skilled resources; however, they may need to be flexible in hiring and look harder for the required skillsets.
- **Process—**Security leaders will do well to ensure their teams leverage technology suited for control systems. ICS security managers should continue to strengthen the culture in which safety is the priority—ICS security supports safety—while further educating the business on the differences between IT and ICS/OT. However, as different as the environments are, a converged technical view of security events from both helps to understand, track, and defeat threats to the overall business.
- **Technology—**Integrating newer systems with legacy components presents a challenge that evolving and innovative technologies from ICS vendors can assist with. Facilities are reminded to test solutions and ensure ICS operations and security-specific questions are not only answered, but also demonstrated in a development environment through a proof-of-concept engagement with vendors before technology purchase and deployment.

Aging engineering systems and technology challenges, together with insufficient labor resources to implement existing security plans, make for a challenging ask of ICS security teams. Without a diligent ICS awareness campaign and specific ICS technology and processes deployed, the adversaries will have the upper hand.

ICS Security Is Not a "Copy/Paste" of IT Security

There's a misconception that IT security practices can be directly applied to ICS environments. Although there's a wealth of knowledge 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. Examples include but are not limited to: (1) network and/or endpoint-based intrusion prevention systems could drop legitimate engineering commands that have been flagged as malicious but are false positives. These could be actual legitimate safety or real-time control system commands that are part of a facility's operation, blocked and impending operations, and possible safety protocols. (2) A traditional antivirus system could incorrectly block an engineering application or process from running or executing a part of its operations due to a bad antivirus signature or heuristics-based rule, thus impeding the view, control, or safety of a control system. (3) Vulnerability scanning could be conducted on devices that do not correctly interrupt IT-type scanning software, thus rendering engineering hardware unresponsive and directly impacting the functionality and reliability of control elements, such as an active safety instrumented system.

Analysis of the top three business risks when it comes to the security of control systems is interesting. Year over year there is a downward trend on the importance of ensuring the health and safety of employees, which fell from 2nd (2019) to 7th (2021) and finally to 8th in 2022. This is surprising in a community that has historically placed so much emphasis on human safety and the protection of physical assets in potentially hazardous environments.

This could be due to the community at large now having very high confidence in and coverage of ICS-specific controls in their control systems, and feeling that a compromise cannot have an impact on ensuring the health and safety of employees in plants. Alternatively, safety could be less prioritized now, providing an opportunity to rebuild awareness that cyber incidents in ICS can cause serious, even catastrophic safety impacts to humans and physical assets.

There has been no change in the top two business concerns: (1) ensuring reliability and availability of control systems, and (2) lowering risk/improving security. See Table 1.

Table 1. Top Business Concerns

	2022		2021		2019	
	Percent	Rank	Percent	Rank	Percent	Rank
Ensuring reliability and availability of control systems	53.6%	1	50.3%	1	52.3%	1
Lowering risk/improving security	39.9%	2	45.5%	2	34.8%	3
Preventing damage to systems	30.4%	3	27.2%	3	27.7%	4
Preventing information leakage	29.1%	4	18.1%	6	14.8%	9
Meeting regulatory compliance	22.9%	5	19.8%	5	22.3%	5
Protecting external people and property	21.9%	6	15.2%	8	20.7%	6
Providing or coordinating employee cybersecurity education and awareness programs	17.0%	7	11.2%	11	10.5%	11
Ensuring health and safety of employees	17.0%	8	17.7%	7	42.2%	2
Securing connections to external systems	15.7%	9	23.3%	4	11.7%	10
Creating, documenting, and managing security policies and procedures	13.7%	10	13.1%	9	8.2%	13
Protecting company reputation and brand	13.1%	11	11.6%	10	17.6%	8
Protecting trade secrets and intellectual property	11.1%	12	6.0%	13	7.8%	14
Preventing company financial loss	7.8%	13	7.9%	12	18.8%	7
Minimizing impact on shareholders	6.9%	14	3.3%	14	9.8%	12

There's an opportunity here to recall, leverage, and tie in the strong physical safety culture shared across many engineering sectors to keep employees and people safe, and then to remind ourselves that cybersecurity incidents (targeted or otherwise) can directly impact the safety of people and the environment. Compared to IT security's CIA[7] triad, ICS/OT does not have the same priorities, mission, risk surfaces, or systems; rather, the engineering safety culture, rightfully so, prioritizes safety first, is concerned about control system command integrity, requires availability of engineering systems, and maintains confidentiality internal to the ICS network. ICS/OT cybersecurity supports the safe operation of critical infrastructure, not the other way around. This may vary in some ICS sectors, however; for example, confidentiality can take a higher priority when it comes to intellectual property in pharmaceuticals (e.g., the formulas for medications or vaccines) or competitive product(s) in manufacturing.

[7] "Information Security," https://en.wikipedia.org/wiki/Information_security

Risks to ICS and Our Critical Infrastructure

As ICS security professionals, we do not get to choose whether we are a target or what adversary group(s) target our infrastructure. However, we can select our defense teams, professional training path, security technologies, and processes conducting ICS incident response. Looking at the ICS threat landscape, we are seeing some sectors more targeted than others; for example, this year, business services, healthcare and public health, and commercial facilities are the top three sectors deemed most likely to have a successful ICS compromise that will impact safe and reliable operations. See Figure 4.

Only 11% positively reported that they had experienced an incident impacting their ICS/OT systems. Of these, most reported fewer than 50 incidents. See Figure 5. Yet even with these low numbers, disruptions could be impactful. See Table 2 for the correlation between number of events and percent disruptive.

Based on your understanding of the ICS threat landscape, which sectors are most likely to have a successful ICS compromise with impact to the safe and reliable operation of the process? ***Choose your top three.***

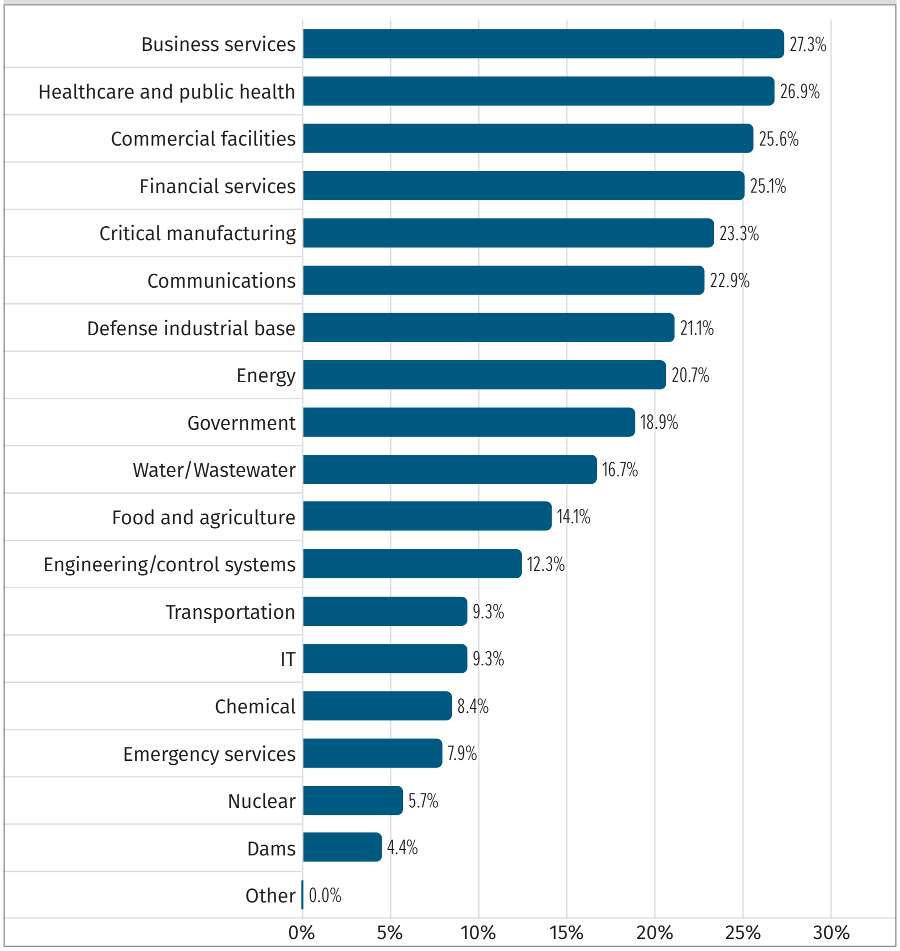


Figure 4. Sectors Most Likely to Be Compromised

How many times did such events occur in the past 12 months?

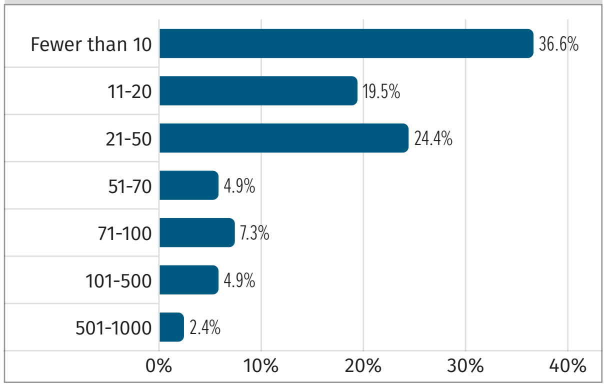


Figure 5. Security Incidents in the Past 12 Months

Table 2. Number of Events vs. Percent Disruptive

		Occurance – Total in 12 Months								
		Total	<10	10–20	21–50	51–70	71–100	101–500	501–1000	>1000
Percent Disruptive | Events	0%	2.3%	2.3%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
	10%	22.7%	18.2%	0.0%	4.5%	0.0%	0.0%	0.0%	0.0%	0.0%
	20%	25.0%	6.8%	9.1%	4.5%	0.0%	4.5%	0.0%	0.0%	0.0%
	30%	22.7%	4.5%	6.8%	4.5%	2.3%	2.3%	0.0%	2.3%	0.0%
	40%	13.6%	2.3%	2.3%	6.8%	2.3%	0.0%	0.0%	0.0%	0.0%
	50%	9.1%	2.3%	0.0%	2.3%	0.0%	0.0%	2.3%	2.3%	0.0%
	60%	2.3%	0.0%	0.0%	0.0%	0.0%	2.3%	0.0%	0.0%	0.0%
	70%	2.3%	0.0%	0.0%	0.0%	2.3%	0.0%	0.0%	0.0%	0.0%
	80%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
	90%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
	100%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
		100.0%	36.4%	18.2%	22.7%	6.8%	9.1%	2.3%	4.5%	0.0%

When asked which control system components were considered at greatest risk for compromise, the top component—the engineering workstation or instrumentation laptop—remains the same as last year, at nearly 54%. See Figure 6. This year, however, servers running commercial operating systems dropped to the third spot while operator assets such as a human machine interface (HMI) or operator workstation took over the second spot at 43%, a notable jump from 32% the prior year. This could be attributed to the increased reporting from ICS threat intelligence showing how ICS adversaries now more than ever are "living off the land" in the control environments.

It is surprising the plant historian is ranked second to last at 4%, given threat intelligence has illustrated data historians could be targeted for sensitive data exfiltration, are among the top five critical assets to protect,[8] and are used by adversaries as pivot points from an IT compromise into the ICS networks.

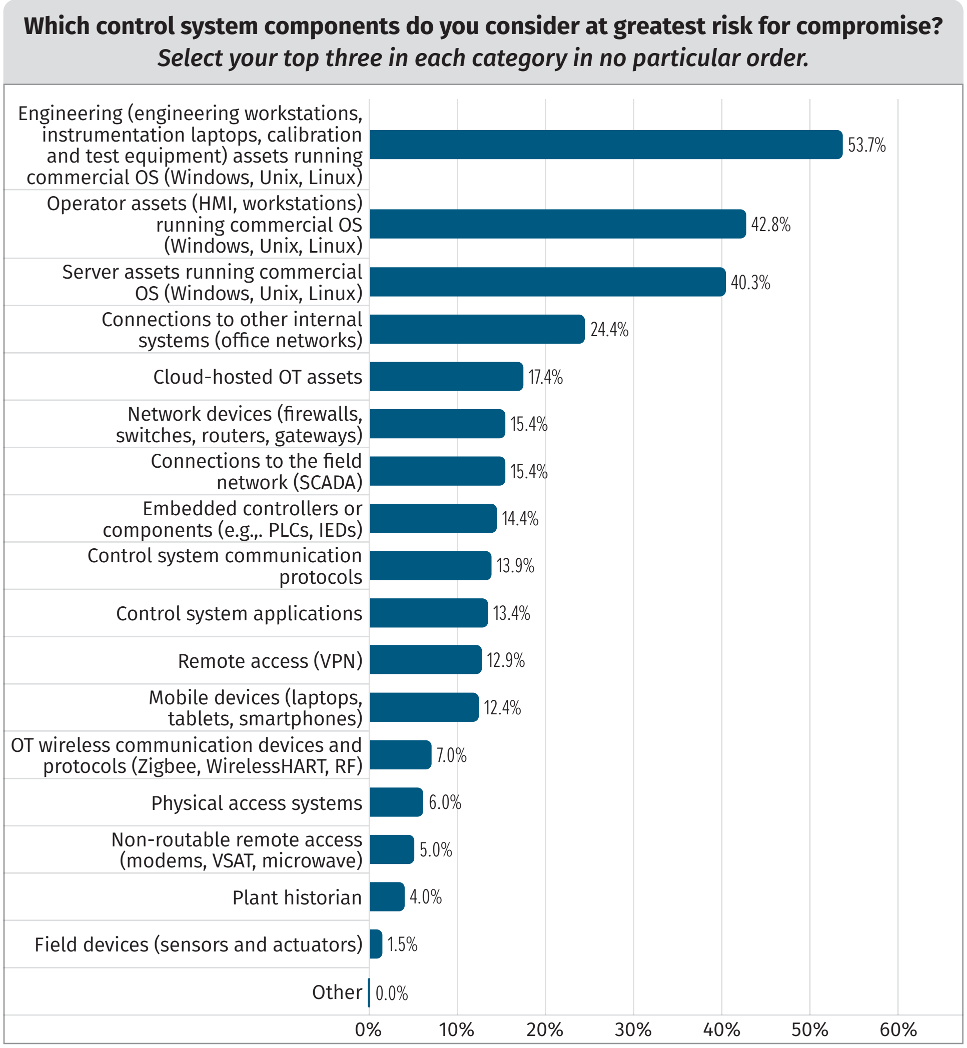

Which control system components do you consider at greatest risk for compromise?
Select your top three in each category in no particular order.

Figure 6. Components at Greatest Risk for Compromise

ICS attack groups have been observed "living off the land"; that is, abusing systems, features, and industry protocols native to industrial environments, turning control systems against themselves. Some examples of living off the land are an attacker gaining access to an HMI with legitimate operator access but then using the HMI commands against the process to, for example, open circuit breakers in the field in an electric substation or change the chemical mixture in a water treatment facility. No malware is used to cause the impact; rather, the adversaries are using built-in and legitimate engineering software, features, and/or ICS protocols to cause impacts. Living off the land can be seen as far back as HAVEX[9] in 2014, more recently with the tailored CRASHOVERRIDE[10] ICS-specific framework targeting electric power, and the 2022 discovery of the Incontroller/PIPEDREAM[11] scalable ICS attack framework.

[8] "Top 5 ICS Assets and How to Protect Them," www.sans.org/webcasts/top-5-ics-assets-and-how-to-protect-them

[9] "ICS Alert (ICS-ALERT-14-176-02A), ICS Focused Malware (Update A)," https://us-cert.cisa.gov/ics/alerts/ICS-ALERT-14-176-02A

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

[11] "Alert (AA22-103A), APT Cyber Tools Targeting ICS/SCADA Devices," www.cisa.gov/uscert/ncas/alerts/aa22-103a

When changing the question to ask which ICS components are considered to have the greatest impact to the business if compromised or exploited, we see some alignment with the prior question. However, we must not forget to protect programmable logic controllers (PLCs), IEDs, and other embedded components (20%) from impacts through the manipulation of controller logic, unauthorized engineering configuration changes, or an unauthorized industrial control system network-based device (15%). See Figure 7.

Engineering systems, although not equipped for traditional anti-malware agents, can be protected through network-based ICS-aware detection systems and industrial-based network architecture practices. Additionally, as part of on-going engineering maintenance tasks for field devices, log capture or log forwarding and regular controller configuration verification are achievable ways to start protecting these critical assets.

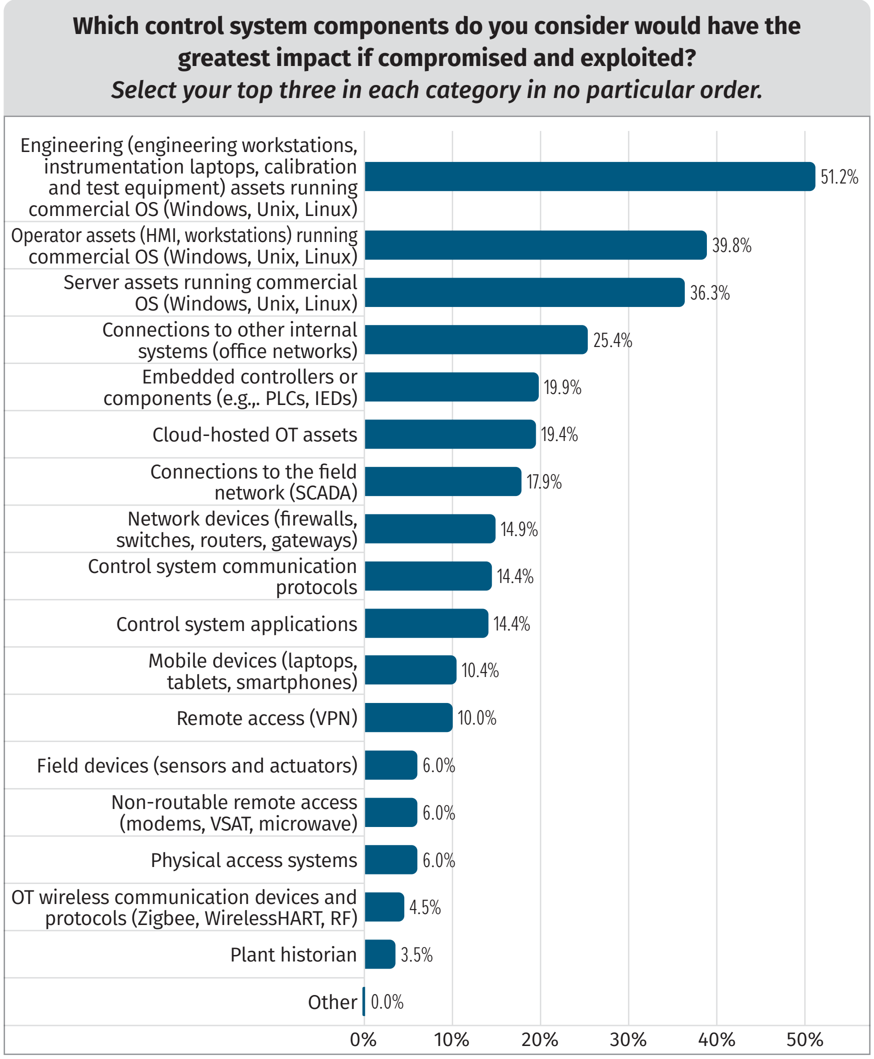

Which control system components do you consider would have the greatest impact if compromised and exploited? ***Select your top three in each category in no particular order.***

Figure 7. Components with the Greatest Impact If Compromised

ICS Vulnerability Management and Patching

Once safety risks and operational impacts from a cyberattack are seen, it's too late. So, looking for threats and vulnerabilities proactively is the most effective approach to defense and operational resilience. Most respondents (60%) use passive monitoring, with a network sniffer being the primary method (and arguably the safest approach) for vulnerability detection in hardware and software. See Figure 8. The second most common method is continual active vulnerability scanning. It is still important to note, active vulnerability scanning can be risky for legacy or other devices unable to properly interpret aggressive or unexpected network scan traffic. However, vendors have caught on to using safer methods, like active querying using native ICS protocols, to obtain asset and vulnerability data. Ranking third is comparing configuration and control logic programs against known-good logic versions.

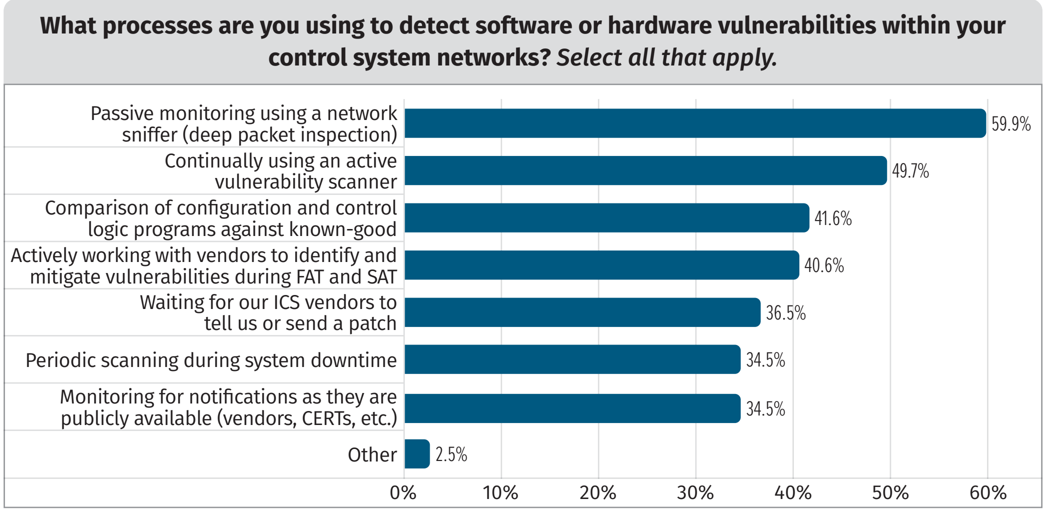

What processes are you using to detect software or hardware vulnerabilities within your control system networks? ***Select all that apply.***

Figure 8. Processes for Detecting Vulnerabilities

Organizations used to spend more time monitoring for vulnerability notifications disclosed by vendors, computer emergency readiness teams (CERTs), and the like as a method of vulnerability discovery. This approach was ranked number one (61%) in 2021; however, in 2022 this method tied for second to last (35%).

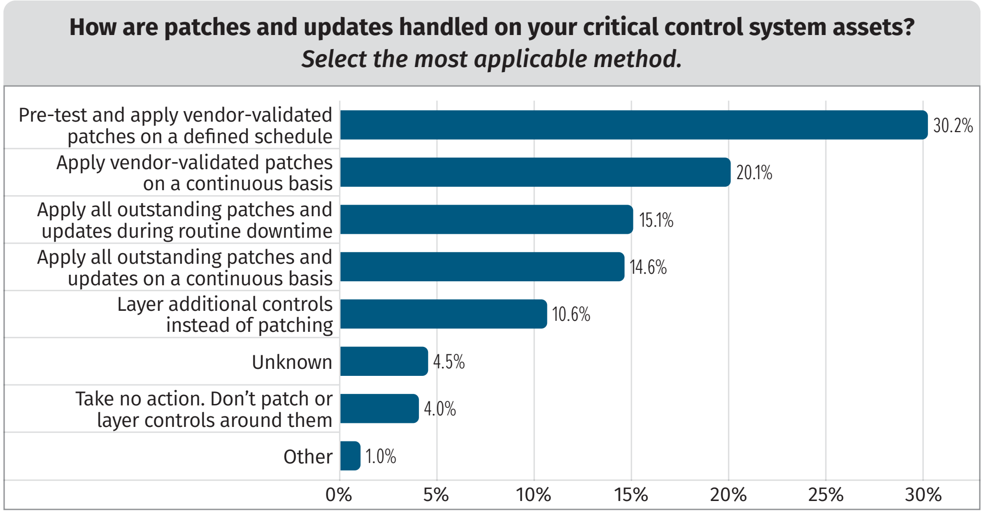


Figure 9. Handling of Patches and Updates

Also important to note is that the number of respondents choosing to apply all outstanding patches and updates during routine downtime doubled in the past 12 months. This could be because organizations are electing to try to reduce the risk of patches causing unintended impacts during production. See Figure 9.

To reduce many vulnerabilities in the first place, however, there is good return on investment in managing them during the factory acceptance testing (FAT) and site acceptance testing (SAT) phases before full production deployments. Some respondents have benefited from this, because its use has increased slightly in 2022 to 41%, up from 40% in 2021 (see Figure 8). Managing ICS vulnerabilities in FAT and SAT, however, does not replace the requirement for vulnerability management in ICS in a regular, on-going cadence.

Patching is not just about reducing security vulnerabilities. Many vendors release non-security patches to fix bugs, furthering the stability of equipment, or to add new operational features. Once security vulnerabilities are detected, facilities have several options for handling them. Many facilities (30%) are handling patches by pretesting and deploying vendor-validated patches on a defined schedule. This is a reasonable goal that lagging facilities can set on their ICS security roadmap as a next step. Only 4% of facilities are taking no action on patching; in contrast, a great goal would be to align with the 15% of respondents that are applying all outstanding patches and updates on a continuous basis.

The Oldsmar[12] event draws attention to the importance of understanding risk surfaces, vulnerability management, and secure remote access that requires multifactor authentication (MFA) for external-facing and internet-connected devices. Common open source intelligence (OSINT) exercises tailored for ICS systems can be used to uncover vulnerable or weakly secured systems directly connected to the internet and prioritize them for protection and vulnerability remediation.[13] Vulnerability management could be prioritized by patching devices directly connected to the internet first, followed by edge network firewalls and switches, remote access solutions, data historians, ICS internal core network infrastructure, critical engineering assets such as the HMIs, engineering workstations, and so on.

[12] "Alert (AA21-042A), Compromise of U.S. Water Treatment Facility," www.cisa.gov/uscert/ncas/alerts/aa21-042a

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

ICS vulnerability mitigation can be prioritized by having an asset inventory combined with ICS threat intelligence to understand the ICS risk surface, and knowing the placement of assets in the control networks—how those assets could be accessed for possible exploitation and protecting critical assets first.

When asked who performed the most recent ICS security assessment, the most common were OT security consultants, at 27%. This was up slightly from last year's 25% and just ahead of internal IT team(s), followed by internal OT team(s). A separation may be emerging in which internal IT teams are less likely to be called on for ICS security assessments; however, it is too early to say whether it is a lasting trend at this time. Critical infrastructure owners and operations may wish to consider Critical Infrastructure Vulnerability Assessments offered by CISA.[14]

Implementing ICS Security Controls

Responsibility for implementing ICS security controls has shifted this year, with the majority of organizations claiming the responsibility belongs to the owner or operator of the ICS (38%) or the engineering manager (36%). See Figure 10.

In 2021, this responsibility was most often assigned to the IT manager role, which fell to third in 2022. This shift in responsible parties appears to align with those working day to day more directly focused on engineering operations and safety.

Although there are some security practices and principles applicable to both environments, organizations are realizing the enterprise IT and ICS/OT environments are not the same. They not only have different types of systems, but also have technologies that are not directly cross-compatible, the missions and risk surfaces differ—even initial attack vectors, impacts, and approaches to incident response are different.

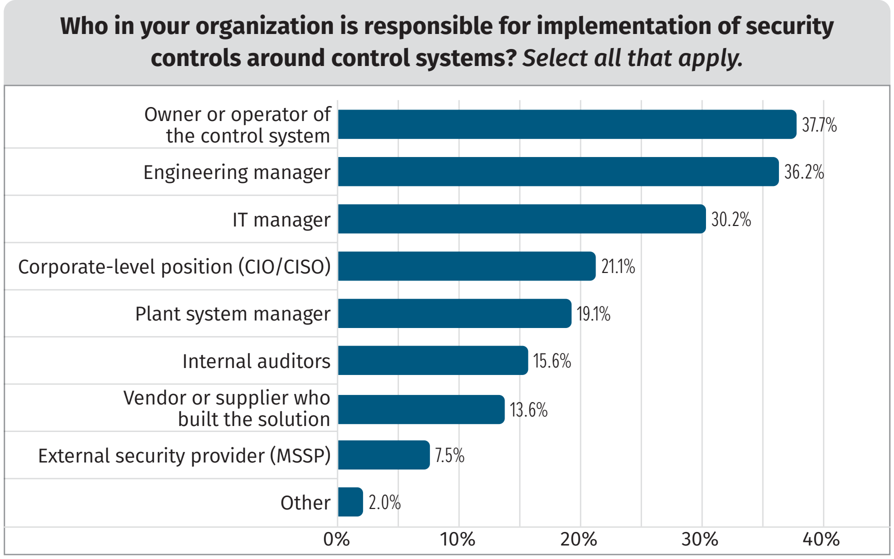


Figure 10. Position Responsible for Security Control Implementation

[14] CISA, "Critical Infrastructure Vulnerability Assessments," www.cisa.gov/critical-infrastructure-vulnerability-assessments

ICS Incident Response: Identified Gaps and Impacts

We asked who would be contacted when there are signs of an infection or infiltration of the control system cyber assets or network. The leading resource remains a cybersecurity solution provider, reaching 57% in 2022, up from 48% in 2021. This is followed with a tie between control system vendor and engineering consultant at 35%, showing a continued upward trend for engineering consultant across 2019 (13%), 2021 (19%), and 2022 (35%). See Table 3.

A reliance on external cybersecurity solution providers for ICS does not mean a fully outsourced ICS cyber defense team; rather, it could mean an augmentation of internal resources with the use of external incident response retainers to close resource gaps as the ICS security teams are spinning up or starting to mature.

In 2021, 40% of survey participants indicated they leveraged IT consultancy to support their ICS incident response efforts; in 2022 we see a positive and significant drop to 13%. This downward trend is a benefit because ICS-aware resources are being called in for ICS incident response vs. observed suboptimal response efforts from IT-only experts.

Internal resources fall to fourth position at 32% compared to its second position in 2021 at 44%. Overall, this shift indicates an increased reliance on external, yet ICS-specific resources, and a sharp decline in the reliance on specific IT consultancy for ICS incident response efforts. Facilities appear to be requiring resources specifically trained and experienced in ICS incident response to work in ICS environments.

Table 3. Who Is Contacted

	2022	2021	2019
Cybersecurity solution provider	56.5%	48.1%	35.6%
Control system vendor	34.8%	32.7%	45.6%
Engineering consultant	34.8%	19.2%	13.4%
Internal resources	32.6%	44.2%	59.0%
Non-regulatory government organizations (e.g., CISA, FBI, National Guard, state or local law enforcement)	23.9%	32.7%	40.6%
System integrator	19.6%	11.5%	15.1%
Security consultant	17.4%	32.7%	37.2%
IT consultant	13.0%	40.4%	18.4%
Main automation contractor	8.7%	11.5%	8.4%
Other	0.0%	3.8%	2.1%

Incident impacts in IT and ICS are different. Incidents 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 death. The Department of Homeland Security makes an accurate statement: “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.”[15]

When selecting and verifying incident response partners for ICS, it is vital to understand the team’s ICS-specific skillsets and prior experience (anonymized case history) specifically in response to incidents in control system environments.

[15] “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

Initial Attack Vectors

When sharing data on the initial attack vectors involved in control system incidents, survey participants cite a compromise in IT allowing threats into the ICS/OT control networks as the highest-ranking threat vector. Interestingly, only 4% chose wireless compromise. See Figure 11.

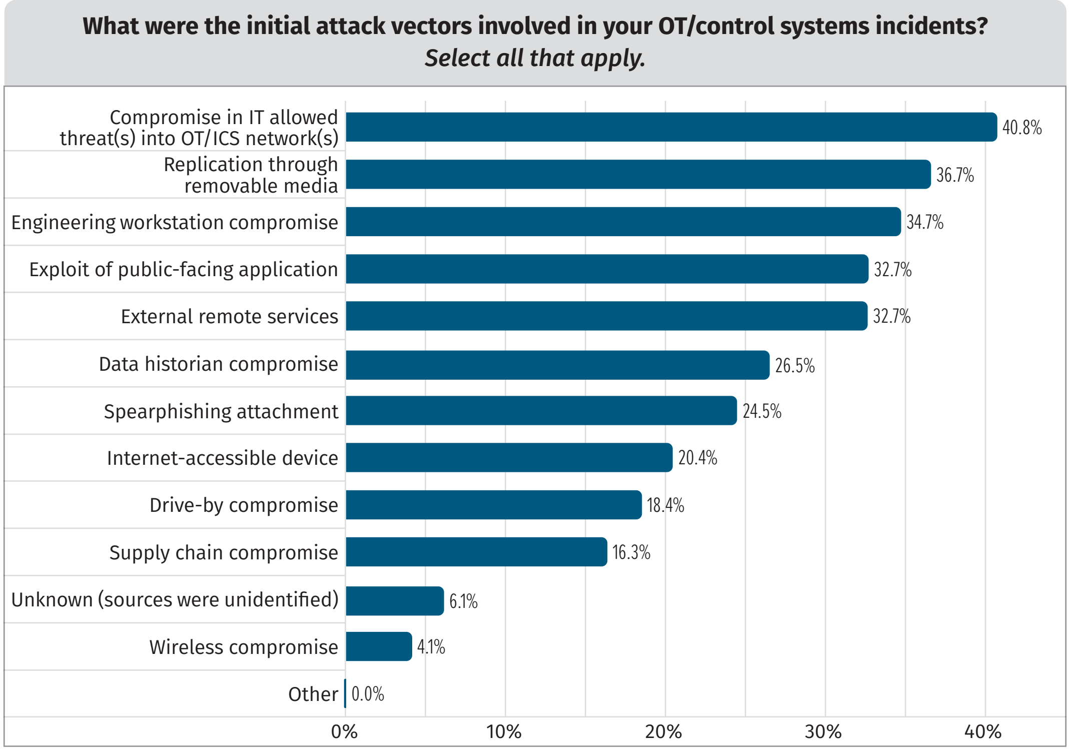


Figure 11. Initial Attack Vectors

This highlights data historians or other trusted and targeted devices with connectivity to both IT and ICS/OT as being a likely target. For example, data historians targeted for possible process data exfiltration could also be leveraged as a pivot point from an IT compromise into the control network(s).

Risk of threats through removable media (USBs, external hard drives, etc.) is a close second. It is worth noting that 83% of respondents have a formal policy in place to manage transient device risks such as removable media devices, and 76% have a threat detection technology in place to manage transient assets. Seventy percent are using commercial threat detection tools, 49% are using homemade solutions, and 23% have deployed ad-hoc threat detection to manage this risk.

Engineering workstations have control system software that is used to program or change logic controllers and other field device settings or configurations. This critical asset could also be a mobile laptop—essentially a transient device—used for engineering device maintenance that could travel throughout facility sites or elsewhere outside the protection of a segmented plant network.

The IT business network remains a common initial intrusion point for adversaries as a possible Stage 1 attack, helping adversaries prepare for a potential pivot into the ICS environment for an ICS Cyber Kill Chain[16] Stage 2 attack with direct impact on engineering operations. Those wishing to fortify network architecture to segment and protect the ICS network(s) from external networks, such as IT networks and the internet, can leverage guidance from the ICS410 SCADA Reference Model[17] on network architecture and ICS asset placement.

The MITRE ATT&CK ICS framework has recently been updated to include methods to mitigate risk in this area tracked as Transient Cyber Asset (T0864)[18] and Replication Through Removable Media (T0847).[19]

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

[17] "ICS410 SCADA Reference Model," www.sans.org/posters/control-systems-are-a-target

[18] "Transient Cyber Asset," https://attack.mitre.org/techniques/T0864

[19] "Replication Through Removable Media," https://attack.mitre.org/techniques/T0847

Top Vectors, Top Threat Concerns

When inquiring about the top threat vectors of concern to respondents, with the influx of ransomware seen globally, it is no surprise that ransomware, extortion, or other financially motivated crimes rank as number one (40%). See Figure 12.

Even ransomware impacting IT business networks may have an impact on ICS operations. This would depend on the location of ICS support services and network architecture, such as dependencies on the enterprise resource planning (ERP) system and manufacturing execution system (MES) for ICS being located on IT networks, and similar takeaways from the Colonial Pipeline[20] ransomware event. Detection and neutralization of ransomware is more complicated when ransomware is tailored to industrial control systems, as seen with the Ekans/Snake[21] ransomware. Organizations can consider ICS-specific endpoint detection and response (EDR) technologies on traditional operating systems in Purdue Level 3 and the ICS DMZ as a control against ransomware that may propagate from IT into ICS/OT networks.

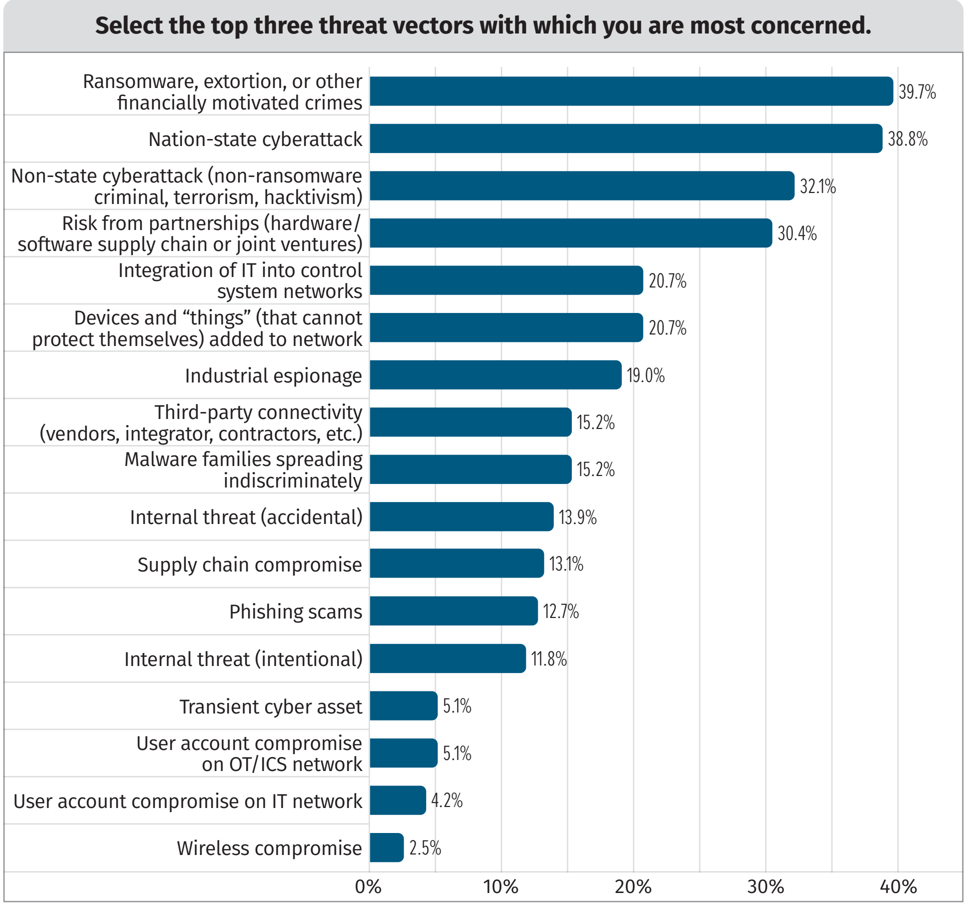

Select the top three threat vectors with which you are most concerned.

Figure 12. Top Threat Vectors

Organizations must still test and verify their backup and recovery strategies on a regular cadence. This needs to include not only traditional operating systems in the ICS network, but also engineering systems—specifically, the recovery of controller configuration and logic code, protection control relays, remote terminal units, and process configurations to ensure engineering process recovery meets the facility's mean time to repair (MTTR) objectives.

Several ICS facilities fell victim to the Ekans ICS-tailored ransomware, including Honda[22] and multinational energy company Enel Group,[23] where the adversary group demanded $14 million in ransom for the decryption key and to prevent the attackers from release terabytes of stolen data.

[20] "Ransoming Critical Infrastructure: Emergency Webcast Transcript," www.sans.org/blog/ransoming-critical-infrastructure-emergency-webcast-transcript

[21] "Ekans/Snake: NJCCIC Threat Profile," www.cyber.nj.gov/threat-center/threat-profiles/ransomware-variants/ekans-snake

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

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

ROI on ICS Asset Inventory

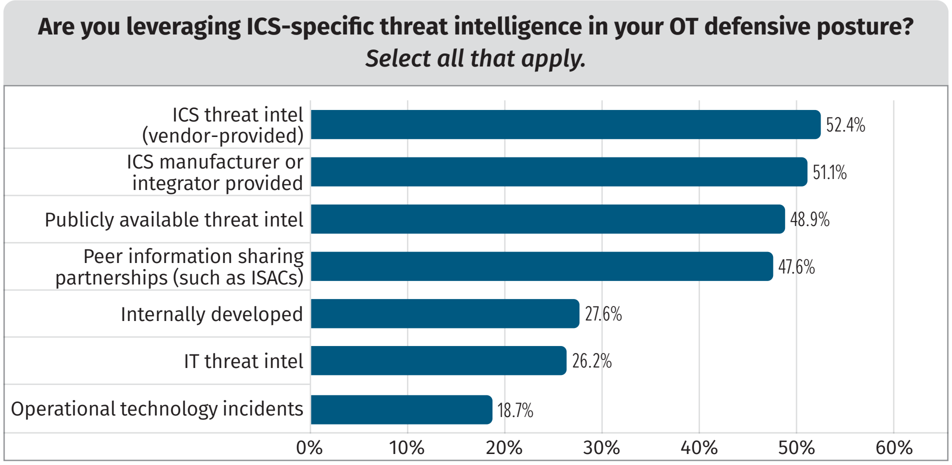
A formal ICS asset inventory of engineering devices is a prerequisite for the maturity of an ICS security program in any sector, and facilities are realizing the benefits. We cannot protect what we do not know we have.

Slightly more than 70% of respondents shared they have a formal process to inventory ICS/OT assets, a 13% jump from 2021. There is still value to be gained, however, for the 23% of facilities that do not yet have a formal process and the 6% of organizations that are unsure or unaware of an existing formal process in this area.

Facilities can expand an existing engineering asset inventory or build one by using any one of or a combination of the four main methodologies for ICS asset identification. One approach is to prioritize physical inspection combined with passive traffic analysis. Details on the basic attributes to capture and an example approach are available online,[24] starting with commonly targeted devices: data historians, human machine interfaces, programmable logic controllers (PLCs), engineering workstations, core network devices, and active safety instrumented systems (SIS).

ICS Threat Intelligence

The ICS threat intelligence market has come a long way in 12 months. More facilities are using vendor-provided threat intelligence for more immediate and actionable defense steps. Unlike most respondents in 2021, respondents in 2022 are no longer just relying on publicly available threat intel. Rather, they are now primarily benefiting from vendor-provided ICS-specific threat intelligence, and secondarily are looking to ICS manufacturers or integrators. This shows less of a reliance on peer information sharing partnerships (e.g., information sharing and analysis centers [ISACs]) and IT threat intel. This is a sign of increased maturity and awareness of the value of ICS-vendor-specific threat intelligence, as well as budget allocation for improved proactive defense in this area. See Figure 13.



Are you leveraging ICS-specific threat intelligence in your OT defensive posture?
Select all that apply.

Figure 13. ICS-Specific Threat Intelligence

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

It's commonplace and valuable to leverage indicators of compromise (IoCs) for technical reactive defense, such as scoping for attacker artifacts in an environment to determine if and where a compromise may be during an incident. Those looking to mature ICS security programs can focus more on threat intelligence tactics, techniques, and procedures (TTP); that is, implementing proactive security changes based on observed adversary tradecraft. This lends itself to longer-lasting proactive defense measures because it makes it harder for the adversary to thrive in the environment.

Facilities leveraging the MITRE ATT&CK framework for ICS can understand and track their detection, mitigation, and security event log data source coverage against sector-specific attacker techniques and tactics observed in previous attacks. The framework can be used to find gaps, tune deployed technologies, and evaluate new vendor solutions and their alignment to the framework in these areas. In fact, to facilitate this, many technology vendors are building MITRE ATT&CK for ICS dashboards directly into their products. We are seeing an increasing number of organizations do exactly this—2022 results show that 78% of respondent organizations have completed a MITRE assessment.

Although the adoption rate to complete assessments has increased in the last 12 months, it reveals that work is still needed to action identified gaps. For example, an area to improve is initial access, to help prevent adversaries from gaining a foothold in the network in the first place. Only 20% of organizations have 51–75% coverage for this tactic, and only 4% have full coverage for it. See Figure 14.

ICS managers will do well to support their tactical teams in leveraging MITRE ATT&CK for ICS to track metrics and show maturity across their detection, mitigation, and security event log data source coverage of their deployed technologies. As ICS cybersecurity programs mature with the use of MITRE ATT&CK for ICS and close identified gaps, more advanced defense through ICS threat hunts[25] will provide much more ROI.

> **Publicly available threat intelligence could come at low or no cost and is a great place to start consuming threat intelligence. Commercial ICS/OT intel services excel in providing improved relevance and timeliness for proactive defense steps against emerging threats and could be more sector specific in some cases.**

If you have completed an assessment of your MITRE ATT&CK® ICS technique coverage in your ICS, what coverage do you have in each of these areas?

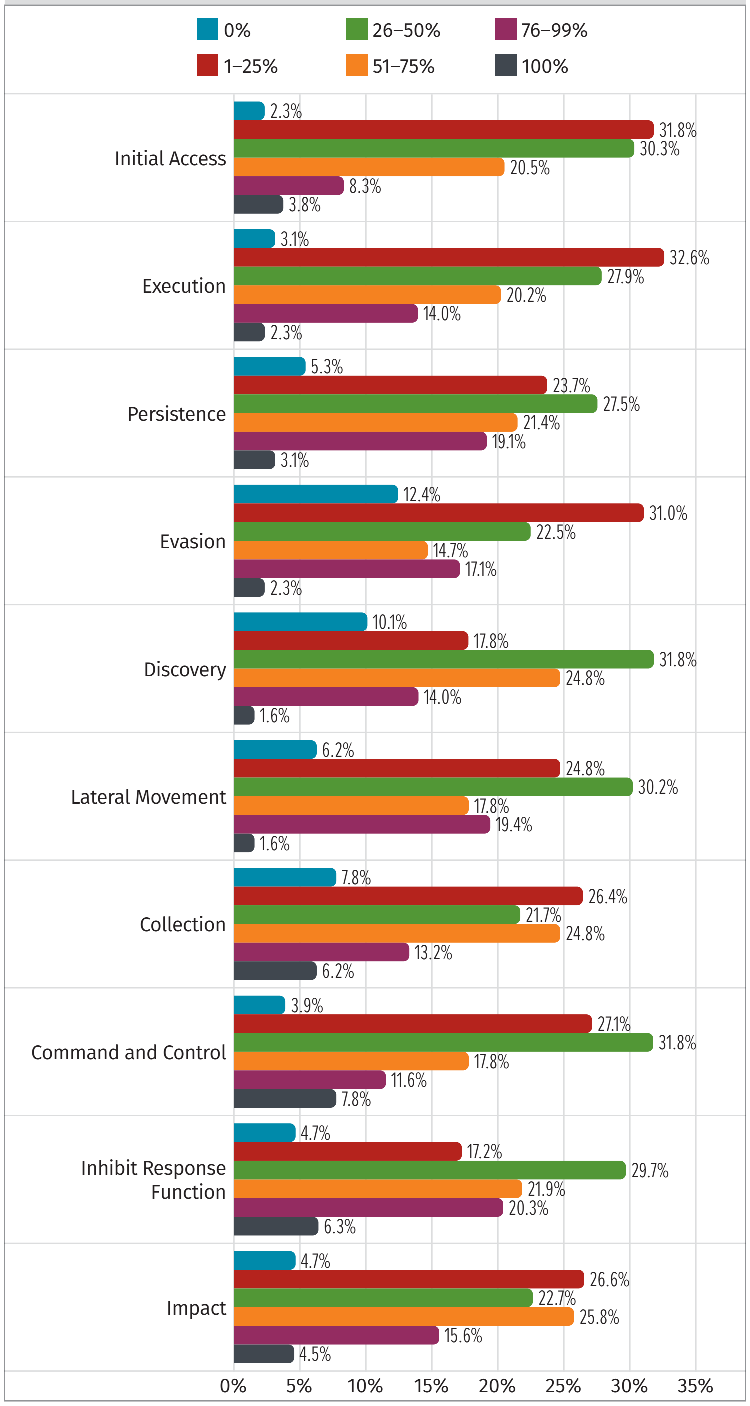


Figure 14. MITRE ATT&CK Area Coverage

[25] "ICS Threat Hunting: 'They're Shootin' at the Lights!'—Part 1," www.sans.org/blog/ics-threat-hunting-they-are-shootin-at-the-lights-part-1

Tomorrow's Defense, Implemented Today

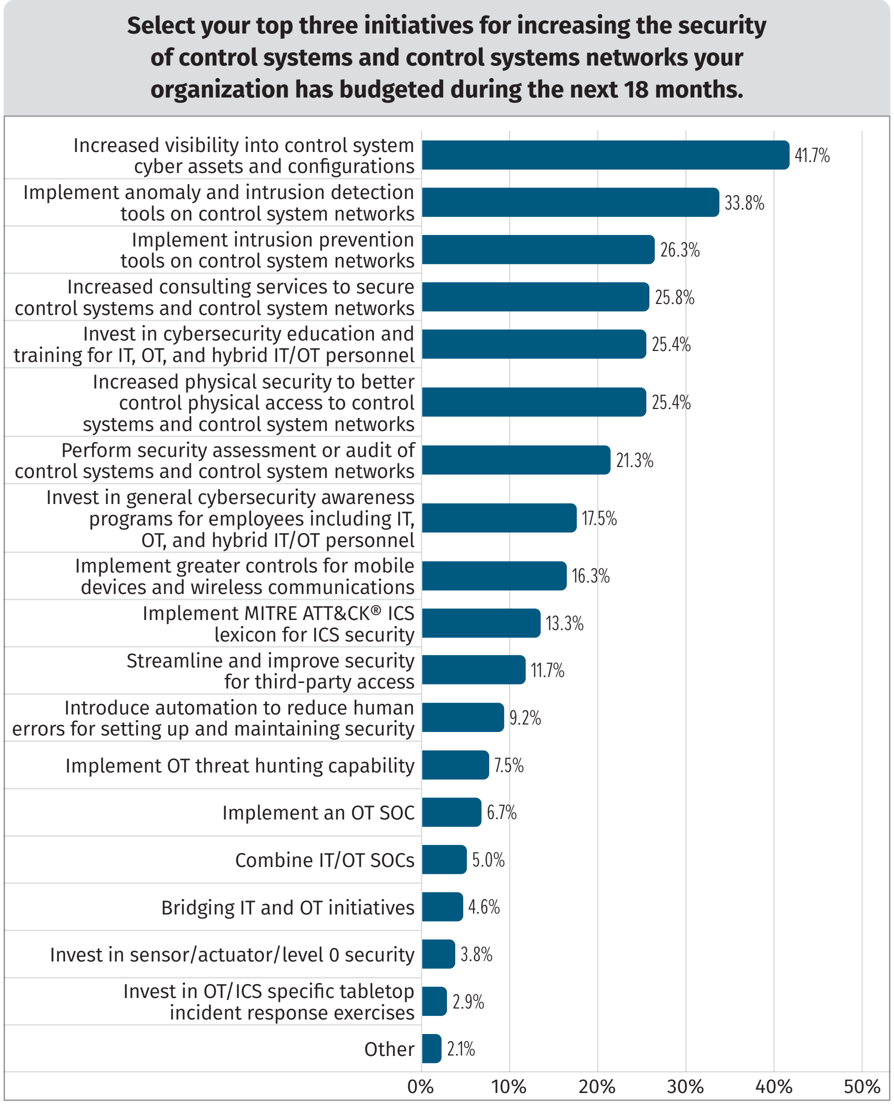
Dedicated resources for people and tools will drive the ICS security program to meet our modern challenges. Only asset owners who continue to invest in control system security can hope to mature, detect, protect, and defend it. Positively, year over year, more organizations are obtaining an ICS security budget, with 2022 seeing only 8% of facilities without one. Most organizations now have budgets allocated between $100,000 and $499,999 USD (27%) or between $500,000 and $999,999 USD (25%). This is positive yet not a massive allocation, so decisions will need to be made wisely. See Table 4.

Table 4. ICS Security Budget

	2022	2021	% Change
We don't have one.	7.7%	23.7%	-16.0% ▼
Less than $100,000 USD	10.2%	19.1%	-8.9% ▼
$100,000 to $499,999 USD	27.0%	24.2%	2.8% ▲
$500,000 to $999,999 USD	25.0%	10.8%	14.2% ▲
$1 million to $2.49 million USD	15.3%	10.8%	4.5% ▲
$2.5 million to $9.99 million USD	7.7%	5.2%	2.5% ▲
Greater than $10 million USD	7.1%	6.2%	0.9% 🟨

Looking to the next 18 months, respondents are allocating those budgets toward several initiatives; planning for increased visibility into cyber assets and their configurations (42%) and the implementation of network-based anomaly and intrusion detection tools (34%) showed the highest focus. Closely behind there's a focus on network-based intrusion prevention tools on control-system networks (26%) followed by increased consulting services. See Figure 15.

Intrusion *prevention* systems could wrongly stop critical control system software or network commands and disrupt operations. For this reason, facilities are strongly encouraged to prioritize intrusion *detection* systems. This is especially important when first deploying network-based detection and response technologies that could remain safely in detection-only mode.



Select your top three initiatives for increasing the security of control systems and control systems networks your organization has budgeted during the next 18 months.

Figure 15. Top Initiatives for Increasing Security

Both ICS endpoint and network visibility are critical for any ICS defense program, for all ICS sectors. We think this is recognized in the community and expect to see a continued investment here in the short term with long-term benefits. ICS network visibility is especially important in the case of adversaries "living off the land" because it's possible endpoint security agents would not detect the abuse of legitimate control system functions or network protocols being abused. Additionally, attacks destined for endpoints must traverse the network first. Network devices and network detection systems are more difficult to compromise than endpoint applications and could have more capabilities for active incident response. Generally, the network is first to see most attacks and prepositioning attack setups.

Conclusion

Adversaries targeting ICS/OT in critical infrastructure have illustrated knowledge of engineering components, industrial protocols, and engineering operations. This reflects in their impactful attacks, targeted ransomware, and a new scalable ICS tailored attack framework[26] that could be leveraged to inflict disruptive, possibly destructive, safety impacts, human injury, and/or death.

Defense efforts are gradually becoming stronger. Together, asset owners and vendors are stepping up to meet new challenges and serious impactful threats the community is facing. The adversaries have clearly upped their game, and it only makes sense that we must up our defenses and staff skillsets to meet the evolving threat. Asset owners have made great strides and several changes with significant focus on ICS operational improvements. Vendors are improving their approach for specific ICS needs; they know it's not the same as IT because ICS/OT has different missions and asset types, and they know technologies for one must be adapted to suit the other.

The ICS security workforce is becoming more skilled and valued. Workers coming into or already in place in ICS security are further seeking and obtaining control system security training and certifications. It may be difficult to find and attract people in this space, so facilities may need to be flexible to ensure they get the right people with the right skills to train and retain them.

The shift in who has responsibility for implementing ICS security controls, and those who are called on for ICS incident response cases, shows a trust level with engineering and ICS trained staff over IT-only skilled experts. The clear improvements in training staff, leveraging sector-specific threat intelligence, and alignment with standard frameworks for assessments like MITRE ATT&CK for ICS are encouraging and can lead to more threat hunting. There is, however, a growing concern that organizations may be holding safety as less important. This may or may not be caused by a lack of awareness or the business not fully embracing the differences between IT's and ICS/OT's missions, risk surfaces, technologies for defense, and finally impacts.

[26] "Alert (AA22-103A), APT Cyber Tools Targeting ICS/SCADA Devices," www.cisa.gov/uscert/ncas/alerts/aa22-103a

Clear defense improvements are seen in investments such as asset inventorying, network detection systems, and arming staff with specific ICS security knowledge. Further progress in key areas is still needed. Those responsible for ICS/OT security at facilities would do well to consider these top takeaways to kick-start or mature their ICS cybersecurity program:

- **Obtain, train, and retain a skilled ICS security workforce.** Without obtaining and retaining skilled resources, we cannot expect to be able to act on existing security plans, let alone keep ahead of evolving threats against our critical infrastructure.
- **Further educate the organization to embrace ICS/OT and IT differences.** Understand and embrace the differences between IT and ICS/OT by prioritizing the safety of human life and the reliability of operations as the mission. ICS/OT cybersecurity will support safety and reliability, not the other way around. Leverage what makes sense from IT security while realizing it is never a "copy and paste" from IT security into a control system environment. Adapt processes and methodologies, ensuring security solutions are tailored and specific to suit the unique objectives and mission of ICS.
- **Enable ICS active defense.** Establish a solid foundation first. Align the ICS network architecture with the Purdue model and prepare for the active defense position on the Sliding Scale of Cyber Security.[27]
- **Augment the network with endpoint solutions.** Both endpoint security solutions tailored for traditional operating systems and ICS-aware network solutions are important. Consider augmenting one with the other, as long as it fits the ICS requirements and is ICS-capable.
- **Use ICS asset discovery, inventory, and management.** This is a prerequisite for effective cybersecurity that enables active cyber defense cycle (ACDC) and streamlines threat and risk analysis by quickly understanding a facility's risk surface on engineering and OT systems. The four main methodologies of creating an ICS asset discovery and inventory can be combined for increased accuracy.

We must remain focused and diligent; circle back to ensure strong ICS-specific controls and processes are established; and prepare for the long haul. Remember, ICS defense is totally doable, and ICS/OT security and risk management is a marathon, not a sprint.

[27] "The Sliding Scale of Cyber Security," www.sans.org/white-papers/36240

Sponsor

SANS would like to thank this paper's sponsor:

NOZOMI
NETWORKS