Industrial Control System Cyber Incident Response

This poster offers guidance on preparing for and performing cyber Incident Response (IR) for Industrial Control System (ICS) environments. For the most effective industrial IR and established industrial NSM (Network Security Monitoring) program an updated ICS Asset Inventory is best. See related ICS NSM Poster to assist with this control system network security monitoring and proactive defense.

DIFFERENCES BETWEEN IT SECURITY AND ICS SECURITY

Industrial engineering control system assets are often compared to traditional information technology (IT) assets. However, traditional IT assets focus on digital data at rest or data in transit. Operating technology industrial control systems (OT/ICS) manage, monitor, and control real-time engineering systems for physical input values and control output for physical actions in the real world. This is the primary difference between IT and OT/ICS systems, which have differing requirements, skills needed, and processes, including cyber incident response:

UNIQUE CONSIDERATIONS FOR ICS INCIDENT RESPONSE

Unique Systems—Nontraditional computer systems with industrial and proprietary protocols.

Reliance on external vendor support—Engineering systems with external engineering team support that may require special secure remote access.

Legacy Systems—Devices that may not be suitable for patching or firmware updates, or that are only available for patching or firmware updates to internal operating systems at infrequent times.

Non-traditional operating systems—Purpose-built embedded and/or proprietary operating systems that are common in control environments where many traditional security defenses are not effective or applicable.

Safety of people—The main goal for control systems is not confidentiality, integrity, or availability, but rather safety, then integrity to trust operations, and availability.

Protection of physical assets—Control systems that use physical components to change the physical world. Impacts such as a cyber attack could result in physical damage, safety implications, and environmental impacts.

CRITICAL ICS ASSETS

Industrial incident response should deploy proactive monitoring, baseline traffic and system activity, and prioritize data acquisition from the critical assets in the environment. Critical industrial assets can be targeted with malware, and human adversaries can cause negative impacts on the process by directly interacting with the control environment using legitimate operational software with malicious intent. Several critical ICS assets are outlined below. At a minimum, access control, network traffic, and system changes should be regularly monitored, starting with these assets.

Data Historian—A database that stores operational process records. It can be abused to act as a pivot point from a compromised asset in IT to an asset in the ICS network.

Engineering Workstation—A workstation that has software to program and change a Programmable Logic Controller and other field device settings/configurations.

Human Machine Interface—A visual interface between the physical process and operators that is used to monitor, control, and change most any part of the industrial process.

Programmable Logic Controllers—PLCs connect the physical hardware, run logic code to read the state or to change the state or a process, and interface with devices that make physical changes in the real world.

INDUSTRIAL INCIDENT RESPONSE – GETTING STARTED

ICS asset inventory and control system network security monitoring are critical for effective industrial incident response.

ICS Asset Inventory—An established ICS asset inventory of operational technology devices and engineering assets will improve ICS Incident Response scenarios. Common methodologies to establish the inventory, physical inspection, passive traffic analysis, configuration file analysis, active scanning, can be combined for improved accuracy. For example, physical inspection takes advantage of face-to-face security awareness and educational discussions on-site with engineering and operational teams. Augmented with passive network captures, it can create and verify an inventory and provide network traffic to sift through for threat detection.

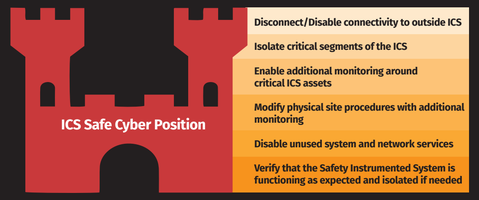
ICS Network Security Monitoring—Network Security Monitoring is a human-driven, proactive, and repeatable process of collection, detection, and analysis. While not specific to ICS, NSM excels in control system networks because the environment is usually more static and has fewer users than in traditional information technology (IT) environments. NSM is most effective with an established ICS asset inventory to assist with an active approach control system thread detection and drives industrial incident response to reduce impacts to operations, and safety of people, the environment and engineering assets.

ICS Incident Response—NSM will lead to ICS Incident Response. An effective ICS IR Plan will incorporate safety decisions at each step, has outlined communications plans, a designated war room, out of band communication, a contact list of key personnel—safety and engineering teams etc. Traditional IR steps need to be adapted to consider safety impacts at each step in industrial environments:

1. Preparation (test jump bag in ICS dev.)
2. Establish a Safe and Defensible Cyber Position
3. Integrated Identification & Detection
4. Quick Triage on ICS impacts, safety
5. Safe Containment—maintain operations
6. Safe Eradication, Recovery
7. Lessons Learned

ICS SAFE CYBER POSITION

Once triage of the cyber situation deems it necessary, a facility can decide to enter a safe and defensible cyber position. This would be determined by the level of risk deemed as acceptable by the facility owners, with input from ICS security, engineering, safety, and other teams. The ICS Safe Cyber Position should be tested as part of the preparation phase of the ICS Incident Response Plan. It will enable more in-depth threat containment and aid the eradication and recovery phases when it is safe to do so.



INDUSTRIAL CYBER INCIDENT RESPONSE TRIAGE

Successful ICS incident response requires a clear understanding of roles, responsibilities, physical safety, the engineering process, network visibility, industrial protocols, and forensics capabilities. It also requires having a defensible cyber position. Traditional incident response steps can be adapted to suit industrial control environments by considering and acquiring:

- System memory from top critical ICS assets
- Engineering field device (local) log events
- Engineering field device configuration and logic (compare logic file hashes to baseline)
- Engineering workstation field device programming software usage
- Engineering workstation removable media connections
- Operator workstations, HMI application, and system access logs
- Operator workstations and HMI remote access events
- Removable media connections for operator workstations
- Remote access logs—VPN, Jumpbox, Access Control Lists across trusted zones on Firewalls, etc.

ICS INCIDENT RESPONSE ROLES

Conduct specific ICS tabletop scenarios with key teams to reinforce safety, roles, and responsibilities. Effective industrial incident response teams have technical IT and ICS cybersecurity, engineering, overall facility, and safety backgrounds.

Incident Response Director—Interfaces with executive leadership team on the status of an incident, resources, impacts, and options to maintain operations and safety.

Lead Responder—Guides incident response personnel and quick triage/impact timeline analysis, and advises the Incident Response Director on available actions to reduce the impact on safety and operations.

Incident Handlers—Cybersecurity and ICS field and technical personnel who may be required to make environment and asset changes. These personnel handle evidence acquisition, scope threats and infections, and undertake analyses, among other tasks.

Fire & Security, Safety and Law Enforcement – Teams prepared for physical first aid, emergency response, evacuation strategies for physical site safety, and efforts beyond the site.

INDUSTRIAL CYBER INCIDENT RESPONSE PROCESS

In industrial environments, safety to people, the environment and to the engineering assets is goal #1.

Preparation & Planning—Expanding on traditional IT incident response, it will be critical to ensure that site safety teams are involved in cyber incident response planning. External organizations such as ICS peers, government agencies, Information Sharing and Analysis Centers (ISACs), and Computer Emergency Response Teams (CERTs) will also need to be part of the overall plan. Tools for those teams in the control system are to be tested in development environments at this stage.

Integrated Detection and Identification—Incident response teams will work with other ICS security and engineering personnel on network security monitoring. Threat identification can be conducted based on consuming and applying threat intelligence to find and identify threats and impacts to systems and components for operations.

Evidence Acquisition—Teams will use already-tested and deployed or available tools to quickly acquire meaningful forensics data from critical ICS assets to help determine threats.

Time Critical Analysis—Analysis will be performed to determine impacts based on the threat(s) analyzed and provide options to stakeholders on ways to contain and preserve the safety of operations.

Containment Considering Safety—Ensuring safety will be prioritized and considered at each step of containment or change in the industrial environment, operational technology. or engineering systems.

Eradication, Recovery Considering Safety—This will involve removing threats such as malware, adversary remote access, etc. in order to reestablish a safe and trusted industrial process. This could require rebuilding the operating system, reloading industrial software, uploading controller logic, etc.

Lessons Learned—This will involve applying knowledge, technology, personnel resourcing, and process gaps to the ICS or IT/OT converged Cyber Incident Response Plan.

Information Sharing—Sharing key takeaways from incidents with the ICS community and peers in the sector will help maintain the safety and reliability of operations in facilities across other sectors globally. Key information would be in the form of adversary attack tactics, techniques and procedures observed, indicators of compromise of a specific attack, and the campaign of malware capability used.

ICS INCIDENT RESPONSE PLAN

The convergence of information technology (IT) and operational technology (OT) can enable effective management of control systems. Convergence can improve uptimes, performance, quality and productivity, and access to business data about the process to identify efficiencies—all of which leads to increased profits for those who adopt these solutions.

While IT/OT convergence of both technology and workforce development perspectives poses unique challenges, it can also enable and drive a more realistic view of cyber threat detection and incident response that could further protect the industrial process.

A converged incident response plan will consider available cybersecurity defenses in both environments and work to reduce the impact of attacks through IT into ICS, rendering a more realistic view for detection and response. This can provide early warning signs of an attack that could impact or specifically target the industrial process.

The converged plan must prioritize safety, and defenders should understand security processes and technologies in order to detect where an adversary is in an ICS attack. ICS incident response plans are most effective when exercised on a frequent basic, such as annually, through such initiatives as tabletop exercises.

SANS ICS CURRICULUM

ICS310: ICS Cybersecurity Foundations™

ICS410: ICS/SCADA Security Essentials™
Global Industrial Cyber Security Professional (GICSP)

ICS418: ICS Security Essentials for Leaders™

ICS456: Essentials for NERC Critical Infrastructure Protection™
GIAC Critical Infrastructure Protection (GCIP)

ICS515: ICS Visibility, Detection, and Response™
GIAC Response and Industrial Defense (GRID)

ICS612: ICS Cybersecurity In-Depth™

ICS613: ICS/OT Penetration Testing & Assessments™

SANS ICS CURRICULUM

- sans.org/ics
- ics-community.sans.org/signup
- @SANSICS
- Free and open-source tools for ICS are available at **ControlThings.io**

WHERE IS THE ADVERSARY IN THE ATTACK

After reviewing detection data from NSM and gaining an initial understanding of the malicious actions, incident response steps will be determined by where the adversary or threat is, what the impact has been already, and what the potential impact is moving forward for control system operations and safety. An essential question is: "How far along is the adversary in the attack?"

Is the adversary stealing sensitive data to build a harmful industrial attack?

Is the adversary attempting to move laterally towards the control environment?

Is the adversary attempting to elevate permissions to maintain a foothold in the control environment?

Is the adversary attempting to enumerate and map out the control network?

Is the adversary attempting to communicate with field devices to disable safety protections or affect quality assurance?

Is the adversary attempting to disrupt, manipulate, or damage physical assets or cause harm to people or the environment?

Has the adversary established a C2 and is the adversary enumerating the control network, laterally moving in the environment, attempting to access a Human Machine Interface, or accessing PLCs or other field devices on programming service ports?

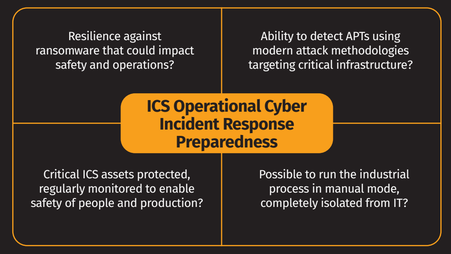
WHEN TO INITIATIVE ICS INCIDENT RESPONSE

Analysis drawing on ICS NSM will contribute to escalating the factors that will ultimately determine when industrial incident response steps are to be invoked. Use the questions listed above to help determine the potential risk that an intrusion will disrupt the industrial process or safety, and to understand the progression of an attack already in progress. Answers to these questions will help drive defense steps and shift to potential incident response steps.

ICS INCIDENT RESPONSE TABLETOPS

An incident response tabletop is a paper-based exercise that facilitates security discussions across several teams and focuses on existing preparedness. A tabletop exercise can help verify deployed security technologies, controls, event monitoring, and security processes to help identify areas for improvement. Beyond traditional IT incident response tabletops, industrial tabletops must consider additional teams, controls, and environments built for industrial operations, which have a different mission than IT.

Regularly conducted incident response tabletop exercises as part of a mature ICS Security Program serve to identify weak points in security efforts and enable proactive defense to address the range of threats.



ICS incident response tabletops are much like the pre-game practice drills that sports teams run before a game. Like pre-game drills, ICS incident response scenarios are designed to test all that will be needed once the game begins. In this case, however, the game is the serious business of cybersecurity, and it requires ICS defense capabilities, safety processes, and cyber preparedness. These proactive exercises test the effectiveness of an ICS Security Program prior to an attack. Tabletops are conducted in roundtable discussions guided by an Incident Response Plan, knowledge of the engineering processes, and an understanding of the existing ICS security defenses. Weak points are identified and assigned to be addressed immediately to strengthen the program. ICS incident response tabletops provide a high return on investment in several important areas:

Validation—Tabletop exercises validate readiness by comparing optimal defense controls against existing controls. Areas in need of improvement are identified in industrial incident response plans and security and safety playbooks. Simultaneously, tabletops help train both new and established team members about the industrial process and ICS-specific security.

Situational Awareness and Team Building—Reviewing threat intelligence with the teams involved educates them about adversary capabilities and attack techniques. Regularly performing tabletops establishes and strengthens cross-departmental relationships needed for incident response events that could span multiple industrial sites across large geographic regions.

Practical Defense Actions—Tabletop exercises can identify gaps in such critical areas as threat detection, data source collection, log correlation, network segmentation changes, access control updates, security and safety process changes, and the communication of roles and responsibilities. Effectiveness in all these areas is key for a mature program. The results of tabletop exercises will directly improve overall response time, reduce impacts on the engineering process, and increase safety.

INDUSTRIAL IR TABLETOPS KICK-START GUIDE

1. Select one of the presented realistic ICS Incident Response Tabletop Scenarios for the organization's next ICS IR exercise.
2. Mature the process by creating specific scenarios based on the organizations' ICS threat landscape by leveraging ICS threat intelligence, internal or external gap assessments, compliance reports, etc.
3. Custom scenarios should consider cyber to physical safety risks at every step and include the operational top critical ICS assets.
4. Involve as many teams as practical, including Safety, Process Controls Engineering, Operators, ICS Network Architects, ICS Security, Plant Management, etc.
5. Discuss, learn, act, and repeat. "ICS Defense Is Doable!"

ICS INCIDENT RESPONSE JUMPBAG

The objective in industrial environments during a cyber incident is to maintain safety and operations. Use these tools for quick analysis and triage to understand the threat(s), operational impacts, and present options to facility owners to minimize loss and ensure safety. Store Jump Bag (ideally rolling protective cases) at critical site(s) or deploy them with the IR team as they conduct IR.

- Data acquisition tools (prioritize memory)
- Laptops with Security Onion, REMnux, SIFT
- Baseline images of critical ICS assets
- Hashes of field device logic/configuration files
- Log, packet analysis, and timeline tools
- Approved digital camera (no photo metadata)
- Hardcopy ICS incident response playbooks, network diagrams
- Site physical safety training certificates
- Network/converter cables (USB <-> Serial)
- Contact list for safety, engineering, integrators, security, emergency response team
- Out-of-band communications, handheld radios on site
- Forensically clean USBs, external drives
- CD-ROM drives and discs
- Personal protective equipment (PPE) for safety
- Malware analysis tools (static, automated)

ICS INCIDENT RESPONSE MUST-HAVES

1. ICS-Specific Incident Response Plan
Execute realistic tabletop exercises driven by sector-specific threat intelligence or gaps identified in your facility.

2. ICS-Specific Network Security Monitoring
Ensure "plant floor" network visibility with ICS deep-packet inspection to drive incident response or proactive threat hunting. Network visibility capabilities should go beyond just querying about indicators of compromise and include capabilities to assist with analyzing threat tradecraft.

3. Trained ICS-Specific Security Defenders
Trained ICS cybersecurity personnel who understand the nuances between traditional IT and ICS security, the ICS mission, safety, the engineering process, and ICS protocols and active defense procedures.

ICS INCIDENT RESPONSE IN PRACTICE

Successful ICS incident response requires a clear understanding of roles, responsibilities, physical safety, the engineering protocols and process, network visibility, detection, and forensics capabilities. Facilities benefit when having a tested safe defensible cyber position. Consider adapting traditional IR steps to suit industrial control environments:

- Acquire forensics data from key ICS assets
- Quickly triage to understand the threat via static or automated malware analysis
- Execute the Safe Cyber Position
- Contain threats while running operations
- Eradicate when its safe for operations
- Analyze the impact of any reliance on external vendors and IT
- Apply lessons learned to the ICS Incident Response Plan
- Regularly conduct ICS incident response tabletop exercises
- Examine the connectivity and isolation of legacy devices
- Determine operational impacts
- Develop countermeasures
- Use indicator "hits" to scope infection
- Compare production and baselined configs to detect tampering in controllers etc.
- Present analysis and options (blocking C2 access, running ICS in manual mode, removing remote access, etc.) to fight through the attack (contain/eradicate)
- Identify and apply lessons learned (e.g., correct gaps in evidence acquisition, deploy additional ICS network visibility, detection capabilities, determine whether threats are malware or human adversaries).

Malicious code, unauthorized access detected → Exfiltration of sensitive industrial system information → Loss of visibility of control process → Loss of process controls → Manipulation of control system operations → Physical damage to assets or safety concerns

Malicious code, unauthorized access detected

Installation or execution of malicious software. An example would be an adversary gaining physical or logical access to a network, system, or data without authorization, or introducing a cyber containment that could impact process control views or controls.

Exfiltration of sensitive industrial system information

An incident exfiltrating sensitive control system information that could be used to do harm. An example would be the identification of ICS field device ladder logic, control system configuration, or historian database entries being copied off a network. This is an indication of a follow-on (non-immediate but potentially imminent) targeted ICS attack.

Loss of visibility of control process

A cyber incident affecting the ability to view the state of the physical process. An example would be a power generating facility not being able to view the current system load or the current power grid operating frequency to maintain 60Hz.

Loss of process controls

A cyber incident affecting the ability to change the state of the physical process. An example would be an oil refinery not being able to safely shut down its crude oil distillation process or maintain pressure in a pipeline.

Manipulation of control system operations

The abuse of internal native system components or protocols such as Human Machine Interface (HMI) commands, and ICS protocols such as EthernetIP, ModbusTCP, DNP3, 61850, OPC, etc. An example would be the use of DNP3 to send unauthenticated "open breaker" commands to remote terminal unit field devices to open electric circuit breakers to cut power.

Physical damage to assets or safety concerns

An incident affecting the physical properties or integrity of physical assets, or introducing a potential physical safety impact to plant operators, workers, and/or on-site visitors, contractors, etc.

PERFORMING INDUSTRIAL INCIDENT RESPONSE TABLETOPS

Planning—Planning time will vary depending on team size, the scenario, resources, and other factors, but it typically can take anywhere from a few days up to a month. Even a planning phase of just 2 to 5 days is enough to provide value in the outcome. Spend time up front properly selecting realistic scenarios for your environment and selecting the right teams. Include as many team players and observers as is practical.

ICS teams—Include all teams that are practical to involve. Invite observers to listen to the discussions for training purposes. Start with the following:

- **Safety—**Include the on-site safety and emergency response team.
- **Physical security—**Include the on-site facility physical security team.
- **Compliance—**Ensure that legal and regulatory compliance requirements are met.
- **Cybersecurity—**Since cybersecurity drives the scenario, participants must understand the defenses and the Incident Response Plan, the technologies and the industrial operations process, protocols, critical assets, the network layout, etc.
- **Engineering—**Include process control and field device technicians.
- **Operators—**These are the persons who control the process via remote and embedded HMIs, etc.
- **Management—**Management and director-level stakeholders for all teams involved need to have an awareness and understanding of ICS cybersecurity risk, impacts, protections, budget, resourcing, etc.

TOP 3 ICS TABLETOP EXERCISES

Regular Incident Response (IR) tabletop exercises are part of a mature ICS Security Program and works to identify strong and weak points in ICS defense efforts. The scenarios designed to test ICS defense capabilities and cyber preparedness are critical. Here are ICS IR Tabletops for consideration.

SCENARIO #1: Human Machine Interface Hi-Jack—On-screen Suspected Activity.

Human Machine Interface Operators notice the on-screen mouse moving and clicking on different control buttons on the HMI, which is not consistent with normal operations or a scheduled change or safety emergency.

Discussion—Which accounts, and individuals have access to HMIs for local or remote access?

Teams—Engineering, operators, ICS security, network architects

Protection—Purdue Network Architecture, process control, operators having a process for reporting cyber events

Detection—Secure remote access event monitoring—external->internal, internal->Internal—RDP, multi-factor authentication, use of a jump box in ICS DMZ (Purdue Level 3, etc.)

Response—Disable remote access, run ICS on plant floor via embedded HMIs, investigate NSM network traffic patterns, enable islanding from Internet, IT, etc.

SCENARIO #2: Physical Access to Cyber Access Event

The Physical Security team notices a hole cut into the physical security perimeter – the fence surrounding a remote facility. The Physical Security team investigates and determines the physical attack could be a two-part attack. Physical access was gained, then attackers pivoted to a cyber-attack as a containment was introduced into the control network at remote site. Traditional break-ins have been observed to be for monetary value, such as copper theft in Electric utilities. Some critical remote ICS sites could be vulnerable to physical and a physical-cyber-attack. This also presents a safety concern for workers in remote facilities such as electric substations, switching yards, oil and gas valve stations, fuel storage facilities such as marine terminals, etc.

Discussion—Physical security at remote sites could be the most vulnerable ICS facilities (substations, oil/gas storage facilities, valve stations, etc.)

Teams—Physical security teams, engineering, cybersecurity, safety

Protection—Security guards stationed at site(s) or security checks on rotation

Detection—Physical door alarms, surveillance cameras, rotating security guards, etc.

Response—Roll trucks to site, law enforcement

Safety—A concern for adversaries in dangerous life-threatening situations and workers on-site in the event of a break-in

SCENARIO #3: Ransomware on IT or ICS/OT networks

ICS Operator Workstations in a control center(s) are infected with Ransomware and are inoperable to view or control the industrial process. Alternatively, the IT business network is inoperable due to a ransomware infection in the enterprise—critical ICS process application such as industrial billing, shipping logistics applications are inoperable.

DISCUSSION: Does ICS rely on IT, and to what extent? Is it possible to island ICS from IT in a safe cyber defensive position?

TEAMS: IT, IT security, ICS security, engineering, operators, safety

PROTECTION: Email security (if IT is infected with the common email phishing vector), whitelisting on ICS endpoints, IT - ICS Network Segmentation (Purdue Network Architecture)

DETECTION: ICS-specific endpoint protection, ICS NSM (lateral movement)

RESPONSE: Is it possible or feasible to run the ICS process in manual mode from embedded HMIs on the plant floor in the event the primary HMIs are inoperable due to Ransomware or another threat? It may be possible to respond by cutting or limiting network segment communication for containment while fighting through the attack.

Remember, ICS Defense Is Doable!

SANS ICS RESOURCES sans.org/ics · ics-community.sans.org/signup · @SANSICS · **ControlThings.io –** Free and open-source tools for ICS

ICSPS_ICSCIR_0525
This poster was created by Dean C. Parsons.