WATER ISAC

# 12 Cybersecurity Fundamentals for Water and Wastewater Utilities

## Recommended Practices to Reduce Exploitable Weaknesses and Consequences of Attacks

MARCH 2024

**Fundamental 1 | Plan for Incidents, Emergencies, and Disasters**
**Fundamental 2 | Minimize Control System Exposure**
**Fundamental 3 | Create a Cyber Secure Culture and Protect from Insider Risks**

waterisac.org/fundamentals

# PREFACE

The last iteration of the *fundamentals* was published just under five years ago in 2019 and WaterISAC is excited to bring this refresh to our members and the larger water and wastewater systems sector.

- At that time, we went from 10 to 15.
- This time, we've condensed down to 12.

**Why the change?** A desire to make it a little more manageable, but still touch on key fundamentals that water and wastewater utilities should consider addressing.

**What changed to get us from 15 to 12?** A few things were combined, most notably:

- *Tackle Insider Threats* section was appropriately merged with building a cyber secure culture (this quarters' release).
- *Address All Smart Devices (IIoT, IoT, Mobile, etc.)* was consolidated with the fundamental on asset management (which will be released next quarter in June 2024).
- Among other things, given AWIA requirements it was decided that Assess Risks (risk assessments) is an "assumption" and as such there will be a discussion in the introduction.

**What other changes?** In an attempt to keep the fundamentals practical, especially for smaller systems to address, the refreshed fundamentals will be released in small manageable chunks - three per quarter (in March, June, September, and December).

- **Note:** the current 2019 version of WaterISAC's *15 Cybersecurity Fundamentals for Water and Wastewater Utilities* will remain on the website until the end of the year, so there will be a full set available until all 12 refreshed ones have been released.

**What's new?** While reviewing the 15 Fundamentals, we quickly realized that much of the information was still relevant and applicable and didn't see any reason to reinvent the wheel. However, there's been a lot of newly published guidance lately and updated information and resources over the past 5 years and we wanted to incorporate some of that into this document – kind of "mappings" to the relevant resources as appropriate.

- **One of the most significant updates to this version is extensive incorporation throughout each section of CISA's Cross-Sector Cybersecurity Performance Goals (CPGs)[1] and references to The Five ICS Cybersecurity Critical Controls.**[2]
- A "Why this is important" message.
- Also, in most of the *fundamentals* we've incorporated Small Systems Guidance.
- We've added a lot of visual elements. Everyone loves eye candy! Instead of just a bunch of words, we've added visual elements to emphasize the more practical/notable applications, information, resources, etc. Specifically, we've either added new or pulled out existing info that could be best described as:

  1. Practical Application
  2. For Consideration
  3. Risk Scenario
  4. Bonus Material
  5. *Additional Resources, Examples, How to get started, and more…*

Thank you for accessing WaterISAC's ***12 Cybersecurity Fundamentals for Water and Wastewater Utilities*** and we hope you appreciate the thoughtful updates. Please let us know what you think!

The WaterISAC Team

1 **https://www.cisa.gov/cross-sector-cybersecurity-performance-goals**
2 **https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/**

# 1 Plan for Incidents, Emergencies, and Disasters

**WHY THIS IS IMPORTANT: The inability to promptly and efficiently contain, mitigate, and communicate about cybersecurity incidents, emergencies, or disasters could result in significant operational disruption. Effective response plans will limit damage, reduce recovery time and costs, and increase confidence of partners and customers.**

It might be surprising to find response planning at the beginning of a recommended practices guide. *The Five ICS Cybersecurity Critical Controls*[1] makes a solid case for prioritizing incident response planning, especially an **ICS-specific Incident Response Plan** over other fundamentals, practices, or controls. As response plans are developed, utilities may find the planning activity extremely useful for identifying significant cybersecurity and continuity of operations gaps, and informing subsequent best practices for implementation.

### Practical Application

Effectively responding to a cyber incident or attack requires things like logging to be in-place and properly configured. The lack of sufficient log data hinders incident response efforts by reducing visibility and delaying incident identification. Cyber Incident Response Plan (CIRP) development would help identify if logs are available and effectively configured.

### Five ICS Cybersecurity Critical Controls | Control No. 1: ICS-specific Incident Response Plan

- Organizations must have an ICS-specific incident response plan to account for the complexities and operational necessities of responding in operational environments. **A common mistake for organizations is thinking about incident response as a final element in its security program.**

### RESOURCE | Dragos OT-CERT Host-Based Logging Guidance

Members of Dragos OT-CERT have access to *Host-Based Logging Guidance: Instructions for Managing Windows Event Logs*. In addition, OT-CERT has jump start videos which provide demonstrations of every-thing covered in the guide.

### BONUS MATERIAL | Mandiant DFIR Framework for Embedded Systems

Collecting and analyzing forensic data is a core component of the incident response process. This process is central to determining the existence, and subsequent scope of a compromise, the tools used by adversaries, and their capabilities. However, obtaining digital forensics and incident response (DFIR) data is not always a simple task, especially when operational technology (OT) systems are involved. Mandiant's DFIR Framework for Embedded Systems is comprised of three steps focused on preparation and gathering information from embedded devices during the early stages of the incident response process.

Developing plans for how a utility will respond to incidents, emergencies, and disasters is critical for recovering from such events quickly. IT and OT teams should be concerned primarily with cyber incident response plans and disaster recovery plans. These are just two elements of, or adjuncts to, overall business continuity or continuity-of-operations plans.

1 https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

These plans should not be developed by a single department, but rather in collaboration with teams across all departments. Including external stakeholders such as emergency response and law enforcement authorities in the development of the plans can also be valuable. This holistic inclusion will ensure a cooperative and unified response that leverages all organizational resources for more accurate plans.

### CPG | 2.S Incident Response (IR) Plans

Organizations have, maintain, update, and regularly drill IT and OT cybersecurity incident response plans for both common and organization-specific (e.g., by sector, locality) threat scenarios and TTPs.

- When conducted, tests or drills are as realistic as feasible.
- IR plans are drilled at least annually and are updated within a risk-informed time frame following the lessons learned portion of any exercise or drill.

### CPG | 5.A Incident Planning and Preparedness

- Develop, maintain, and execute plans to recover and restore to service business or mission-critical assets or systems that might be impacted by a cybersecurity incident.

In January 2024, CISA, EPA, and FBI, as well as the federal government and WWS Sector partners created an Incident Response Guide (IRG) for Water and Wastewater Sector.[2] The unique value of this IRG is that it provides water and wastewater sector owners and operators information about the federal roles, resources, and responsibilities for each stage of the cyber incident response lifecycle. Sector owners and operators can use this information to augment their respective IR plans and procedures.

### RESOURCE | Incident Response RACI Matrix

Red Canary has developed a fully customizable Incident Response RACI matrix[3] to help visualize and manage the delegation of responsibilities as they relate to significant incidents. This matrix is also a useful tool for understanding incident response in the context of business, while pinpointing areas for improvement.

## Cyber Incident Response Plan

Despite established safeguards, many organizations still experience cybersecurity compromises. Indeed, experts note experiencing a compromise is not a matter of if, but when. However, organizations that fare best will be those that are able to quickly detect the intrusion (Fundamental 4)[4] and have a defined plan in place to respond. An effective CIRP will limit damage, increase confidence of partners and customers, and reduce recovery time and costs. Furthermore, the incident response plan needs to be in place before an incident occurs and should be incorporated into organizational business continuity plans.

### For Consideration

The value of CIRPs is priceless. However, Talos Intelligence outlines seven common mistakes[5] that organizations make when creating or updating an incident response plan. Avoiding some of these pitfalls ensures your utility's plan will be updated faster and is more thorough, so you are ready to act when, not if, an incident happens.


2 https://www.cisa.gov/sites/default/files/2024-01/WWS-Sector_Incident-Response-Guide.pdf
3 https://redcanary.com/blog/incident-response-and-readiness-guide/
4 Fundamental 4 | Implement Threat Detection and Monitoring will be released in June 2024
5 https://blog.talosintelligence.com/seven-common-mistakes-companies-make-when-creating-an-incident-response-plan-and-how-to-avoid-them/

Two recommendations to include in the CIRP are:

- emergency operating procedures for industrial process operation – at least as appendices or in references. It's important to plan in advance for how water operations staff will maintain system operations during an incident, with potentially degraded capability.
- pre-planned steps for common or high impact incident scenarios, such as a ransomware infection, compromise of remote access, or a loss of a critical function. (In other words, according to the *Five ICS Cybersecurity Critical Controls,* these intelligence-driven, common, or high-impact scenarios should be prioritized because the likelihood of them being repeatable is high. Additionally, they are real-world scenarios that have already happened, and because there are a small enough number, they can serve as especially useful focus areas.)

Proactively considering the details of maintaining operations during these incidents in advance will also result in improved response effectiveness, and likely reduce impacts and time to recover.

### Cyber Incident Response Team

For enhanced response capability in the event of a cybersecurity incident, organizations should consider forming a cyber incident response team to develop and manage the incident response process. The security operations center is responsible for day-to-day investigations, but a separate team should be established to respond to critical cybersecurity incidents. The cyber incident response team should develop the incident response governance model (Fundamental 10),[6] including defining the types and severity of incidents that will require a comprehensive response.

The cyber incident response team should be comprised of organizational stakeholders, including other departments and external entities. In addition to IT and OT security staff and operators, team composition should include other staff such as executives, communications and public relations teams, human resources, legal, product, and engineering personnel.

## System Backups

System backups play a critical role in timely recovery and reducing the risk of data destruction or inhibiting system recovery after a cyber incident. Backups need to be protected from the risk of being corrupted or destroyed (such as during a ransomware attack), validated, and tested to ensure effective recovery when needed.

Restoration from backups need to be tested periodically. Assuming backups can be used for restoration without verifying efficacy through test restorations can often prove costly. It is also recommended to take the time to create human readable backups in addition to automated/native backup functions. In the event replacement devices cannot use the automated backup file, the human readable version will increase the efficiency of restoration.

**Practical Application**

Use resource planning tools, such as automatically generated work orders to have staff verify data back up integrity, rotate backup media, locate backup files, and perform test restorations from backups.

**CPG | 2.R System Backups**

- All systems that are necessary for operations are backed up on a regular cadence, no less than once per year.
- Backups are stored separately from the source systems and tested on a recurring basis, no less than once per year.
- Stored information for OT assets includes at a minimum: configurations, roles, PLC logic, engineering drawings, and tools.

## Cyber Insurance

Recovering from a cyber incident can be expensive. Average estimates for the cost of cyber attacks run from tens of thousands of dollars for small organizations to millions of dollars for large organizations. Expenses can include emergency support of vendors that specialize in incident forensics and recovery, replacement of corrupted software, computers and other hardware, complimentary credit monitoring for customers whose data was stolen, customer notification, lost productivity of employees who cannot work until the system has been restored, legal fees and liabilities, and even public relations outreach.

6 Fundamental 10 | Develop and Enforce Cybersecurity Policies and Procedures is scheduled to be released in December 2024

Cyber insurance is a tool in the resilience toolkit. Not only can insurers reimburse or pay for some or all expenses listed above, many policies provide expert emergency support in the form of knowledge and vendors and contractors specializing in forensics and recovery. While cyber insurance has matured, there is still a lack of standardization across policies, so researching insurers, comparing policies, and "right-sizing" a policy is important.

For instance, some policies may not pay claims for pre-existing breaches, acts of war, or if the cause of the breach was an employee who fell victim to a phishing email or other social engineering tactic. Most insurers insist on minimum required security controls, risk assessment, or cyber risk profile before granting a policy.

## Disaster Response Plans

Under America's Water Infrastructure Act, drinking water systems must develop emergency response plans (ERPs) and update them every five years. The plans must address both cyber systems and physical systems. The plans required under the act go beyond emergency response. The law's provisions also require utilities to document how they will mitigate threats and how they will enhance mitigation and resilience.

While ERPs are not required for wastewater utilities under the law, these utilities may find it useful to prepare them. Regardless of the law, these plans can provide guidance during times of heightened confusion or stress. For this reason, plans help reduce the severity of impacts and facilitate a faster recovery for the system and the affected organization's overall operations.

IT and OT professionals may be more familiar with the concept of the disaster response plan (DRP), which can be folded into a utility's ERP. Both documents are traditionally part of an organization's business continuity plan or continuity of operations plan, which is described in the Water Research Foundation's *Business Continuity Planning for Water Utilities*.

During the preparation of the emergency response plan, input should be obtained from various stakeholders, which can include personnel from IT, OT, physical security departments of the organization, and external partners. All stakeholders should regularly train on and exercise the plan.

DRPs can include:

- A list of major goals of the disaster plan.
- Names and contact information of IT and OT personnel, vendors, and contract support.
- Roles and responsibilities.
- Profiles of software and hardware used by the utility, including a discussion of which utility functions rely on each software and hardware item.
- Service level agreements for outsourced services during a disaster.
- Recovery time objectives.
- Maximum tolerable downtime.
- Backup procedures.
- Plans for mobilizing to temporary work locations.
- Plans for backing up to a temporary site.
- Plans for restoring the home site.
- Plans for testing and exercising the DRP.

## Backup Out-of-Band Communications

Does your utility have a backup communications plan? It is important to consider such critical response dependencies before an incident occurs. Out-of-band communications play a vital role during incident response by providing alternative methods or technologies that enable teams to maintain secure communications during an incident. For example, the email server may be down due to a compromise or ransomware attack, the internet may be out due a DDoS attack – or worse, the incident could coincide with larger regional incidents which could likely result in cellular carrier capacity becoming saturated. Therefore, it is important to consider how response would be impacted if communication mechanisms were not available.

**For Consideration**

When choosing out-of-band communications, utilities may wish to consider the following:

- What common dependencies does it share with your primary communications mechanism?
- Are the cyber incident response and operations teams onboarded to that mechanism?
- Is the backup communications mechanism encrypted?
- Does your utility have two-way radios?
- Is your utility signed up for telecommunications priority services[7] such as Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS)?

## Power Resilience

Utilities require power to operate their IT and ICS equipment, and they can protect their systems against the impacts of power outages by having on-site generation available in emergencies. Generators can be either utility-owned or supplied during an incident through preexisting contracts. NIST encourages utilities to have an uninterruptible on-site power supply that can span the time between when power is lost, and emergency power generation is activated. Utilities should also have plans in place to ensure that generators will have adequate fuel throughout an emergency. Water utilities can also coordinate with their local power utility to ensure that critical facilities are a high priority during power restoration efforts. Additional information about power outage resilience is available on WaterISAC's "Power Outage and Black Sky Resilience resources" web page.

**For Consideration**

It is important to consider protecting automatic transfer switches (ATS) and intelligent circuit breakers once you start to think about the cyber in power dependency. If your ATS is on the network, it can become a single point of failure for both utility and emergency power. The same considerations should be addressed with network connected uninterruptable power supplies (UPS).

## Practice Makes Proficient

As is true for all response and recovery plans, CIRPs and DRPs are not complete once they have been developed. The plans need to be operationalized, regularly reviewed, practiced, and updated accordingly. Organizations should practice their plans through regular operational and tabletop exercises (TTXs). To further test readiness, consider incorporating a red team and/or blue team approach to the exercises. Additionally, purple teaming[8] exercises will promote enhanced collaboration between red and blue teams.

### Tabletop Exercises (TTXs)

As stated, utilities are highly encouraged to practice CIRPs through workshops and tabletop exercises (TTXs). There are multiple options available for exercising, from a basic workshop discussion to full-scale and coordinated functional exercise. CISA offers several TTX options, from self-service to end-to-end exercise planning and conduct support, to assist utilities in examining their cybersecurity plans and capabilities.

*CISA Tabletop Exercise Packages (CTEPs)*[9] are a comprehensive set of resources designed to assist stakeholders in conducting their own exercises. Each package is customizable and includes template exercise objectives, scenarios, and discussion questions as well as a collection of references and resources. CTEPs cybersecurity scenarios cover various cyber threat vector topics such as ransomware, insider threats, phishing, and **industrial controls.** CTEPs also include physical scenarios and cyber-physical convergence scenarios. **The cybersecurity[10] and cyber-physical convergence[11] scenarios include exercises specifically designed for Water and Wastewater Systems.**

Utilities may wish to engage external entities to help plan, develop, and execute exercises. Through its Stakeholder Exercises,[12] CISA offers fully supported end-to-end exercise planning and conduct support. NCEP support includes planning meetings, document and scenario development, facilitation, and after-action report development. Utilities can participate in CISA-led discussion-based exercises in the form of seminars or workshops. Stakeholder exercises also support operations-based exercises that leverage functional and full-scale drills to test security plans and capabilities more comprehensively.

7 https://www.cisa.gov/topics/emergency-communications/priority-services
8 https://scythe.io/roles/purple-teaming
9 https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages
10 https://www.cisa.gov/resources-tools/resources/cybersecurity-scenarios
11 https://www.cisa.gov/resources-tools/resources/cyber-physical-convergence-scenarios
12 https://www.cisa.gov/resources-tools/services/stakeholder-exercises

There are also private options such as WaterISAC Champion organizations, Gate 15 and Dragos, that support various exercise activities. Gate 15[13] specializes in activities such as TTXs, drills, continuous improvement workshops, and more. Dragos TTX Service[14] can help test and strengthen your ICS cybersecurity strategy in a collaborative workshop. When engaging private third parties, to ensure a cohesive experience, WaterISAC recommends working with firms that use the FEMA *Homeland Security Exercise and Evaluation Program (HSEEP)*[15] principles. HSEEP provides a set of guiding principles for exercise and evaluation programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning.

There are additional opportunities to participate in exercises on a regional or national level that incorporate multiple stakeholders across multiple critical infrastructure sectors to practice responding to and recovering from coordinated cyber and physical security threats and incidents.

*Cyber Storm*[16] is a CISA-sponsored cybersecurity exercise focused on policy, procedure, information sharing, coordination, and decision-making. The exercise provides a venue to simulate discovery of and response to a large-scale, coordinated cyber-attack impacting critical infrastructure, and an opportunity for the Federal Government, SLTT organizations, and the private sector to address cyber incident response as a community.

*GridEx*[17] is the largest grid security exercise in North America. It is hosted every two years by NERC's Electricity ISAC (E-ISAC).

*Black Sky Exercise*[18] allows organizations to perform a reality check in a no-fault environment without a bad day happening. It allows discretionary time to prepare for that rare but very possible Black Sky Event.[19]

**BONUS MATERIAL | Critical infrastructure cybersecurity prioritization: A cross-sector methodology for ranking operational tech-nology cyber scenarios and critical entities[20]**

Today, critical infrastructure cyber protection correlates sixteen different sectors, with no way to compare a standardized risk metric from a municipal water facility in Wyoming with a large commercial energy provider in Florida or a rural hospital in Texas with a train operator in New York. This section proposes a scoring methodology for cross-sector entity prioritization using qualitative scenario planning and quantitative indicators for severity scoring, assessing the potential for scenarios to cause public panic and to stress/overcome local, state, and federal response capacity.

This methodology has two primary use cases:

1. The scoring matrix provides a way to rank and prioritize relevant cyber scenarios for a single entity, organization, facility, or site in scope.
    a. The ranking, based on weighted scores, will allow any entity, organization, facility, or site to choose scenarios to exercise based on a choice of two real-world impacts (impact A, impact B) or to assess both impacts when choosing a tabletop scenario.
    b. This ranking has the potential to prioritize scenarios that will cause public panic and/or overwhelm response resources over scenarios that simply have a higher cyber severity rating (see Table 1).
2. The standardized priority score provides an overall priority score for the entity, organization, facility, or site.
    a. This score can be used to compare and rank different entities, locations, facilities, or sites within a given jurisdiction—city or local, state, federal, sector-specific, etc.

**This methodology can be incorporated into assessments, training, and tabletop exercises in the planning phase of cyber risk mitigation and incident response.** It can also be used by leaders to prioritize multiple critical infrastructure sectors or locations in their jurisdiction from a cybersecurity perspective.

13 **https://gate15.global/services/**
14 **https://www.dragos.com/tabletop-exercise/**
15 **https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep**
16 **https://www.cisa.gov/resources-tools/services/cyber-storm**
17 **https://www.nerc.com/pa/CI/ESISAC/Pages/GridEx.aspx**
18 **https://eiscouncil.org/what-is-a-black-sky-exercise/**
19 **https://eiscouncil.org/black-sky/**
20 **https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/critical-infrastructure-cybersecurity-prioritization/#introduction**

**For Consideration**

A fun and engaging exercise option is Backdoors & Breaches, an Incident Response Card Game,[21] from Black Hills Information Security and Active Countermeasures. Backdoors & Breaches contains 52 unique cards to help you conduct incident response tabletop exercises and learn attack tactics, tools, and methods. To enhance play even more, there are several expansion decks available, including ICS/OT, cloud security, and more.

## Manual Operations

Manual control of water and wastewater systems should also be practiced as part of IR procedures to help understand limitations and inform design enhancements that can make future manual control more efficient.

IR plans should include measures for reacting to destructive malware in an ICS environment. In such situations, organizations should be prepared to restore from off-line backups and to "island" their ICS environments by disconnecting from non-ICS networks. They should also be prepared to revert to manual operations if network conditions impact visibility from the SCADA system, or if malware potentially renders control devices inoperable or untrustworthy.

Practice ensures that all stakeholders understand the procedures that would be implemented in the event of a significant cyber disruption or breach, enabling a more effective and efficient response.

**Practical Application**

Use organizational resource planning tools, such as automatically generated work orders, to have operations operate in manual mode. This will create the muscle memory for operating that mode during an incident under more stressful conditions.

21 https://www.blackhillsinfosec.com/projects/backdoorsandbreaches/

## SMALL SYSTEMS GUIDANCE

Smaller systems and less cyber mature utilities may find benefit in CPG practice ***2.S Incident Response Plans*** that requires **little to no monetary investment.** Likewise, this goal has a **high impact** toward risk reduction and is considered **low complexity** to implement.

### CPG | 2.S Incident Response (IR) Plans

Organizations have, maintain, update, and regularly drill IT and OT cybersecurity incident response plans for both common and organization-specific (e.g., by sector, locality) threat scenarios and TTPs.

- When conducted, tests or drills are as realistic as feasible.

IR plans are drilled at least annually and are updated within a risk-informed time frame following the lessons learned portion of any exercise or drill.

Participating in or executing tabletop exercises (TTXs) may seem daunting, but for smaller or less resourced utilities the process will be extremely valuable and probably enlightening. According to VERVE, *even a rudimentary low-cost cyber-focused TTX, or paper-based training can be devised to illustrate gaps in your utility's processes, resources, training, and technology. Tabletop exercises don't need to be "hacker" orientated and don't require elaborate props or expensive third-party trainers and platforms to be effective.*[22]

### For Consideration

Executing low-cost ransomware or cyber-event tabletop (TTX) or paper-based training has several benefits:

- It raises awareness within the organization about the current state of maturity and incident/event preparedness.
- It satisfies a compliance or framework checkbox.
- Such training offers a low-cost, high-reward way to illuminate gaps that could threaten the organization's overall event response.
- The exercises can be devised internally by individuals who understand how the facilities actually run.
- It brings all parties to the table and settles disputes over who owns what.
- Communication/collaboration driven by the tabletops often facilitate organizational change and foster improved inter-domain trust.

VERVE
A ROCKWELL AUTOMATION COMPANY

### RECOMMENDED RESOURCE

Dragos OT-CERT[23] members have access to the following CIRP and TTX resources:

- Cyber Incident Response Plan Getting Started Guide
- OT Cyber Incident Response Plan Worksheet
- Exercise Scenario Briefing: OT-CERT Self Service Tabletop: Ransomware Disrupts Operations
- OT-CERT-Self Service TTX Ransomware Facilitator Kit

OT-CERT
OPERATIONAL TECHNOLOGY
CYBER EMERGENCY READINESS TEAM

22 https://verveindustrial.com/resources/blog/getting-prepared-tabletops-and-scripts-to-act-through-a-ransomware-event/
23 https://ot-cert.dragos.com/

## RECOMMENDED RESOURCES

**Incident Response Guide for Water and Wastewater Sector** | CISA | EPA | FBI

**CISA Tabletop Exercise Packages (CTEP)** | CISA

**Stakeholder Exercises** | CISA

**Planning Considerations for Cyber Incidents: Guidance for Emergency Managers** | FEMA | CISA

**Cybersecurity Incident & Vulnerability Response Playbooks** | CISA

**Business Continuity in a Box** | CISA & Australian Cyber Security Centre (ACSC)

**Cyber Storm** | CISA

**Develop and Conduct a Water Resilience Tabletop Exercise with Water Utilities** | EPA

**GridEx** | Electricity ISAC (E-ISAC)

**Homeland Security Exercise and Evaluation Program (HSEEP)** | FEMA

**Incident Command System for Industrial Control Systems (ICS4ICS)** | ISA Global Cybersecurity Alliance

**Backdoors & Breaches, an Incident Response Card Game** | Black Hills Information Security & Active Countermeasures

**How Incident Response (IR) Tabletop Exercises Strengthen OT Security Posture** | Dragos

**From reaction to resilience: Our reimagined Incident Response & Readiness Guide** | Red Canary

**Is your IR plan DOA?** | Red Canary

**7 common mistakes companies make when creating an incident response plan and how to avoid them** | Talos Intelligence

**Getting Prepared: Tabletops and Scripts to Act Through a Ransomware Event** | VERVE – *A Rockwell Automation Company*

**Power Outage and Black Sky Resilience Resources** | WaterISAC

**Emergency Planning for Water & Wastewater Utilities - M19** | AWWA

**Business Continuity Planning for Water Utilities** | WRF

**Introducing Mandiant's Digital Forensics and Incident Response Framework for Embedded OT Systems** | Mandiant

**How to Manage the Rising Cost of OT Cyber Insurance** | VERVE – *A Rockwell Automation Company*

# 2 Minimize Control System Exposure

**WHY THIS IS IMPORTANT: Unidentified connections into the OT network present unnecessary risk to availability, control, and safety of industrial automation and control systems (IACS).**

All communication pathways that exist between the ICS/OT network and hostile networks – internal (IT, business) and external (internet) – must be identified. Isolating (air-gapping) a control system from the rest of the world would be ideal. However, complete isolation is likely not practical and may not even be possible.

Connections are difficult to avoid given the demands for remote system access by staff and third parties due to system monitoring/maintenance or to export control system data for regulatory and business purposes. Even if these connections could be avoided, there are always control system upgrades and patches that make some kind of communication with the outside world unavoidable. Implementing a defensible architecture is the key to minimizing control system exposure and requires a combination of physical and logical network segmentation, hardware and software that restrict traffic, protection of control system design and configuration documents, encrypted communications, restrictive procedures, and physical security.

### Five ICS Cybersecurity Critical Controls[1] | Control No. 2: Defensible Architecture

Minimizing control system exposure contributes to having a defensible architecture. As highlighted in the Five ICS Cybersecurity Critical Controls, Control No. 2., common attributes of defensible architectures related to minimizing control system exposure include:

- Segmented environments where possible to reduce ingress and egress into as few pathways as possible, ultimately creating "choke points" for enhanced security and monitoring.
- Determining when bi-directional access is needed, both now and in the future vs. truly read-only applications.

### CPG | 2.X Limit OT Connections to Public Internet

- No OT assets are on the public internet, unless explicitly required for operation.
- Exceptions must be justified and documented, and excepted assets must have additional protections in place to prevent and detect exploitation attempts (e.g., logging, MFA, mandatory access via proxy or other intermediary).

According to **NIST Special Publication NIST SP 800-82r3 Guide to Operational Technology (OT) Security** (September 2023),[2] minimizing control system exposure encompasses (but is not limited to) the following:

- Implementing a network topology for the OT system that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.
- Providing logical separation between the corporate and OT networks (e.g., stateful inspection firewalls between the networks, unidirectional gateways).
- Considering where physical separation may be required as opposed to logical separation.
- Employing a DMZ network architecture (e.g., prevent direct traffic between the corporate and OT networks).
- Using multi-factor authentication for remote access to the OT system.
- Restricting physical access to the OT network and devices. *This will be discussed further in Fundamental 7.*
- Applying security techniques, such as encryption and/or cryptographic hashes, to OT data storage and communications where appropriate.

1 https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/
2 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

## External (Untrusted) Pathways

The control systems of some utilities may not directly face the internet. However, a connection likely exists if those systems are connected to another part of the network, such as the enterprise IT network that has a communication pathway to or from the internet. These connections can be identified through a comprehensive asset inventory (Fundamental 5)[3] and evaluated with a thorough risk assessment.

It is not uncommon for compromises to ICS networks to emanate from the IT/business network. Therefore, it is vital to eliminate any unnecessary communication channels discovered between devices on the control system network and equipment on other networks. Any connections that remain need to be carefully evaluated and managed to reduce network vulnerabilities.

## Segmentation

Access to network segments can be restricted by physically isolating them entirely from one another, which is optimal for industrial control systems, or by implementing technologies such as firewalls, demilitarized zones (DMZs), virtual local area networks (VLANs), and unidirectional gateways/data diodes.

- **Firewalls** are a hardware device or software program that filter inbound and outbound traffic between different parts of a network, or between a network and the internet.
- **ICS-DMZs** are a network segment that sit between the control system network and any untrusted or other internal network to protect unwanted traffic from communicating directly with critical devices within the control system zones.
- **VLANs** are logical connections that partition different segments of a network, often by function.
- **Unidirectional gateways** and **data diodes** allow for one-way traffic from the control system network and prevent traffic from flowing back into the control system network.

### RISK SCENARIO

A utility may have equipment or components that use Bluetooth or other short-range communications protocol for configuration. Despite the limited communication range of such devices, these connections represent another entry point for an adversary. Organizations may be unaware of these short-range connections, but cyber threat actors can find such pathways to access and exploit industrial control systems.

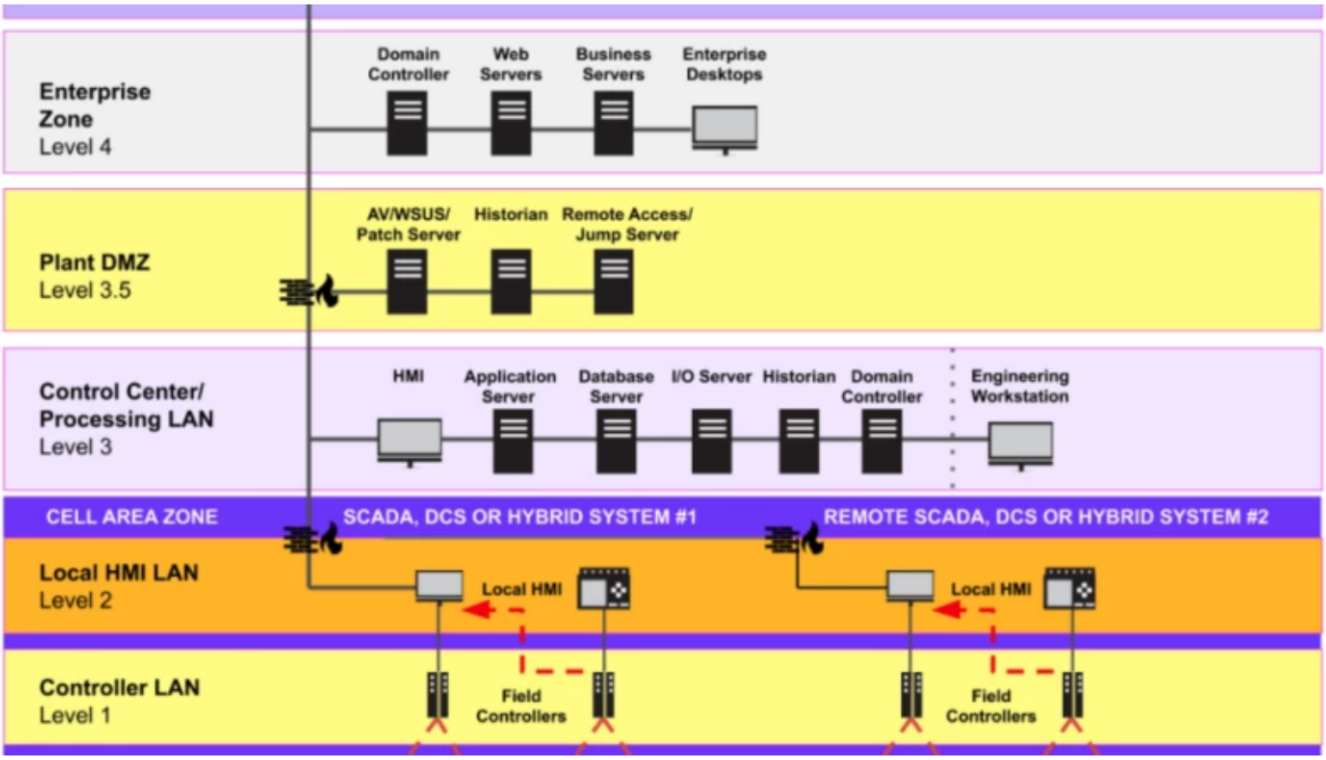
### CPG | 2.F Network Segmentation

- All connections to the OT network are denied by default unless explicitly allowed (e.g., by IP address and port) for specific system functionality.
- Necessary communications paths between the IT and OT networks must pass through an intermediary, such as a properly configured firewall, bastion host, "jump box," or a demilitarized zone, which is closely monitored, captures network logs, and only allows connections from approved assets.

3 Fundamental 5 – Accounting of Assets will be released June 2024

## Zone Restrictions

Network segmentation also entails classifying and categorizing IT and ICS/OT assets, data, and personnel into specific groups or zones, and restricting access based on these groupings. By placing resources into different segments of a network, and restricting access to specific zones, a compromise of one device or system is less likely to translate into the exploitation of the entire system. The Purdue model in the image below is used to best illustrate industrial network zones.




This diagram shows the standard architecture of an industrial network configured according to the Purdue Model. Industrial devices are located at levels 0 through 3.[4]

When computer systems are interconnected, cyber threat actors may be able to exploit any vulnerability within an organization's network to gain entry and move laterally throughout the environment to access sensitive equipment and data.

## Restrict Traffic

When installed and configured properly, firewalls, ICS-DMZs, VLANs, and unidirectional gateways/ data diodes provide crucial functions in filtering or blocking unwanted traffic that could adversely impact availability, reliability, and safety of the control system network. By reducing the number of pathways into and between networks and by properly implementing security protocols on the pathways that do exist, it is much more difficult for a threat actor to compromise the network and gain access to other systems.

Creating network boundaries and segments and classifying assets and data empowers an organization to enforce both detection and protection controls within its infrastructure. The capability to monitor, restrict, and govern communication flows enables defenders to baseline network traffic, especially traffic traversing a network boundary, and identify anomalous or suspicious communication flows. To ensure unwanted traffic is not traversing the network, firewall and segmentation rules should be reviewed regularly and validated with packet inspection of network traffic to assess the status of unnecessary ports or services.

Ensure assets don't have unknown internet connectivity. As adversaries and red teams gain access to a new asset, it is common practice to test for external connectivity. It is not uncommon to find a particular asset that has unknown or forgotten connectivity to external or untrusted networks. When an artifact like that is discovered, it is often used as a mechanism to establish command and control traffic and persistence within the environment.

4 https://claroty.com/blog/ics-security-the-purdue-model

## Encrypted Communications

Another way to limit control system exposure is to encrypt all communications. Encryption can protect control system maintenance traffic on an internal network, external remote access traffic destined to the control system, or device-to-device traffic over the public telecommunications network or private radio network.

Protocols like IPSec can be used to encrypt traffic over a public telecommunications network. Built-in encryption options or add-on serial traffic encryption devices can be used to protect data radio communications. Encryption makes it very difficult for malicious actors to fake or intercept control system traffic.

### For Consideration

While it's desirable to encrypt all traffic on the local area network, it may not be practical and could be cost prohibitive for some organizations to perform packet inspection of the encrypted traffic. Two alternatives for consideration are follows:

- Allow local LAN traffic to remain unencrypted to enable network monitoring and apply encryption as traffic leaves the electronic security perimeter.
- Apply IPSec encryption for the authentication process only. This approach provides data integrity to prevent malicious manipulation but still allows asset owners to perform traffic inspection without the cost of decrypting and re-encrypting the traffic.

## Restrictive Procedures

Only dedicated and properly secured devices should be permitted within the control system environment. This restriction applies to laptops, USB memory flash drives, backup hard drives, and any other device that could be infected with malware, including mobile, and "internet of things" (IoT) devices. Each device that has been vetted should be clearly marked. This procedure is required for everyone – staff, contractors, consultants, and vendors.

### CPG | 2.V Prohibit Connection of Unauthorized Devices

- Organizations maintain policies and processes to ensure that unauthorized media and hardware are not connected to IT and OT assets, such as by limiting use of USB devices and removable media or disabling AutoRun.
- OT: When feasible, establish procedures to remove, disable, or otherwise secure physical ports to prevent the connection of unauthorized devices, or establish procedures for granting access through approved exceptions.

### Practical Application

During periods of large-scale control system enhancements or upgrades, additional restrictive measures may be needed, such as requiring the integrator to use utility owned laptops and software, or possibly developing and testing the new system on a parallel network not connected to the active control system.

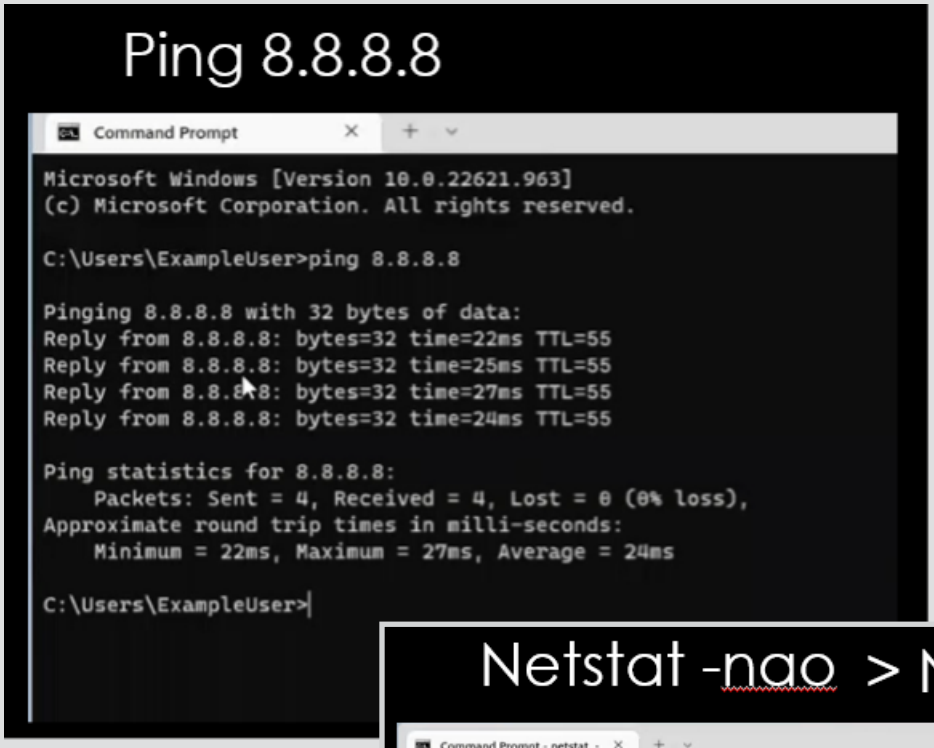
While external connections to the control network should always be disabled, that may not be practical. There are instances where a connection is necessary and exceptions must be made for updates, remote administration, vendor access, or other reasons. In these instances, employing an ICS-DMZ is necessary to secure the communication pathways between the networks for those occasions when secure access is temporarily enabled.

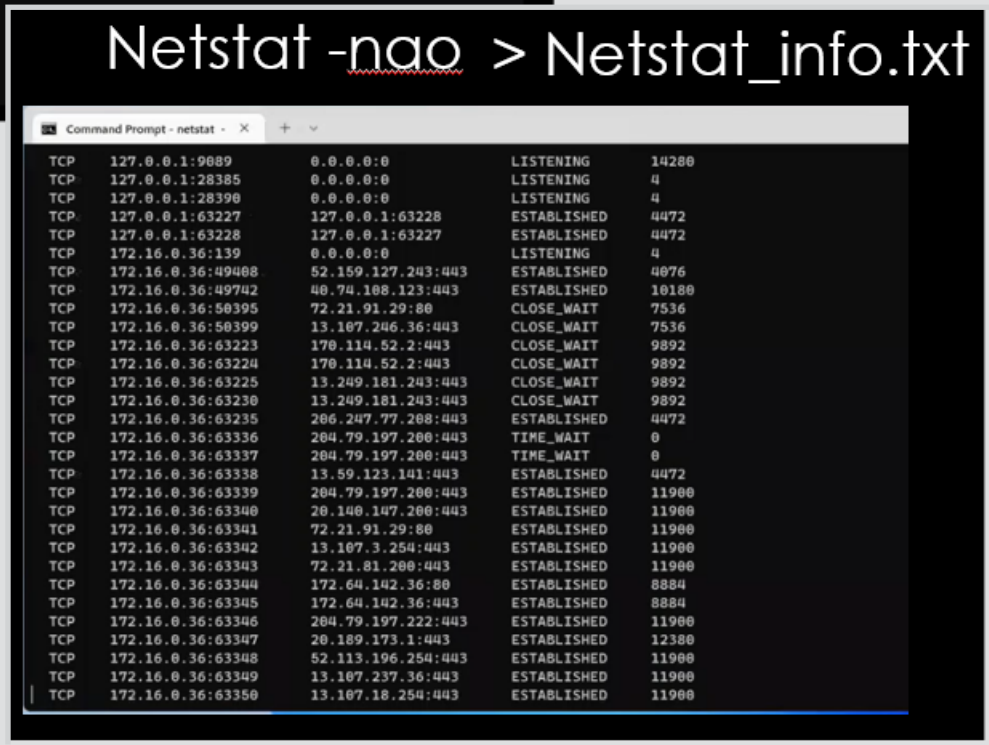
Once access is no longer needed, connections must be disabled immediately. Never leave a connection to the control network enabled for an undetermined timeframe. Likewise, in lieu of enabling temporary network access, consider requiring the use of a dedicated and hardened, non-ICS connected PC for things like patch downloads. Downloads should be scanned for malicious content, and cryptographic hashes or digital signatures validated before applying to control system devices.

## Practical Application

Hunting for unknown or undocumented connectivity in your ICS/OT environment is not complicated. There are simple, native, non-intrusive commands to test the assets in your environment for external connectivity.

Two very useful command-line/terminal commands are **ping** and **netstat**. The quickest way to check an asset for external connectivity is to check for reachability to an external destination. Google's public DNS IP address (8.8.8.8) is a good test. Likewise, assets should be checked for additional network connections. The following images demonstrate how the **ping** and **netstat** commands are easily executed for each function.




In this example, the netstat output is sent to a text file so the results can be reviewed for legitimate connections and any undesirable connections (internal or external) can be addressed accordingly.

## Secure Remote Access

Remote access has become part of normal operations in industrial environments. The ability to remotely connect to a network adds a great deal of convenience for end users, engineers, systems administrators, integrators, and support vendors. However, it also provides an opportunity for threat actors to infiltrate the network. Methods of remotely connecting securely should be implemented to minimize risk. Implementing a secure remote access architecture for the ICS environment is so important and necessary that it is one of the *Five ICS Cybersecurity Critical Controls* (Control No. 4) which states, establishing secure remote access is a must in modern-day industrial operations.

Firewalls, demilitarized zones, jump servers, virtual private networks (VPNs), secure shell (SSH), multifactor authentication (MFA), and many commercial solutions are viable options that provide increased security when remote access is required. Additionally, remote access can further be restricted with access control lists that only allow access from specific IP addresses and/or ranges and geographic locations (Fundamental 6).

When implementing a secure remote access solution, Dragos recommends:[5]

- Leveraging existing infrastructure and expertise.
- Implementing a DMZ with a secure jump host.
- Multi-factor authentication (MFA).
- Third-party remote access requirements.
- Monitoring and auditing of remote access sessions.

### Jump Servers

Jump servers are intermediate servers that reside in the demilitarized zone (DMZ). When remote access is required, jump servers are used for authentication and to provide connectivity to less secure remote servers in the control network. Jump servers provide the ability for remote users to connect to an intermediary device without having to connect directly to other control network servers, workstations, or other less secure devices.

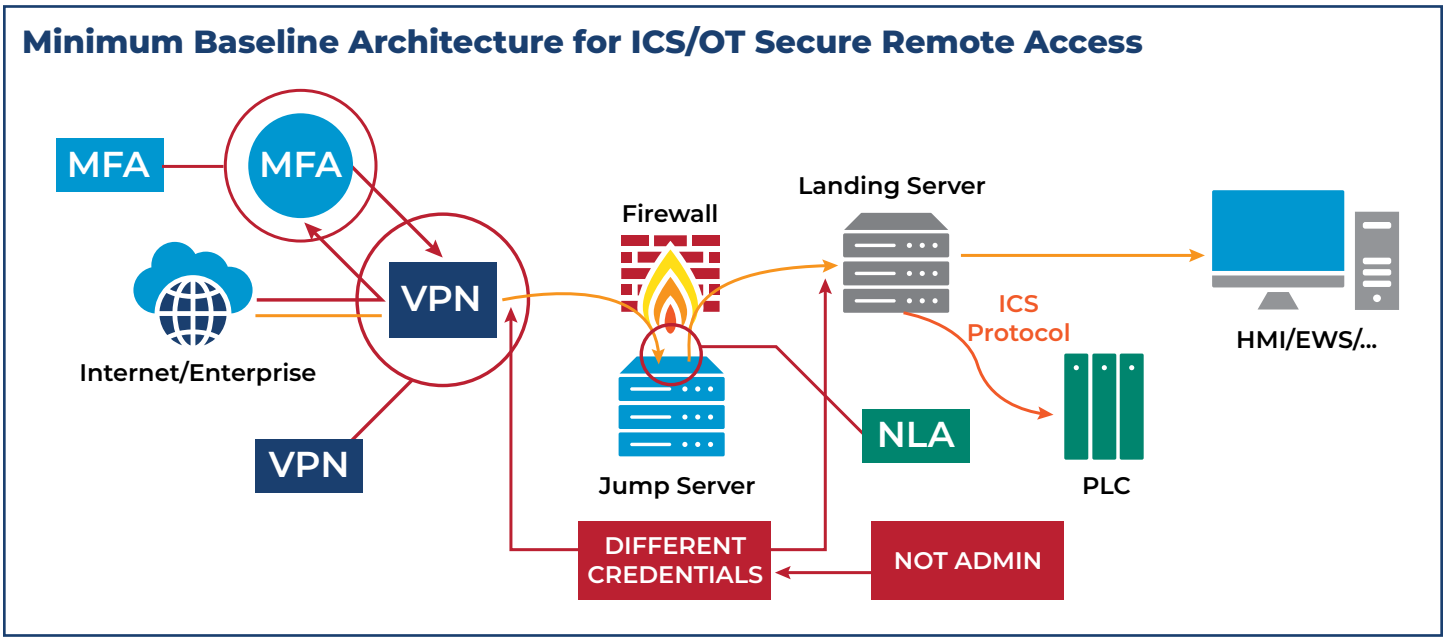
### VPN

A VPN is an encrypted data channel to securely send and receive data via public IT infrastructure (such as the internet,) or to securely connect to the control network from other segments of the enterprise network. Through a VPN, users can remotely access internal resources like files, printers, databases, websites, and management interfaces as if directly connected to the network. However, a VPN is only as secure as the devices connected to it; an authorized device infected with malware can still propagate that malware onto the network, leading to additional infections and negating the security of the VPN.

### SSH

SSH provides secure authentication and authorization to hosts when remote administration is required. SSH is used to safely and remotely connect to devices to perform management or file transfer activities. It should be disabled by default and access granted only to explicitly defined hosts and networks.

### Minimum Baseline Architecture for ICS/OT Secure Remote Access




5 https://www.dragos.com/blog/recommendations-to-implement-secure-remote-access-today/

## Securing Programmable Logic Controllers

Another facet of minimizing control system exposure and implementing a defensible architecture involves hardening control system engineering devices including supervisory control and data acquisition (SCADA), distributed control systems (DCS), programmable logic controllers (PLCs), etc. This section specifically discusses securing PLCs. *In a way, PLCs are the quintessential OT. PLCs are the devices that are deterministic, have real-time capabilities, operate in rough environments, and often run decades without being substituted* (Fluchs, 2022).[6] PLCs are often (and aptly) described as insecure-by-design, but they don't have to stay that way anymore.

Until 2021, there was no standard PLC security guidance. The industry lacked a common reference to leverage PLCs' built-in security capabilities or to address threats and vulnerabilities – let alone an effective way to implement secure coding. In 2021, the first of its kind guidance resource to help secure the inherently insecure-by-design PLCs was published. *The Top 20 Secure PLC Coding Practices (Version 1.0, published 15 June 2021)* were written by engineers for engineers and technicians that program and maintain PLCs.[7] The following are examples from the *Top 20 Secure PLC Coding Practices*.

### EXAMPLES | 20 Secure PLC Coding Practices

#### 2. Track operating modes

**Keep the PLC in RUN mode. If PLCs are not in RUN mode, there should be an alarm to the operators.**

| Security Objective | Target Group |
|---|---|
| Integrity of PLC logic | Integration / Maintenance Service Provider<br>Asset Owner |

#### 3. Leave operational logic in the PLC wherever feasible

**Leave as much operational logic e.g., totalizing or integrating, as possible directly in the PLC. The HMI does not get enough updates to do this well.**

| Security Objective | Target Group |
|---|---|
| Integrity of PLC logic | Product Supplier<br>Integration / Maintenance Service Provider<br>Asset Owner |

#### 19. Monitor PLC memory usage and trend it on the HMI

**Measure and provide a baseline for memory usage for every controller deployed in the production environment and trend it on the HMI.**

| Security Objective | Target Group |
|---|---|
| Monitoring | Integration / Maintenance Service Provider<br>Asset Owner |

6 https://fluchsfriction.medium.com/one-year-of-top-20-secure-plc-coding-practices-c2f0042ad4a2
7 Background: The idea of secure coding practices for PLCs was the brainchild of water sector veteran Jake Brodsky and was presented during an S4x20 Conference session.

The coding practices are intended to be used by automation engineers and technicians that program and maintain PLCs. Moreover, these practices are designed to be implemented with native PLC functionality to securely program PLCs with little to no additional software tools or hardware to increase PLC integrity, monitoring, hardening, and resilience. Additional benefits of these coding practices are that they are not an all or nothing approach and can be applied to existing architecture. There is no need to wait until an infrastructure upgrade or greenfield project to start securing PLCs.

### EXAMPLE | Template for RFP Language for PLC Security

If your utility outsources SCADA support, be intentional about asking if secure coding practices such as these are being implemented on your project. Likewise, include this as a requirement in your next RFP. PLC Security has provided a sample template for public use.

This Specification sample document is focused on outlining requirements inspired by the Top 20 list for vendor control equipment (e.g., a new process unit is being added to the facility and a vendor skid package with a vendor template design and program). These requirements or the policy can be developed and provided to the vendor to improve the security and integration while beginning to adopt the practices. See ***Cybersecurity PLC Vendor Policy Example*** in the Resources section.

## Zero Trust in OT Networks

According to CISA's Zero Trust Maturity Model,[8] zero trust provides a collection of concepts and ideas designed to **minimize uncertainty** in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. **The goal is to prevent unauthorized access to data and services and make access control enforcement as granular as possible.**

Given the criticality, OT networks should epitomize the concept of zero trust. Unfortunately, that isn't always easy. However, many zero trust components enforce the concepts discussed in this fundamental and those that will be discussed in Fundamental 6, Enforce Access Controls. Consider the following inset box which has been excerpted from the Software Engineering Institute on how to get started extending zero trust principles into ICS.[9]

### How to Get Started | Zero Trust

Creative thinking can help organizations extend zero trust principles even into sensitive industrial environments.

- Depending on the current architecture of the ICS network, it may be necessary to accept that the industrial network is one large implicit trust zone. Where feasible, network segmentation can reduce this trust zone into more manageable pieces.
- Take a hard look at the industrial network and ensure that all interconnections are identified and managed. For example, did a vendor install a cellular modem for maintenance that is providing an unknown back door?
- Restrict interconnections to a limited number of assets that can initiate a remote session from the enterprise network and are mediated by a jump host that itself has robust monitoring.
- Implement logical access restrictions to enforce least privilege by limiting the users that can establish remote connections to only those necessary to meet operational requirements. For example, the organization may grant remote access privileges to engineers who perform maintenance tasks using a remote desktop client.
- Implement stronger authentication, such as multifactor authentication or a privileged access-management system, to provide additional assurance for the assets that are permitted to establish remote access sessions.
- Implement unidirectional gateways for information leaving the industrial network, such as process data being replicated to a database.
- Consider physical access controls that may provide a satisfactory, risk-informed, compensating level of control and monitoring for those who have physical access to OT devices.

8 **https://www.cisa.gov/zero-trust-maturity-model**

9 Benestelli, B., and Kambic, D., 2022: IT, OT, and ZT: Implementing Zero Trust in Industrial Control Systems. Carnegie Mellon University, Software Engineering Institute's Insights (blog), Accessed February 16, 2024, **https://insights.sei.cmu.edu/blog/it-ot-and-zt-implementing-zero-trust-in-industrial-control-systems/**.

## SMALL SYSTEMS GUIDANCE

Smaller systems and less cyber mature utilities may find benefit in this CPG practice, ***2.W No Exploitable Services on the Internet*** that requires **little to no monetary investment.** Likewise, this goal has a **high impact** toward risk reduction and is considered **low complexity** to implement. Generally speaking, this could prove useful for water and wastewater utilities to identify devices that are accessible from the internet that they may not have been aware.

### CPG | 2.W No Exploitable Services on the Internet

- Assets on the public internet expose no exploitable services, such as RDP.
- Where these services must be exposed, appropriate compensating controls are implemented to prevent common forms of abuse and exploitation.
- All unnecessary OS applications and network protocols are disabled on internet-facing assets.

Removing exploitable services (CPG | 2.W) that do not need to be accessible from the internet is considered *low cost to implement*. This activity can often be a "quick win" for smaller systems in reducing cyber risk. However, for critical services that may be deemed a necessity, such as remote access, it is imperative that access be securely implemented, which will likely require a financial investment. *See Secure Remote Access discussed earlier in this Fundamental for guidance.*

Discovering internet facing assets is trivial for threat actors. Small systems are encouraged to learn which assets are accessible from the internet before adversaries exploit/compromise them. CISA's Stuff Off Search (S.O.S.) guide[10] provides information on how to use some well-known publicly available full spectrum search engines including Shodan, Censys, and Thingful to help protect your assets and get your "Stuff Off Search" (S.O.S.)

### ADDITIONAL SERVICE | The Shadowserver Foundation

Utilities may wish to request free, detailed, relevant, daily remediation reports about the state of your networks or constituency. Shadowserver reports will provide a free daily potential attack surface report as well as potential malware or other malicious activity seen originating from your network/ constituency.[11]

10 https://www.cisa.gov/sites/default/files/publications/Assets_Showing_Primer_508c.pdf
11 https://www.shadowserver.org/what-we-do/network-reporting/get-reports/

## RECOMMENDED RESOURCES

**Cyber Resource Hub** | CISA

**"Stuff Off Search" Guide** | CISA

**Know What Your Adversaries Know!** | CISA

**Get Your S.O.S* How-to Guide (Stuff Off Search*)** | CISA

**Recommendations to Implement Secure Remote Access (SRA) Today** | Dragos

**Purdue Model as a Reference for Segmentation** | SynSaber

**Data Diodes Protect Critical Water Infrastructure** | Fend

**Learn About Data Diodes** | OWL Cyber Defense

**Top 20 Secure PLC Coding Practices** | PLC Security

**Cybersecurity PLC Vendor Policy Example** | PLC Security

**Zero Trust Maturity Model** | CISA

**IT, OT, and ZT: Implementing Zero Trust in Industrial Control Systems** | Software Engineering Institute

**5 Considerations to Implementing Zero-Trust in OT Environments** | Claroty

**Zero Trust Security to Protect All OT Environments** | Palo Alto Networks

# 3 Create a Cyber Secure Culture and Protect from Insider Risks

**WHY THIS IS IMPORTANT: Cybersecurity is a shared responsibility among all staff. Every employee, executive, and board member is accountable for the overall cybersecurity posture of an organization. Creating a cyber secure culture relies on leadership support and staff engagement.**

When employees are not involved in cybersecurity, not only can vulnerabilities and threats proliferate or go unnoticed, but employees can become insider threats or conduits through which incidents occur – intentionally or unintentionally. Utilities should instill good cyber hygiene practices in every facet of employees' daily tasks. All staff should know what to do when faced with a potential security incident, whether it is a physical or cyber attack. Developing a strong culture will also minimize insider threats.

## Executive and Board Engagement – Leadership is Crucial for Culture Change

Effective cybersecurity starts at the top. Unfortunately, leadership at small organizations often lacks sufficient awareness of cybersecurity threats and needs. Many organizations remain unprepared to manage cyber risk due to a lack of recognition, understanding, commitment, participation, or empowerment from leadership and/or boards. Leaders don't have to be cybersecurity or technology experts, but they must take responsibility for cultivating a positive cybersecurity culture.

Cybersecurity and culture support from the top-down involves identifying someone to be responsible and accountable for cybersecurity. Without a formal cybersecurity leader there is a lack of sufficient cybersecurity accountability, investment, and effectiveness. The cybersecurity leader could be from or assigned by the executive team or board. Typically, this role is the Chief Information Security Officer (CISO). Furthermore, for effective support, the CISO or equivalent role, should be included on the executive team and meet with the board on a regular basis.

## Cybersecurity Awareness and Readiness Training

The National Cybersecurity Alliance (NCA) promotes creating a culture of cybersecurity from the break room to the boardroom. Creating a cybersecurity culture through awareness training is a key organizational risk strategy component to manage human cyber risk by affecting positive behavior change. To create and maintain a culture of cybersecurity, all personnel should receive regular, ongoing cybersecurity awareness training. In addition, role-specific training should be provided for commonly targeted staff like executives, executive assistants, human resource, finance personnel, IT administrators, engineers, SCADA staff, and operators. According to the SANS ICS/OT Cybersecurity Survey: 2023's Challenges and Tomorrow's Defenses,[1] *short-format ICS-specific awareness modules with knowledge checks will strengthen the culture and reduce risk across many roles. ICS practitioners will further enhance defense, response, and recovery capabilities, and administrative and non-technical employees will gain the knowledge to better understand their crucial role and contribution to critical infrastructure protection.*

While cybersecurity is an expansive subject, there are certain principal topics that should be regularly emphasized for general awareness and to promote positive cyber hygiene. One common theme that warrants frequent inclusion in training materials is social engineering-based tactics, such as phishing. Training should regularly incorporate the importance of safe internet browsing and best practices for secure email handling.

1 https://www.sans.org/white-papers/ics-ot-cybersecurity-survey-2023s-challenges-tomorrows-defenses/

### Advanced Training for Technical Staff

In addition to role-specific training, utility OT, IT, and even legal staff should all be introduced and encouraged to delve into advanced cyber security training. Many free training opportunities are available online and in person.

If the utility is a state or local government organization, there are a variety of classes available from the Federal Virtual Training Environment (FedVTE). There are several free classes available through DHS at Idaho National Laboratory (INL) and classes hosted virtually. Hands-on red team/blue team exercises are available as part of the Industrial Control Systems Cybersecurity (301) training course. Access other training opportunities through the National Initiative for Cybersecurity Careers and Studies (NICCS) Education and Training Catalog. WaterISAC and other organizations such as the SANS Institute, the Electricity ISAC (E-ISAC), and the Multi-State ISAC (MS-ISAC) hold regular, insightful webinars.

Participation in national and regional cyber drills is another valuable training experience. Since defense is informed by offense, to help defenders think like adversaries, attending grey- or black-hat conferences is another valuable approach. Finally, holding monthly internal cross-departmental meetings with staff involved in all aspects of cybersecurity is a valuable practice to reinforce the importance of remaining vigilant. These departmental meetings should include discussions on threats and vulnerabilities in the news, as well as organizational concerns, successes, and priorities.

## SMALL SYSTEMS GUIDANCE

The AWWA Risk Management Guide for Small Systems baseline cybersecurity controls includes Training Staff to be Cybersecurity Aware which involves training staff to reduce the risk associated with a cyberattack. Training should be based on staff members' roles and responsibility within the organization. In addition, training may be informed by the current situational awareness provided by intelligence and law enforcement agencies.[2]

Likewise, for creating a cybersecurity culture, the following CPG practices may be beneficial for smaller systems and less cyber mature utilities. These practices *generally* require **little to no monetary investment,** are considered **low complexity to implement,** and when implemented yield a **high impact toward risk reduction.**

### CPG | 1.B Organizational Cybersecurity Leadership

- A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of cybersecurity activities.
- This role may undertake activities, such as managing cybersecurity operations at the senior level, requesting and securing budget resources, or leading strategy development to inform future positioning.

### CPG | 1.C OT Cybersecurity Leadership

- A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of OT-specific cybersecurity activities.
- In some organizations this may be the same position as identified in 1.B.

### 2.I Basic Cybersecurity Training

- At least annual trainings for all organizational employees and contractors that cover basic security concepts, such as phishing, business email compromise, basic operational security (OPSEC), password security, etc., as well as foster an internal culture of security and cyber awareness.
- New employees receive initial cybersecurity training within 10 days of onboarding and recurring training on at least an annual basis.

For small systems, where employees are not exposed to cybersecurity incident data, there can be a misconception that the organization is too small or "why would someone want to attack us?" It is important to help staff understand that organizations often become victims of circumstance or targets of opportunity. For instance, a utility may use a particular device or application that has a known and exploited vulnerability. Attackers frequently scan the internet for such vulnerable devices and exploit them with

2 https://www.awwa.org/Portals/0/AWWA/ETS/Resources/TechnicalReports/WaterSectorCybersecurityRiskMgmt.pdf?ver=2022-03-17-102456-127

no knowledge of the target. It is helpful to show public examples of incidents and impacts that are relevant to each organization to help employees understand the importance of being vigilant. Consider periodically bringing staff together for lunch-and-learn opportunities to talk about relevant public incidents. These opportunities will help foster a culture of cybersecurity. Even if you don't know how to explain the incident yourself, there are usually good videos available on YouTube to help. **Just make sure to use reputable education sources so that the information is accurate and useful.**

### 2.J OT Cybersecurity Training

- In addition to basic cybersecurity training, personnel who maintain or secure OT as part of their regular duties receive OT-specific cybersecurity training on at least an annual basis.

### RESOURCE | Resiliency for Water Utilities Program

The Cyber Readiness Institute,[3] in partnership with the Center on Cyber and Technology Innovation and Microsoft, is actively recruiting participants to participate in a free cybersecurity training program for small and medium-sized water and wastewater utilities. Complementing other technical assistance programs, the CRI program provides coach-supported training and resources focused on improving cybersecurity risk management and ability to respond and recover from a cybersecurity incident.

The program only requires about an hour per week for six weeks and very minimal technical expertise. Participants proceed at their own pace, with the help of a coach to work through implementing organization-wide trainings and policies for strong passwords, multi-factor authentication, patch management, anti-phishing, business continuity, and other core cyber readiness topics. The program will help utilities establish an asset inventory and improve employee awareness of cybersecurity issues.

If you are interested in participating in this program or learning more, please visit the Cyber Readiness Program - Resiliency for Water Utilities Program[4] on the Cyber Readiness Institute's website.

CYBER READINESS
INSTITUTE

3 https://cyberreadinessinstitute.org/
4 https://cyberreadinessinstitute.org/water-utilities-cyber-ready-training-interest/

All orgaizations face threats from trusted insiders, but utilities operating within critical infrastructure can experience dire consequences to the environment or humans should industrial control systems be compromised, even unintentionally. The more awareness employees have regarding cyber threats, the less likely they are to cause harm to critical assets or systems.

Strong protective cybersecurity controls and system architecture can quickly be defeated by an adversary with physical or privileged access. It is common to believe our greatest threat is external and remote. However, an insider, whether an employee, visitor, vendor, contractor, integrator, or other trusted consultant can cause as much or more damage than an external threat actor.

**RESOURCE | National Insider Threat Awareness Month**

Every September is *National Insider Threat Awareness Month (NITAM).*[5] Utilities may wish to consider leveraging available NITAM resources to help prevent the exploitation of authorized access from causing harm to your organization.

### What Makes an Insider a Threat?

An insider threat is a people problem, not a technology problem; without people, there would be no problem. The bottom line is that every person represents a potential insider threat. However, not all insider threats are malicious.

**DEFINITION**

Insider Threat: The potential for an individual who has or had authorized access to an organization's critical assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.[6]

Many insider threat incidents occur due to simple negligence – the incidents were accidental, lacking malicious intent or motive to cause harm. For instance, a tired, distracted, or hurried employee can make an honest, careless mistake, or an employee who is inattentive may not perceive how their actions could precipitate a threat. According to the Ponemon Institute's *2023 Cost of Insider Risks Global Report,* the most prevalent insider security incident is caused by careless or negligent employees.[7]

Incidents caused by unintentional actions commonly involve accidental disclosure of sensitive information. For example. unintentional actions are often a result of phishing. Individuals lacking malicious intent are generally referred to as "unintentional" or "accidental" insiders.

On the other hand, individuals with motive and intent to cause damage are considered "malicious" or "intentional" insiders. Malicious insiders typically experience some sort of psychological trigger that motivates them to act with malice. The trigger could be the result of personal stressors, coercion, or a combination of both. Malicious insiders typically commit criminal acts like fraud, theft, espionage, or sabotage.

### Top Five Stressors

| | Incidents |
|---|---|
| **1.** Termination | **375** |
| **2.** Resignation | **245** |
| **3.** Internal Position Change | **55** |
| **4.** Oganization M&A Activity | **43** |
| **5.** Emerging Financial Problems | **33** |

*Image credit: Common Sense Guide to Mitigating Insider Threats, Seventh Edition*

5 https://securityawareness.usalearning.gov/cdse/nitam/index.html
6 https://insights.sei.cmu.edu/library/common-sense-guide-to-mitigating-insider-threats-seventh-edition/
7 https://ponemonsullivanreport.com/2023/10/cost-of-insider-risks-global-report-2023/

It takes specialized knowledge to compromise or "hack" into a control system undetected, but it does not take specialized knowledge to misconfigure a control system. Likewise, while some water and wastewater utilities strive to maintain an "air gap" around OT/ICS networks, air does not stop someone from walking up to obtain direct physical access. Furthermore, former employees with specialized knowledge, authorized access, and malicious intent can cause significant harm, including damage to facilities, the environment, and human lives if effective procedures are not followed to disable privileged (physical and cyber) access to the facility and control systems.

An insider threat incident can be accomplished by trusted individuals within your organization – employees, contractors, systems integrators, support vendors, former employees, etc. Trusted insiders do not always purpose to cause harm or destruction, but sometimes damage is the goal or occurs by accident. Alternatively, former disgruntled employees with ongoing access to systems and intent often will do harm if comprehensive termination/off-boarding procedures are not followed to disable access. *Off-boarding will be discussed further in Fundamental 6 – Enforce Access Controls.*[8]

### Real-World Incident[9]

TOPEKA, KAN. – A Kansas man pleaded guilty to tampering with the computer system at a drinking water treatment facility in Ellsworth County. Wyatt Travnichek, 23, of Lorraine pleaded guilty to one count of tampering with a public water system and one count of reckless damage to a protected computer system during unauthorized access.

According to court documents, the Post Rock Rural Water District hired Travnichek in January 2018, and his duties included monitoring the plant after hours using a remote login system. Travnichek resigned his position in January 2019. On March 27, 2019, the remote log in system was used to shut down the plant and turn off one of its filters. Investigators established Travnichek's cell phone was used to perpetrate the intrusion, and that the phone was in his possession at the time of the shutdown. He told investigators he was intoxicated and didn't remember anything about the night of March 27, 2019.

## Start Somewhere

The *Common Sense Guide to Mitigating Insider Threats, Seventh Edition* recommends that organizations consider implementing policies, procedures, and practices to mitigate insider threats and manage insider risk. Not every organization has the resources to develop a formal insider risk management program (IRMP). However, it is still important to consider some basic steps.

Creating a culture of cybersecurity among all levels of your organization will help deter or prevent many insider threats. However, that is not enough. Every organization needs to implement some controls beyond security awareness efforts to prevent, detect, and respond to all types of insider threats.

### Practical Application

Consider establishing a committee of relevant stakeholders to begin evaluating viable methods to prevent, detect, and respond to insider threats. The committee should have representation from key departments across the organization such as human resources, legal, information technology, cybersecurity, physical security, and communications.

***Deter.*** Culture plays a significant role in deterring insider risk. It is important to set expectations through a positive culture. These expectations should be communicated beginning with the recruitment phase, continuing through the employee lifecycle, and even beyond separation. For deterring insider threats, consider:

- Establishing, **communicating,** and enforcing policies/procedures.
- Maintaining separation of duties and least privilege account access.
- Implementing physical security and cybersecurity controls.
- Training **all** new employees (and trusted partners) in security awareness (culture), including insider risks, before granting access to buildings or systems – *and regularly thereafter.*

### Additional Consideration

This should include janitorial and maintenance staff for security situations they may encounter, such as social engineering, active shooter, and sensitive documents left out in the open.

8 Fundamental 6 – Enforce Access Controls is scheduled to be released June 2024
9 **https://www.justice.gov/usao-ks/pr/kansas-man-pleads-guilty-water-facility-tampering**

- Evaluating Cyber-informed Engineering (CIE) principles[10] (Fundamental 8)[11] to safeguard from internal accidents or intentional actions.

  ***SIDE NOTE:*** "Cyber-physical" safety systems can be effective at safeguarding from events or incidents from insider threats as well as external incidents or other failure scenarios.

***Detect*** *(observe and monitor).* Despite best efforts to deter insider threats through cultural awareness, we are all human. While it's important to trust employees and partners, it is equally important to establish controls to detect insider threat activity. Detecting insider risk is a holistic approach that involves technical solutions and behavioral observation. To detect insider risk, it is important to:

- Involve multiple disciplines/departments within the utility *(remember, it's a "people problem").*
- Recognize and report **behavioral** indicators/ stressors.
- Apply technical solutions such as auditing/ logging/monitoring employee accounts.

***Mitigate*** *(controls and consequences).* It is important to effectively establish controls and consistently enforce consequences for all employees. The CERT National Insider Threat Center's "Common Sense Guide to Mitigating Insider Threats, Seventh Edition" offers quick wins and high-impact solutions to help you get started mitigating insider threats. The following figure highlights suggestions for beginning with the hiring process.[12]

- ☑ Ensure that potential workforce members undergo a thorough background check, which, at a minimum, should include a criminal background check and credit check.
- ☑ Encourage workforce members to report suspicious behavior to appropriate personnel for further investigation.
- ☑ Provide a confidential method for reporting suspicious behavior without repercussions.
- ☑ Investigate and document all suspicious or disruptive behavior.
- ☑ Enforce policies and procedures consistently for all workforce members.
- ☑ Consider offering an EAP. These programs can help workforce members deal with many personal issues confidentially.

10 **https://inl.gov/cie/**
11 Fundamental 8 – Implementing Cyber-Physical Safety Systems is scheduled for release September 2024
12 Software Engineering Institute. Common Sense Guide to Mitigating Insider Threats, Seventh Edition. Software Engineering Institute. 2022.

## RECOMMENDED RESOURCES

**OUCH! Newsletters** | SANS Institute

**STOP. THINK. CONNECT.™** | National Cybersecurity Alliance (NCA)

**Cyber Readiness Program - Resiliency for Water Utilities Program** | Cyber Readiness Institute (CRI)

**Federal Virtual Training Environment (FedVTE) Course Catalog** | CISA

**ICS Virtual Learning Portal** | CISA

**NICCS Education and Training Catalog** |NICCS

**How to Talk to the C-Suite and Board About OT Security** | Dragos

**SANS ICS/OT Cybersecurity Survey: 2023's Challenges and Tomorrow's Defenses** | SANS

**Common Sense Guide to Mitigating Insider Threats, Seventh Edition** | Software Engineering Institute, Carnegie Mellon University

**The 13 Key Elements of an Insider Threat Program** | Software Engineering Institute, Carnegie Mellon University

**2023 Cost of Insider Risks Global Report** | Ponemon Institute, DTEX

**National Insider Threat Awareness Month** | USA Learning

**Reducing data exfiltration by malicious insiders** | UK National Cyber Security Centre

1620 I Street, NW, Suite 500
Washington, DC 20006
1-866-H2O-ISAC (1-866-426-4722)

waterisac

waterisac