WATER ISAC

12 Cybersecurity Fundamentals for Water and Wastewater Utilities

Recommended Practices to Reduce Exploitable Weaknesses and Consequences of Attacks

Fundamental 4 | Implement System Monitoring for Threat Detection and Alerting
Fundamental 5 | Account for Critical Assets
Fundamental 6 | Enforce Access Controls

waterisac.org/fundamentals

4 Implement System Monitoring for Threat Detection and Alerting

WHY THIS IS IMPORTANT: While many of the cybersecurity fundamentals in this publication are developed with prevention in mind, in this "assume breach" world, we must be able to detect suspicious and nefarious activity. Without the ability to detect threats within your environments, adversaries will go unnoticed.

Continuous monitoring and threat detection is necessary for the visibility into both IT and ICS/OT networks. The ability to detect threats enables faster threat identification, satisfies regulatory or compliance requirements, and typically reduces adversary dwell time within the network(s). Effective monitoring and threat detection can prevent or minimize financial losses by identifying and mitigating threats before they cause substantial harm.

CPG | 3.A Detecting Relevant Threats and TTPs

Organizations have documented a list of threats and cyber threat actor TTPs relevant to their organization (for example, based on industry, sectors, etc.), and have the ability (such as via rules, alerting, or commercial prevention and detection systems) to detect instances of those key threats.

Monitoring critical infrastructure is so crucial to the security of the U.S. that in 2021, President Biden launched the *Industrial Control Systems (ICS) Cybersecurity Initiative*.[1] The initiative began with a pilot for the electricity subsector and in 2022 it was expanded to include the water and wastewater systems sector.[2] The *ICS Cybersecurity Initiative* was established as a voluntary, collaborative effort between the federal government and the critical infrastructure community to facilitate the deployment of vendor neutral, interoperable technologies that provide asset visibility, **threat detection**, and actionable intelligence for ICS/OT environments. The highest priority for the *ICS Cybersecurity Initiative* is to defend U.S. critical infrastructure by **urging owners and operators to implement monitoring technologies that enhance detection, mitigation, and forensic capabilities.**

The Five ICS Cybersecurity Critical Controls | Control No. 3: ICS Network Visibility and Monitoring[3]

ICS network visibility and monitoring is not just a technology problem. Among the five ICS Critical Controls, ICS Critical Control No. 3 is most often approached by organizations with the question, "what product do we buy to solve our problems?" There is no silver bullet technology that addresses this security control. An organization needs to consider the following factors to inform a technology selection:

- What data acquisition capabilities exist or are planned in connection with ICS Critical Control No. 2? *(Note: ICS Critical Control No. 2 Defensible Architecture was discussed in Fundamental 2 | Minimize Control System Exposure)*
- What vendors and protocols are in use across systems of interest?
- What workforce staffing and capabilities exist or are anticipated to support the program?
- What processes exist or are anticipated in connection with ICS Critical Control No. 1 that will drive incident response actions?

As part of the *ICS Cybersecurity Initiative*, a document was drafted regarding *Considerations for ICS/OT Monitoring Technologies with an Emphasis on Detection and Information Sharing*[4] that outline appropriate detection and response capabilities to help guide critical infrastructure owners and operators. The considerations include things such as:

1 https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/
2 https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/27/fact-sheet-biden-harris-administration-expands-public-private-cybersecurity-partnership-to-water-sector/
3 https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/
4 https://www.cisa.gov/sites/default/files/publications/ICS-Monitoring-Technology-Considerations-Final-v2_508c.pdf

- Develop ICS network traffic baselines for expected operations, compare monitored traffic to the developed baseline, and generate alerts for deviations from that baseline.
- Detect and alert on:
  - Indicators of known malicious activity.
  - Unauthorized or suspicious connections between OT networks and any external network, including enterprise IT networks or the public internet.
  - Unauthorized or suspicious connections between network segments within the OT network, including non-Internet Protocol (IP) connections.
  - Configuration changes to OT assets
  - **Other tactics, techniques, and procedures (TTPs) in the MITRE ATT&CK® Framework.**
  - The installation or operation of new or unauthorized applications on ICS/OT assets.
  - The exposure and/or usage of ports, protocols, and services that are not necessary for the operation of ICS/OT assets.

SPECIAL RESOURCE | Protecting Critical Water Systems with the Five ICS Cybersecurity Critical Controls[5]

SANS Whitepaper By Dean Parsons

ICS CYBERSECURITY CRITICAL CONTROL NO. 3: ICS Network Visibility and Monitoring

To maximize benefits across ICS security, safety, asset identification, vulnerability detection, operational reliability, and engineering troubleshooting, this control requires active involvement of trained ICS-specific cybersecurity analysts. Essential for real returns on investment and water system safety, those using the control must understand the overall water facility operations, including the common ICS protocols found in water and wastewater environments (DNP3, ModbusTCP, OPC, Profibus, EtherNet/IP and CIP, etc.).

ICS-specific network visibility tools possess advanced capabilities to analyze engineering commands and network interactions between systems, effectively detecting irregularities in water system traffic and alerting to unauthorized access and cyber attacks.

Logging, auditing and monitoring systems, and employing independent process monitoring are valuable network traffic and communications detection methods. Furthermore, by establishing a security operations center (SOC) and integrating an ICS/OT focus into the SOC, utilities are better able to leverage monitoring tools and detection methods to proactively defend ICS/OT networks.

One significant advantage with monitoring a control system is the relatively stable hardware design and network traffic patterns. This stability results in a baseline of network behavior that monitoring systems can evaluate for changes or anomalies in equipment configurations or activity.

Logging and Auditing

Detailed logs are essential for monitoring system, application, and network activity. Without sufficient logs, the ability to detect and respond to cyber incidents is exceedingly hindered. Properly configured logs enable utilities to conduct thorough root-cause analyses to find the source of issues or suspicious activity. Once enabled, logs are often collected and aggregated into a security information and event management (SIEM) system for real-time analysis and correlation. SIEMs ingest event logs from systems like firewalls, VPNs, intrusion detection systems and intrusion prevention systems, antivirus software, proxy servers, end-user devices, servers, and applications.

While utilities may enable logging on capable devices, many fail to aggregate relevant logs to a centralized log management system or SIEM for correlation and analysis. Likewise, even though logging may be enabled, many neglect to **regularly review (audit) the logs** for unusual and suspicious activity for remediation or mitigation. Continuous auditing of logs allows utilities to discover unauthorized activity before it's too late.

CPG | 2.T Log Collection

Access- and security-focused (e.g., IDS/IDPS, firewall, DLP, VPN) logs are collected and stored for use in both detection and incident response activities (e.g., forensics). Security teams are notified when a critical log source is disabled, such as Windows Event Logging.

Operational Technology (OT): For OT assets where logs are non-standard or not available (e.g., legacy devices), network traffic and communications to and from logless assets is collected.

5 https://www.sans.org/white-papers/protecting-critical-water-systems-five-ics-cybersecurity-critical-controls/

CPG | 2.U Secure Log Storage

Logs are stored in a central system, such as a security information and event management (SIEM) tool or central database, and can only be accessed or modified by authorized and authenticated users. Logs are stored for a duration informed by risk or pertinent regulatory guidelines.

Monitoring

Many commercial ICS-specific cybersecurity monitoring tools and platforms are available. These tools can provide control system inventories, detect unauthorized connections – including mobile devices – and spot potentially malicious activity. Non-commercial and open-source software is also available to provide similar monitoring. Both commercial and non-commercial monitoring technology will ingest network traffic for monitoring by either taking a direct data feed from a "span" port on a network switch or using network taps, which make a copy of data traversing a network cable.

For Consideration

While non-commercial low-cost or open-source solutions are an option, they will likely require more in-house technical administration to configure and maintain than a commercial solution with an available support contract. Implementing a cybersecurity monitoring capability involves much more than the acquisition of the technology – this is not a "set it and forget it" endeavor. Planning for knowledgeable personnel to review the monitoring data and technical staff to maintain the technology must be considered. It also important to note that the alert information that is sent from cybersecurity monitoring technologies will require a knowledgeable analyst to interpret and analyze the information to determine the severity, applicability, potential impact, and appropriate response.

Passive, Active, or Hybrid Monitoring

ICS monitoring solutions are either passive, active, or hybrid. *Passive monitoring* is essentially eavesdropping on the network and hoping to get useful information. Passive monitoring is considered non-intrusive and does not impact OT device operations, making it less risky. However, passive monitoring does require the interpreting of ICS/OT system operations and threats by dissecting and analyzing data communications over the wire between assets in the environment. In other words, passive technology requires the capability to understand the myriad of communication protocols used in each environment and the ability to inspect those communication packets for suspicious activity. Passive monitoring limitations include not being able to provide detailed endpoint data like software/firmware versions unless that data is present in network communications in an ingestible format.

Active monitoring involves directly scanning or polling the network and devices with requests for specific information. Due to direct polling, active monitoring can provide more granular details like software, configurations, and vulnerabilities. Some solutions are also able to perform active blocking/response actions. Active monitoring carries more risk due to the potential disruption of sensitive OT devices and processes, but this method also provides more complete data than passive monitoring.

Hybrid monitoring ostensibly offers the best of both world by combining passive and active techniques. Hybrid monitoring provides some benefits of active monitoring without some of the potential risks historically experienced in ICS/OT environments by active solutions.

Fundamentally, passive monitoring is considered well-suited for initial discovery and baselining OT networks, while active monitoring provides deeper endpoint details. A hybrid strategy balancing both techniques is often recommended for comprehensive ICS/OT cybersecurity monitoring. Additionally, once a detection solution is implemented, monitoring and analysis can be performed in-house by a security operations center (SOC) or outsourced to a managed security service provider (MSSP).

Practical Application

Independent Monitoring of Critical Instrument Values

If an adversary gains access to a control system, they can hide malicious activity by registering false readings on the control system displays. Utilities can counter this by identifying the most important process readings, such as a particular tank or wet well level, the pressure at an important distribution system location, or a specific water treatment chemical concentration. These critical measurement points can be monitored independently from the control system by connecting their milliamp signals to independent data loggers with real-time reporting and alerting. If the instrument is connected to a communications protocol that could be compromised, a separate instrument should be installed and monitored by the data logger.

In the event of a normal water or wastewater system problem, both the process control system alarms and the independent data logger alarms should trigger. If only the data logger alarms trigger, that could indicate a problem with the instrument, control system, or an active cybersecurity incident. Operations staff can check the alarm comparison manually and investigate discrepancies. Another approach is to establish automated divergence alarms outside of the control system for when the two instrument values exceed a predetermined value.

Host-based vs. Network-based Monitoring

Host-based and network-based cybersecurity monitoring are two fundamental approaches to protecting information systems. Host-based monitoring involves the event information available on individual devices or servers, including the deployment of security tools directly on them. Host-based monitoring allows for the close examination of system activities, such as file modifications, process activities, and system logs on the devices themselves. Host based logging provides detailed visibility into the actions on each host, enabling the detection of threats that might bypass network defenses, such as insider threats or malware that doesn't generate network traffic.

On the other hand, network-based monitoring focuses on the analysis of data flowing across the network. It uses tools like intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor traffic for signs of malicious activity. The key benefit of network-based monitoring is its ability to provide a broader view of traffic patterns and potential threats, including those targeting multiple hosts. Both approaches are complementary: host-based monitoring excels at in-depth, localized security, while network-based monitoring offers a wider perspective on external and lateral movement threats. Together, they form a comprehensive security posture that helps organizations detect and respond to a wide array of cybersecurity threats.

Security Operations Center

Ultimately, a utility without a security operations center (SOC) lacks the ability to quickly investigate or respond to suspicious activity and potential threats. One of the primary capabilities of a SOC is to gather, correlate and analyze network, host, and application security events. Analysis is typically aided through SIEMs and other event detection technologies that provide an interface for detecting and alerting on anomalous activity, indicators of compromise, and adversary behaviors.

Building an ICS/OT-centric SOC or incorporating ICS/OT-specific functions into an existing SOC, must combine the people, processes, and technology necessary to detect and prevent an ICS/OT impacting cyber incident. According to Dragos, building specialized industrial SOC competencies and toolsets and integrating them into a broader enterprise SOC program can create a defensible architecture and accelerate readiness for OT cybersecurity risks. However, that integration is not without its challenges.[6]

6 https://www.dragos.com/blog/bridge-ot-it-cybersecurity-gap/I

SMALL SYSTEMS GUIDANCE

OT threat detection and monitoring is important for small utilities and shouldn't be overlooked. However, there are many small utilities that still lack threat detection and monitoring on the IT network. IT threat detection and monitoring is equally important and small systems may find it a more straightforward endeavor to gain visibility before embarking on OT monitoring. Nonetheless, both IT and OT monitoring are important, and it would be practical to consider implementing them at the same time.

While log collection (CPG | 2.T) is **more costly** and **complex (medium)** to implement, CISA has a free resource to assist. *Logging Made Easy* (LME)[7] is a viable solution for small utilities with limited IT security tools and resources seeking a no-cost logging service. LME is a reliable, centralized log management alternative. **LME serves as a SIEM tool, tailored to organizations currently lacking this pivotal capability.** LME equips even the most vulnerable entities with the means to swiftly detect and respond to suspicious activity. At the time of this writing, LME only covers Windows-based devices and is limited to on-premises networks with an Active Directory.

Likewise, another resource to assist with logging is the *Host-Based Logging Guidance: Instructions for Managing Windows Event Logs* from Dragos OT-CERT.[8] Members of OT-CERT have access to a two-part series that provides more understanding and recommended practices for host-based logging. The resource includes guides (documents) and jump-start videos that provide detailed technical "how-to" information for implementing a reasonable level of centralized logging in Windows domain environments. Part 1 covers a recommended set of specific Windows event logs to monitor and the process to create a custom filter view to review the logs. Part 2 includes a technical how-to for configuring each Windows device in the domain to forward its logs to a centralized log collection server.

Recommended Practice

In addition to host-based logging, small systems are encouraged to log events from secure email gateways (SEGs). Logging email events is vital for detecting unauthorized access, data breaches, and compliance, as well as for troubleshooting, forensic analysis, and incident response.

Practical Goal

When bolstering ICS/OT monitoring and threat detection, smaller systems should consider planning for future capacity. According to the U.S. Department of Energy, the bare minimum devices that should be monitored in an ICS/OT environment are:[9]

Programmable Logic Controllers (PLCs) and other field devices that directly control physical processes. These devices are critical as they can be targeted by attackers to cause physical damage or disruption.

Human-Machine Interfaces (HMIs) and operator stations that allow personnel to monitor and control the ICS/OT systems. Monitoring these devices can detect unauthorized access attempts.

Supervisory Control and Data Acquisition (SCADA) servers and Distributed Control System (DCS) controllers that manage and coordinate the overall control system. Monitoring these central components is essential for detecting anomalous activity.

Network switches, routers, and firewalls that interconnect the various ICS/OT components. Monitoring network traffic can reveal unauthorized access, malware communication, and other suspicious activity.

Engineering workstations used to program and configure the ICS/OT devices. Monitoring these workstations can detect unauthorized changes to the control system configurations.

Domain controllers and authentication servers that manage user accounts and permissions in the ICS/OT environment. Monitoring these servers can detect credential misuse and unauthorized access attempts.

The monitoring should focus on detecting unauthorized access, malware, and anomalous behavior that could indicate a cyber attack. The monitoring solution should be tailored to the specific ICS/OT environment and integrate with ICS protocols and communications.

7 https://www.cisa.gov/resources-tools/services/logging-made-easy
8 https://www.dragos.com/community/ot-cert/
9 https://www.energy.gov/ceser/considerations-icsot-cybersecurity-monitoring-technologies

Maintaining Awareness of the Threat Environment

Following threat and analysis reports provided by WaterISAC, CISA, FBI, and others is an effective way to maintain awareness of critical infrastructure threat trends. These reports often include threat actors' tactics, techniques, and procedures (TTPs), behaviors, and other indicators of compromise (IoCs) to help detect known intrusion activity within your environment. Smaller utilities may find it useful to follow WaterISAC for the most relevant threats to water and wastewater utilities and are strongly encouraged to pass along the information to systems integrators and other third-party support to assist with detection and protection.

RECOMMENDED RESOURCES

The Five ICS Cybersecurity Critical Controls | SANS Institute

ICS Cybersecurity Field Manual Series | SANS Institute

Dragos Community Defense Program (CDP) | Dragos

Logging Made Easy | CISA

Considerations for ICS/OT Cybersecurity Monitoring Technologies | Department of Energy

Bridging the IT-OT Cybersecurity Gap: Strengthening OT Cybersecurity with Advanced SOC Capabilities | Dragos

Detecting OT Cybersecurity Threats Using the Known-Unknown Matrix | Nozomi Networks

MITRE ATT&CK® Framework | MITRE Corporation

MITRE ATT&CK® Matrix for ICS | MITRE Corporation

5 Account for Critical Assets

WHY THIS IS IMPORTANT: By identifying, inventorying, classifying, and documenting the most critical ICS/OT assets, utilities can prioritize and allocate security resources effectively to protect those assets from potential threats, attacks, or failures that could disrupt operations or cause safety incidents.

Critical assets could include, but are not limited to, sensors, actuators, variable frequency drives (VFDs), circuit breakers, automatic transfer switches (ATSs), critical skid systems, programmable logic controllers (PLCs), human machine interfaces (HMIs), distributed control systems (DCSs), SCADA systems, remote terminal units (RTUs), data radios, industrial control software, industrial firewalls and other security appliances, domain controllers, and critical databases.

Internet of things (IoT) and industrial internet of things (IIoT) within in the control system environment must also be considered.

Identifying assets is one of the foundations of a cybersecurity risk management strategy. Most frameworks and seminal guidance resources prominently list asset inventory. Even the 2019 version of this publication included "Perform Asset Inventories" as the #1 fundamental leading with the cliché, *'you can't protect what you don't know you have.'* However, it has been argued[1] that you *can* protect what you don't know you have. In this argument, industrial cybersecurity expert Dale Peterson uses the illustration of a safe deposit box.

> *"You may not know what is in that box or drawer, and yet its contents are protected by the physical security of the building, office, and box or drawer."*
>
> – Dale Peterson

Despite Dale's contention, he does submit that "*You Can Provide Better Protection If You Know What You're Protecting.*" OT network defenders do need to know which assets are on their networks and what information those assets provide. But as Dale eludes,[2] the juice may not be worth the squeeze regarding the amount of information we need to *know*. Additionally, because such cybersecurity guidance is written to cover multiple critical infrastructure sectors, not only water/wastewater systems, this guidance is often more applicable to other sectors with larger, more complex OT environments.

CPG | 1.A Asset Inventory

Maintain a regularly updated inventory of all organizational assets with an IP address (including IPv6), including OT. This inventory is updated on a recurring basis, no less than monthly for both IT and OT.

It is highly recommended for cyber mature utilities to undertake a more comprehensive asset management strategy for all IT, OT, and internet connected (IoT, IIoT, etc.) assets as outlined in the CPGs, IEC 62443-2-1, NIST Cybersecurity Framework, CIS Controls, and other authoritative guidance. Such an all-encompassing asset strategy greatly enables things like more efficient incident response and recovery, forensic investigations, vulnerability management, network security monitoring, etc.

1 https://dale-peterson.com/2023/11/14/wrong-you-cant-protect-what-you-dont-know/
2 https://dale-peterson.com/2023/11/21/part-2-what-does-know-mean/

Recommended Practice

The IEC 62443 standards emphasize that having a comprehensive, actively maintained asset inventory is crucial for enabling effective risk assessments, vulnerability management, patch management, incident response, and overall cybersecurity management within ICS/OT environments. The asset inventory should provide real-time visibility into all components, configurations, and interdependencies to support robust security controls and ongoing lifecycle management as per the IEC 62443 framework.

While the following CPGs map well to this Fundamental, given the greater cost and complexity to automate with technology, smaller systems may not find them as practical. In those cases, manual asset inventory process should be acceptable, as long as they are updated periodically (see Small Systems Guidance section below).

CPG | 2.0 Document Device Configurations

Organizations maintain accurate documentation describing the baseline and current configuration details of all critical IT and OT assets to facilitate more effective vulnerability management and response and recovery activities. Periodic reviews and updates are performed and tracked on a recurring basis.

CPG | 2.P Document Network Topology

Organizations maintain accurate documentation describing updated network topology and relevant information across all IT and OT networks. Periodic reviews and updates should be performed and tracked on recurring basis.

CPG | 2.Q Hardware and Software Approval Process

Implement an administrative policy or automated process that requires approval before new hardware, firmware, or software/software version is installed or deployed.

- Organizations maintain a risk-informed allowlist of approved hardware, firmware, and software that includes specification of approved versions, when technically feasible.
- For OT assets specifically, these actions should also be aligned with defined change control and testing activities.

Asset Inventory Database

An accurate and comprehensive asset inventory is much more than a list of devices. Data, processes, personnel, supporting infrastructure, and dependencies to other systems should also be identified. An asset repository should include all components on the IT and OT networks and in the field, including third party and legacy equipment. The inventory record should be granular enough for appropriate tracking and reporting. Details should include but not be limited to asset owner, location, vendor, device type, model number, device name, hardware/firmware/software versions, patch levels, device configurations, active services, protocols, network addresses, asset value and criticality. Furthermore, an asset inventory is not a singular task, but an ongoing process. One approach to keeping the asset inventory current is to incorporate it into change management processes.

Unauthorized Assets

Performing an inventory will help reveal blind spots by identifying things that do not belong, such as a rogue wireless access point or other unapproved devices or connections. Inventories also illuminate processes and procedures that could enable the detection of unauthorized configuration changes or other anomalies within the environment.

Obsolete Devices

The Canadian Centre for Cyber Security offers guidance on managing obsolete equipment and the importance for owners/operators to take a proactive approach in the planning for the replacement of ICS/OT systems and components well before they become obsolete. If a replacement strategy is not feasible, then a minimum set of mitigation measures should be in place to protect these systems.

For Consideration

ICS/OT product obsolescence mitigation plan:[3]

- Backup and spares policies that account for non-availability of replacement products due to market conditions.
- Programs to ensure sufficient in-house resources are available and trained to rebuild systems to a known-good configuration.
- Best practices for how to secure products requiring internet/cloud/wireless connectivity.
- Approved vetting process to select vendors that provide proactive lifecycle planning, especially Mean Time Between Failures (MTBF) estimates as well as advance notice of End of Support (EOS) dates.
- Required security controls to implement before the EOS date to protect the ICS/OT networks.

Physical Inspection

An asset inventory would be incomplete without physical inspection. Network scanning methods reveal what is connected to the network at the time of the scan but may not readily account for disconnected devices that could be connected later, such as rogue or wireless devices. Additionally, a network diagram showing the relative physical locations, criticality, and roles of the assets is essential for effectively documenting the system.

SANS ICS Cybersecurity Field Manual Vol. 2[4]

Physical Inspection: This involves physically walking through industrial facilities, documenting the hardware seen in racks and network cabinets, inspecting the software and protocols used, and taking other proactive steps. Physical inspection is time consuming and expensive if it involves traveling to remote sites. Some potential physical risk exists, so PPE will be required at sites.

Vital Data

Not only is asset inventory data a foundation for cyber defense, it is also vital information for incident response (Fundamental 1) and vulnerability management (Fundamental 9).[5] In the same way asset inventory and network diagram documentation are of paramount importance to the asset owner, they are also very attractive to an adversary. Hence, this information needs to be as rigorously protected as the ICS/OT system itself (Fundamental 7).[6]

3 https://www.cyber.gc.ca/en/guidance/obsolete-products-itsap00095
4 https://www.sans.org/mlp/ics-resources/
5 Fundamental 9 | Embrace Vulnerability Management is scheduled to be released in September 2024
6 Fundamental 7 | Safeguard from Unauthorized Physical Access is scheduled to be released in September 2024

SMALL SYSTEMS GUIDANCE

As previously stated, most authoritative cybersecurity guidance leads with some sort of asset management strategy. CISA's *Cross-Sector Cybersecurity Performance Goals* (CPGs)[7] include *Asset Inventory* as the first goal, **1.A**. While this CPG assesses asset inventory as a high-impact outcome, when using automated tools, it's not low-cost (**$$**$$) or low-complexity (**medium**) to implement. Despite the high-impact outcome toward risk reduction, the medium-complexity and cost to implement is above the threshold of this guide's suggestions for small systems, hence the emphasis is placed on a more practical approach of managing the most critical assets with the intent to scale in the future. That said, as the majority of water and wastewater systems in the U.S. have a relatively small number of assets, **managing asset inventories can be done effectively via manual processes such as using a spreadsheet and network drawings that are updated on a periodic basis and/or when new systems are added or upgraded.** Manual asset inventory processes can also be augmented with periodic validation using network traffic capture analysis and other automated discovery tools as point in time validations.

Practical Application

In many cases, third parties can be an important part of understanding and documenting OT assets. For example, systems integrators, design engineers, and OT asset programmers can possess deep knowledge of how an OT system is constructed and the composition of assets. A possible way to capture that knowledge is to include a line item in a scope of work requiring a detailed asset inventory as part of the deliverables. It is often the case that multiple third parties will have varying scope on a given project and so a contribution from each is required to build a complete asset inventory that should include all relevant hardware, software, and data.

For Consideration

The *SANS ICS Cybersecurity Field Manual Vol. 2*[8] outlines a practical example to establishing an ICS asset inventory.

1. Start by reviewing any already-created network diagrams and engineering documentation such as "as-built documents."
2. Use an encrypted laptop with at least a basic spreadsheet application to start cataloging and storing ICS asset information during a physical site walk through, as seen below in Table 1: Sample Asset Inventory Attributes.
3. Augment physical inspection with passive network packet captures on critical network segments that host critical ICS assets by using either a SPAN or mirrored port configuration off a fully managed switch or hardware TAP.
4. Ensure field device configurations are backed up during an incident and securely stored for later comparison to detect whether an unauthorized change occurred and reload trusted configurations and project files (controller logic), if needed.
5. At a minimum, record attributes from the commonly targeted critical assets such as data historians, HMIs, PLCs, RTUs, engineering workstations, core network devices, and active safety instrumented systems.

Table 1: Sample Asset Inventory Attributes

Sample Asset Inventory Attributes
Site location
Facility type
Asset type and ID tag
Asset location room, cabinet, rack
Description of asset function for operations
Impact to operations if assets are unavailable
IP and MAC address
Network protocols used
Model, manufacturer, serial number
Firmware version for controllers and related modules, chassis information
Applications installed on critical assets with versions
Assets deemed critical – data historians, HMIs, primary controllers, control system network switches
Project files and configuration (last change date, secure storage location, etc.)
Dependencies – systems, networks, other assets, etc.
Primary and secondary contact for asset

7 https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
8 https://www.sans.org/mlp/ics-resources/

Additionally, for quick jump-start on the asset inventory, Dragos OT-CERT[9] members have access to the *OT Asset Inventory Template* and *OT Asset Inventory Guide*. The template is a spreadsheet that plant engineers can begin using immediately to develop or refresh an asset inventory. The *OT Asset Inventory Guide* explains how to use the complementary *OT Asset Inventory template*.

Hot, Warm, or Cold Standby Components

In many cases, cyber resilience can be bolstered with the use of standby devices. For example, a critical controller or HMI can be duplicated in both hardware and configuration, then disconnected from the network, and maintained in either a powered or unpowered state. This "offline" cold or warm standby asset will provide resilience for multiple failure modes including cyber incidents.

Practical Application

In the event of a cyber incident, once the threat is contained or mitigated, it is feasible that normal operations can be restored by replacing affected assets with the presumably non-compromised backup device. **An important aspect of this approach is to include updates to backup devices as part of the change management process.** In the case of the HMI, the cold backup can simply be a cloned copy of the hard drive that can be swapped out as part of the incident response procedure. There are considerations here regarding software licensing, malware that could infect other non-volatile memory in an asset, etc.; however, those are details that can typically be considered on a case-by-case basis.

RECOMMENDED RESOURCES

Understanding OT/ICS Asset Discovery: Passive Scanning vs. Selective Probing (Ralph Langner)

Wrong: "You Can't Protect What You Don't Know" | Dale Peterson

Part 2 – What Does "Know" Mean? | Dale Peterson

Part 3: Creating An OT Asset Inventory | Dale Peterson

OT Asset Management in 2024: A product category in its own right | Ralph Langner

Censys

Shodan

Shodan's API For The (Recon) Win! | SANS Internet Storm Center

7 Steps to Start Searching with Shodan | DarkReading

Industrial Internet of Things Safety and Security Protocol | WEF

Securing the Industrial Internet of Things: Cybersecurity for Distributed Energy Resources (Draft) | NIST (NCCOE)

Guidelines for Managing the Security of Mobile Devices in the Enterprise - SP 800-124 Rev. 2 | NIST

Mobile Device Security: Cloud and Hybrid Builds – SP 1800-4A | NIST

Baseline Security Recommendations for IoT - in the context of Critical Information Infrastructures | ENISA

Good practices for Security of Internet of Things in the context of Smart Manufacturing | ENISA

Water/Wastewater Utilities Leveraging IIoT | IIoT World

Industry IoT Consortium

9 **https://www.dragos.com/community/ot-cert/**

6 Enforce Access Controls

WHY THIS IS IMPORTANT: Maintaining strict access controls play a crucial role in protecting resources, data, and systems from unauthorized access, ensuring confidentiality, integrity, availability, and safety. Access controls should be enforced for users and devices. Security measures such as the separation of privileged accounts and zero-trust architectures help prevent unauthorized access and limit lateral movement.

Access control involves providing control system access only to those individuals who are authorized to have it. Restricting access to select individuals limits the number of people who can interact with key systems. When logging and auditing is enabled (Fundamental 4), this restriction also makes it much easier to detect suspicious and unauthorized access. Audit logs identify credentials associated with accidental, unapproved, or misconfiguration changes. The fewer credentials that have access, the more focused an investigation can be. Some important components of access control include role-based controls, principle of least privilege, zero trust, strong authentication, and off-boarding.

Role-Based Access Control

Role-based access control (RBAC) grants or denies access to systems or network resources based on job functions or responsibilities. This control limits the ability of individual users – or attackers – to reach files or parts of the system they should not access. For example, SCADA system operators likely do not need access to the billing department or certain administrative files. Therefore, define permissions based on the level of access each job function needs to perform its duties. In addition, limiting employee permissions through RBAC can facilitate tracking network intrusions or suspicious activities during an audit.

For Consideration

Executives, directors, IT administrators, cybersecurity, software developers, finance, human resources, and SCADA operators are examples of roles that typically involve higher levels of account and resource access that need to be further scrutinized. No matter how "senior" a role, or how much tenure someone has, anyone can intentionally or unintentionally use privileged access in a manner that negatively impacts your utility.

Principle of Least Privilege

Similar to RBAC is the principle of least privilege. By applying the principle of least privilege to a user account, only the absolute minimum permissions necessary to perform a required task are assigned. In other words, administrative or other privileged accounts are reserved for special use and are not to be logged in perpetually. Most malware operates with permissions of the logged in user. By granting access and permissions based on roles and least privilege, malware has limited access to the resources it can compromise.

CPG | 2.E Separating User and Privileged Accounts

No user accounts always have administrator or super-user privileges. Administrators maintain separate user accounts for all actions and activities not associated with the administrator role (e.g., for business email, web browsing). Privileges are reevaluated on a recurring basis to validate continued need for a given set of permissions.

While the least-privilege approach is a defense against many types of malware, unpatched vulnerabilities can still be exploited to elevate privileges regardless of user access rights. Therefore, it is important to maintain an effective patch management regimen (Fundamental 7) to reduce vulnerabilities that could lead to privilege escalation attacks.

Zero Trust

Zero trust is a security model that assumes no user, device, or network is inherently trusted and requires continuous verification and validation before granting access. Implementing Zero Trust principles in OT environments presents unique challenges due to the distinct nature of OT systems.

Implementing Zero Trust principles across OT networks helps with challenges, such as:[1]

- Controlling remote connections into OT systems, securing network jump hosts, and preventing lateral movement across the network.
- Reviewing and reducing interconnections between dependent systems, simplifying identity processes, such as for contractors signing into the network.
- Finding single points of failure in the network, identifying issues in specific network segments, and reducing delays and bandwidth bottlenecks.

For more on Zero Trust, refer to **Fundamental 2 | Minimize Control System Exposure**

Strong Authentication

In June 2017, NIST updated its password guidance to reduce the burden on the end user in an effort to improve password hygiene. While maintaining security, the current guidance seeks to reduce complexity requirements and encourage more user-friendly password policies. NIST updated the password guidelines to generally allow for longer passwords without the special character complexity restrictions. Essentially, this increased length and reduced complexity enables users to create longer but more memorable passwords or passphrases that are more difficult to crack. NIST also advises that requiring users to change their passwords regularly makes memorizing them difficult and makes it more likely users will record their passwords in an unsafe manner.

Longer is Stronger

Malicious actors use readily available software tools to effortlessly crack simple passwords or millions of known character combinations to attempt unauthorized logins. These are called "dictionary" and "brute force" attacks. In addition, users often make common character substitutions or additions that have become predictable, and those variations have been added to the brute force/dictionary tools. To keep systems and information secure, enforce the use of longer passwords or passphrases that accommodate any ASCII printable character, and unique passwords for each account. Use password management software to keep track of and create multiple passwords.

CPG | 2.B Minimum Password Strength

Organizations have a system-enforced policy that requires a minimum password length of 15* or more characters for all password-protected IT assets, and all OT assets where technically feasible.**

- Organizations should consider leveraging passphrases and password managers to make it easier for users to maintain sufficiently long passwords.
- In instances where minimum password lengths are not technically feasible, compensating controls are applied and recorded, and all login attempts to those assets are logged.
- Assets that cannot support passwords of sufficient strength length are prioritized for upgrade or replacement.
- This goal is particularly important for organizations that lack widespread implementation of MFA and capabilities to protect against brute-force attacks (such as web application firewalls and third-party content delivery networks) or are unable to adopt passwordless authentication methods.

* Modern attacker tools can crack eight-character passwords quickly. Length is a more impactful and important factor in password strength than complexity or frequent password rotations. Long passwords are also easier for users to create and remember.

** OT assets that use a central authentication mechanism (such as Active Directory) are most important to address. Examples of low-risk OT assets that may not be technically feasible include those in remote locations, such as on offshore rigs or wind turbines.

Unique Credentials

Countless breaches and data leaks continue to prove that the same leaked information keeps turning up over and over in giant data sets of stolen credential dumps that are widely accessible. These credential dumps are then used by cyber criminals in attempts to gain access to accounts by patiently stuffing these stolen credentials into various web sites and services. When passwords are reused across multiple sites, only one set of leaked credentials will unlock the keys to the entire kingdom.

1 https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/concept-zero-trust

CPG | 2.C Unique Credentials

Organizations provision unique and separate credentials for similar services and asset access on IT and OT networks. Users do not (or cannot) reuse passwords for accounts, applications, services, etc. Service accounts/ machine accounts have unique passwords from all member user accounts.

The best solution (MFA notwithstanding) to creating unique credentials is consistent use of password managers. Password managers can be used to create long and strong passwords to reduce some of the most common password pitfalls – simple password creation, password reuse, password predictability, and passwords on **Post-it®** notes.

For Consideration

PASSWORD MANAGER ADVANTAGES[2]

Password managers not only let you manage hundreds of unique passwords for your online accounts, but some of the services also offer other advantages:

- Saves time
- Works across all your devices and operating systems
- Protects your identity
- Notify you of potential phishing websites
- Alerts you when a password has potentially become compromised

Using unique credentials for every account or system access is a fundamental cybersecurity practice. Unique credentials are crucial safeguards against widespread account compromise, credential stuffing attacks, and unauthorized access.

Multifactor Authentication

Multifactor authentication (MFA) decreases the risk that an adversary could log in with stolen credentials. Organizations should consider requiring MFA by verifying identity when each user attempts to log in. Common MFA methods include biometrics, smart cards, FIDO2 (Fast IDentity Online) enabled hardware devices, or one-time passcodes sent to or generated by previously registered devices.

CPG | 2.H Phishing-Resistant Multi-Factor Authentication (MFA)

Organizations implement MFA for access to assets using the strongest available method for that asset (see below for scope).

MFA options sorted by strength, high to low, are as follows:

1. Hardware-based, phishing-resistant MFA (e.g., FIDO/WebAuthn or PKIbased).
2. If such hardware-based MFA is not available, then mobile app-based soft tokens. (preferably push notification with number matching) or emerging technology such as FIDO passkeys are used.
3. MFA via SMS or voice only used when no other options are possible.

IT: All IT accounts leverage MFA to access organizational resources. Prioritize accounts with highest risk, such as privileged administrative accounts for key IT systems.

OT: Within OT environments, MFA is enabled on all accounts and systems that can be accessed remotely, including vendors/ maintenance accounts, remotely accessible user and engineering workstations, and remotely accessible human-machine interfaces (HMIs).

MFA fatigue. Despite the benefits, cyber threat actors use multiple techniques to bypass MFA. A popular technique is MFA fatigue, also known as MFA prompt bombing. MFA fatigue is the process of sending a high volume of push requests in short succession to a target's mobile device until the user accepts the authentication request, either by accident or to quell the repeated push notifications.

The important bit about MFA fatigue, perhaps more important than the potential victim accepting an unauthorized push request, is that the **threat actor already has the target user's valid credentials** which are required to prompt for the push in the first place.

2 https://staysafeonline.org/online-safety-privacy-basics/password-managers/

> *"Call the employee 100 times at 1 am while he is trying to sleep, and he will more than likely accept it. Once the employee accepts the initial call, you can access the MFA enrollment portal and enroll another device."*
>
> – According to a message captured from Lapsus$ Telegram channel

To combat MFA fatigue and other MFA bypass tactics, CISA strongly urges organizations to implement phishing-resistant MFA as part of applying Zero Trust[3] principles. While any form of MFA is better than no MFA and will reduce an organization's attack surface, phishing-resistant MFA is the gold standard and organizations should make migrating to it a high priority effort.[4]

No Default Passwords

When new devices or software are installed, it is imperative to change all default passwords, particularly for administrator accounts and control system devices. Many factory default passwords are widely known and discoverable through a simple Google or Shodan search. In addition, implement other password security features, such as an account lock-out that activates after too many incorrect password attempts. Likewise, MFA should be implemented wherever possible. However, for devices that don't support MFA, such as many control systems, use the strongest (longest, highest complexity) password the device will allow.

CPG | 2.A Changing Default Passwords

An enforced organization-wide policy and/or process that requires changing default manufacturer passwords for any/all hardware, software, and firmware before putting on any internal or external network. This includes IT assets for OT, such as OT administration web pages.

- In instances where changing default passwords is not feasible (e.g., a control system with a hard-coded password), implement and document appropriate compensating security controls, and monitor logs for network traffic and login attempts on those devices.

OT: While changing default passwords on an organization's existing OT requires significantly more work, CISA still recommends having such a policy to change default credentials for all new or future devices. This is not only easier to achieve, but also reduces potential risk in the future if threat actor TTPs change.

3 https://zerotrust.cyber.gov/federal-zero-trust-strategy/#identity
4 https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

Exploitation of Default Passwords on Unitronics PLCs Across the U.S. Water and Wastewater Sector by CyberAv3ngers[5]

A series of attacks which largely began in November 2023 with news that a small water authority in Western Pennsylvania was the first to be impacted by a threat group known as CyberAv3ngers.

What happened: In late November 2023, the **Municipal Water Authority of Aliquippa** in western Pennsylvania was **attacked by an Iranian-backed cyber group known as CyberAv3ngers**. The water authority reported the actors were able to gain control of a remote booster station serving two townships, but stressed there was no known risk to the drinking water or water supply. An alarm reportedly went off as soon as the attack occurred. The system had been disabled and was operated manually. The compromised device was identified as a Unitronics V570 Vision Series PLC.*

**Unitronics PLCs are commonly used in the Water and Wastewater Systems (WWS) Sector and are additionally used in other industries including, but not limited to, energy, food and beverage manufacturing, and healthcare.*

Who did it? This activity is attributed to the Iranian Government Islamic Revolutionary Guard Corps (IRGC)-affiliated Advanced Persistent Threat (APT) cyber actors using the persona "CyberAv3ngers" (also known as CyberAveng3rs, Cyber Avengers). CyberAv3ngers is a threat group purportedly focused on targeting Israeli water and energy sites – including ten water treatment stations in Israel as of Oct. 30, 2023, according to their X page. The group targeted and compromised Israeli-made Unitronics Vision Series PLCs that were **publicly exposed to the internet. This targeting set included several U.S.-based WWS facilities. All impacted devices were compromised using the default password "1111" and default TCP port 20256**. *Note: the PLCs may be rebranded and appear as different manufacturers and company names.*

On December 1, 2023, the FBI, CISA, NSA, EPA, and INCD (Israel National Cyber Directorate) released a joint Cybersecurity Advisory (CSA), **IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities** (Alert Code AA23-335A).[6] **The CSA confirmed multiple investigations into similar activity impacting WWS across multiple U.S. states**. According to the CSA, since at least November 22, 2023, the IRGC-affiliated cyber actors **compromised default credentials in Unitronics devices,** leaving a defacement image on the HMI stating, *"You have been hacked, down with Israel. Every equipment 'made in Israel' is CyberAv3ngers legal target."*

On December 11, 2023, CVE-2023-6448 was assigned to address the default passwords and CISA added the CVE to its Known Exploited Vulnerabilities Catalog. On December 12, Unitronics released VisiLogic version 9.9.00 software to address this CVE with the requirement for users to change default passwords.

5 **https://www.waterisac.org/portal/tlpclear-water-utility-control-system-cyber-incident-advisory-icsscada-incident-municipal**
6 **https://www.cisa.gov/sites/default/files/2023-12/aa23-335a-irgc-affiliated-cyber-actors-exploit-plcs-in-multiple-sectors-1.pdf**

The threat actors attributed to the Unitronics PLC defacements are considered low-skilled actors using unsophisticated tactics who thus far represent a low-impact risk. However, this activity was extremely high-profile and brought enormous and much needed attention to the larger issue of unsecured internet-connected PLCs (especially ones that the default passwords have not been changed) across all critical infrastructure sectors. It is understandable that there are many cybersecurity recommendations that are challenging, impractical, or nearly impossible to implement (such as patching), especially in smaller ICS/OT environments. However, changing default passwords cannot be ignored, especially by smaller systems that likely lack additional controls.

CISA's Secure-by-Design[7] efforts will hopefully make the default password vulnerability an issue of the past. Until then, it's up to asset owners and their advocates, integrators, and other support vendors to make sure default passwords (and ports) do not get deployed in production environments, or worse, directly connected to the internet. Internet exposed PLCs are exceedingly trivial to discover and default passwords are widely known by attackers, making them easy to gain access to. Utilities who outsource SCADA support are urged to **consult with integrators and other support vendors to confirm/insist that this recommended practice is being followed.**

7 **https://www.cisa.gov/resources-tools/resources/secure-by-design**

Off-Boarding Process

Utilities can be proactive in reducing the risk of insider threats from former employees by implementing effective off-boarding (and onboarding) procedures. From recruitment through separation, it's important to establish clear physical and electronic access control policies, employ tools and resources to identify anomalous behaviors, and increase training and awareness activities across the organization to reduce the risk of an insider threat when employees leave.

To protect utility assets from unauthorized access, physical and cyber access should be disabled as soon as it is no longer required. Terminated and voluntarily separated employees, vendors, contractors, and consultants should have access revoked as soon as possible. Likewise, employees transferring into new roles will likely need to have unnecessary access removed.

A rigorous off-boarding procedure should be established with human resources and contract managers, as well as IT and OT staff. The off-boarding procedure should include an audit process to identify disabled and deleted accounts and to confirm appropriate access deprovisioning due to role transfers. The procedure should also incorporate a method to identify any shared accounts, like system administrator, development environment, application, and vendor accounts.

CPG | 2.D Revoking Credentials for Departing Employees

A defined and enforced administrative process applied to all departing employees by the day of their departure that (1) revokes and securely returns all physical badges, key cards, tokens, etc., and (2) disables all user accounts and access to organizational resources.

Effective deprovisioning of departing employees also reduces the risk posed by a former employee becoming an insider threat. As discussed in **Fundamental 3 | Create a Cyber Secure Culture and Protect from Insider Risks**, employees with ongoing access to systems and intent often will do harm if comprehensive termination/off-boarding procedures are not followed to disable access.

Real-World Incident[8]

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.

8 https://www.justice.gov/usao-ks/pr/kansas-man-pleads-guilty-water-facility-tampering

Two of the CPGs discussed in this section (**2.B Minimum Password Strength** and **2.E Separating User and Privileged Accounts**) are considered low cost (**$**$$$) and low complexity to implement and result in a high impact toward risk reduction. Smaller systems are strongly recommended to implement these CPGs.

CPG | 2.B Minimum Password Strength

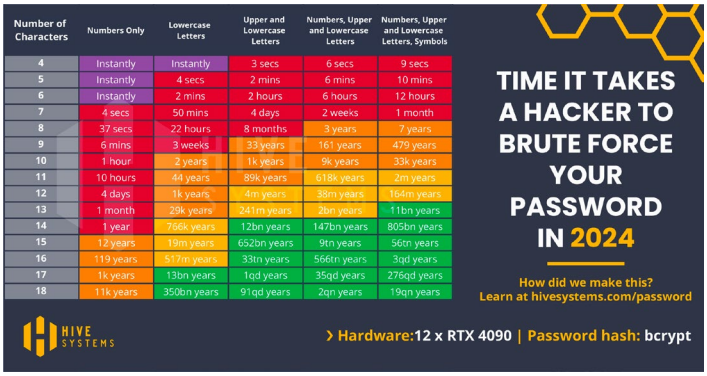
Organizations have a system-enforced policy that requires a minimum password length of 15* or more characters for all password-protected IT assets, and all OT assets where technically feasible.**

- Organizations should consider leveraging passphrases and password managers to make it easier for users to maintain sufficiently long passwords.
- In instances where minimum password lengths are not technically feasible, compensating controls are applied and recorded, and all login attempts to those assets are logged.
- Assets that cannot support passwords of sufficient strength length are prioritized for upgrade or replacement.
- This goal is particularly important for organizations that lack widespread implementation of MFA and capabilities to protect against brute-force attacks (such as web application firewalls and third-party content delivery networks) or are unable to adopt passwordless authentication methods.

* Modern attacker tools can crack eight-character passwords quickly. Length is a more impactful and important factor in password strength than complexity or frequent password rotations. Long passwords are also easier for users to create and remember.

** OT assets that use a central authentication mechanism (such as Active Directory) are most important to address. Examples of low-risk OT assets that may not be technically feasible include those in remote locations, such as on offshore rigs or wind turbines.

Implementing minimum password strength policies in small ICS/OT environments can significantly enhance security without incurring high costs. Utilities should set password strength and complexity requirements and communicate the standard to all staff and contractors. While the recommended minimum password length varies, it is typically accepted to be greater than eight characters, incorporating a mix of upper- and lower-case letters, numbers, and special characters to increase complexity. The following image from Hive Systems[9] denotes the time it takes to brute force a password in 2024.



A critical consideration in adopting standards and requirements for password policies is to understand the capabilities of the devices and software in the specific OT environment and set technically feasible requirements.

CPG | 2.E Separating User and Privileged Accounts

No user accounts always have administrator or super-user privileges. Administrators maintain separate user accounts for all actions and activities not associated with the administrator role (e.g., for business email, web browsing). Privileges are reevaluated on a recurring basis to validate continued need for a given set of permissions.

The concept of least privileged applies to configuring user accounts that allow the given user with least amount of privilege to meet their job requirements. This helps ensure that if their account is compromised, the attacker is limited in the actions they can take without executing additional steps to increase privileges. In some cases, personnel have multiple roles. In those cases, it is recommended that they have multiple accounts for each role that can be utilized accordingly.

9 https://www.hivesystems.com/password

Practical Application

Educating employees on the importance of strong passwords and the risks of using simple or common passwords will help to motivate personnel to comply with password policies where device configurations cannot automatically enforce them. Encourage or mandate the use of free, low-cost, or professional password management tools to help employees generate and store complex passwords securely. **Regularly update and enforce password policies, ensuring that default passwords are changed immediately.** Additionally, conduct periodic audits to ensure compliance and to identify any weaknesses in the password management system.

Practical Application

Use cases for consideration around account privilege for water and wastewater utilities:

HMI Accounts

- *Default Account* – The HMI should boot into and, after inactivity or logoff, return to a default Guest user account with limited privileges to see screens but no capability to change setpoints, acknowledge alarms, etc.
- *Operator Privilege account* – System operators who are users of the HMI but have some limitations for control and alarm changes should have individual accounts with their privilege restrict to operations capabilities within their role only.
- *Senior Operator/Manager privilege account* – Operators and managers with the authorization to change critical operational setpoints and other similar actions, should have individual accounts with capabilities associated with their role.
- *Engineer account* – Engineers who have authorization to make administrative and configuration changes on the HMI should have individual accounts with the capabilities within their role.

OT/IT Department Access

- *User Account:* An IT technician, who uses a regular user account (*name.user*) for daily tasks such as email, documentation, and accessing non-administrative applications.
- *Privileged Account:* For system maintenance, server configuration, or installing software, the technician switches to the privileged account (*name.admin*), which has administrative rights on the network and critical systems.

Database Management

- *User Account:* A database analyst has a lower privileged user account (*name.user*) to run queries, generate reports, and analyze data from the database.
- *Privileged Account:* When the analyst needs to perform database maintenance tasks, such as creating or deleting tables and managing user permissions, the privileged account (*name.dba*) is used.

Finally, while *CPG 2.H, Phishing-Resistant Multifactor Authentication (MFA)*, is not low cost (**$$**$$) or low complexity (medium) to implement, it is practical for small systems to consider for significantly reducing risk. However, due to those same challenges, phishing-resistant MFA may still not be practical for some of the smallest utilities.

As such, CISA recommends enabling "number matching" on MFA configurations to prevent MFA fatigue. Number matching is a setting that forces the user to enter numbers from the identity platform into their app to approve the authentication request.[10]

10 **https://www.cisa.gov/sites/default/files/publications/fact-sheet-implement-number-matching-in-mfa-applications-508c.pdf**

RECOMMENDED RESOURCES

Multi-Factor Authentication (MFA) | CISA

What is FIDO? |FIDO Alliance

Passkeys | FIDO Alliance

CISA Releases Guidance on Phishing-Resistant and Numbers Matching Multifactor Authentication | CISA

Role Based Access Control | NIST

Security and Privacy Controls for Federal Information Systems and Organizations – SP 800-53 Rev. 5 | NIST

Implementing Least-Privilege Administrative Models | Microsoft

Digital Identity Guidelines – SP 800-63-3 | NIST

Exploitation of Unitronics PLCs used in Water and Wastewater Systems | CISA

Zero Trust Maturity Model | CISA

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

Zero Trust and your OT networks | Microsoft

Advancing Zero Trust Maturity Throughout the Visibility and Analytics Pillar | NSA

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

waterisac

waterisac

waterisac.org/fundamentals