WATER ISAC

12 Cybersecurity Fundamentals for Water and Wastewater Utilities

Recommended Practices to Reduce Exploitable Weaknesses and Consequences of Attacks

SEPTEMBER 2024

Fundamental 7 | Safeguard from Unauthorized Physical Access
Fundamental 8 | Install Independent Cyber-Physical Safety Systems
Fundamental 9 | Embrace Risk-Based Vulnerability Management

waterisac.org/fundamentals

7 Safeguard from Unauthorized Physical Access

WHY THIS IS IMPORTANT: Physical security is equally as important as cybersecurity in protecting data, computing, networking, other data center and control systems infrastructure. Weak physical security can undermine cybersecurity efforts, as attackers may exploit physical vulnerabilities to bypass digital defenses. By preventing unauthorized physical access to critical assets, utilities can reduce the risk of theft, tampering, or destruction that could compromise safety. Therefore, it is imperative to limit physical access to IT and OT environments, including communications equipment and assets at remote locations.

There is a common adage, "If you can touch it, you own it." In the context of cybersecurity, this adage serves as a reminder that physical access to devices or systems can lead to unauthorized control or other cyber incidents. It highlights the importance of securing physical assets to prevent malicious actors from gaining access to sensitive information or critical systems. Utilities are encouraged to implement robust physical security measures to safeguard their infrastructure, as unauthorized physical access can compromise even the most secure digital systems.

Gaining Unauthorized Physical Access

Attackers may seek to gain unauthorized physical access for surveillance or other intelligence-gathering activities to facilitate a follow-on attack (physical or cyber). Therefore, it is imperative to limit physical access to restricted areas and networked environments only to those who need it. Non-technical, physical barriers, like fences, barricades, gates, guards, and locked doors should be used to establish a security defense around the physical perimeter of buildings containing IT and ICS/OT equipment. Locked cabinets, cabinet intrusion alarms, and conduits for network cables can be used to further protect IT and ICS/OT equipment and systems from unauthorized physical access and subsequent damage.

The use of identification badges, key cards, cameras, motion detectors, security personnel, and intrusion alarms are often used to preclude unauthorized physical access. However, those methods have limited to no effectiveness against persons who use social engineering methods such as piggybacking/tailgating along with authorized personnel or non-employees who are otherwise treated as "trusted."

Physical infiltration could lead to attackers having direct network access, allowing them to plant remote "hacking" software or hardware tools[1] to be leveraged later in the next phase of an attack.

Social Engineering Methods Used to Gain Unauthorized Physical Access

Attackers interested in accessing your facilities have no qualms about employing social engineering tactics to trick employees into unwittingly granting

Real-World Risk | Publicly Available Information

There is a lot of information on the internet about our water and wastewater systems. It's practical to become familiar with what is accessible/searchable. In some cases, you can work to remove detailed and sensitive information - it takes time and persistence, but it is possible. However, some information is intentionally part of the public record for citizens. We need to be aware of this class of data, so we are not fooled into trusting whoever has it because we believe only privileged sources have access to it.

While it may be difficult to remove some publicly available information, utilities should perform their own reconnaissance to learn what facility and employee information is publicly available. Unnecessary public disclosures should be mitigated.

[1] https://attack.mitre.org/versions/v15/techniques/T1200/

unauthorized physical access. Through social engineering techniques and by combing through social media and the internet, attackers can acquire knowledge of people and processes to create credible ruses to gain physical access to a facility.

We all want to be helpful. Unfortunately, attackers know this and will sometimes take advantage of (social engineer) this part of our human nature. A very common method to gain unauthorized access through a secured entry or restricted area is to piggyback or tailgate someone with valid access. Typically, attackers will employ a ruse by *impersonating* another employee, security guard, or service worker (delivery, utility, etc.). Impersonating IT staff is a particular favorite of attackers. Attackers may also disguise themselves as pregnant (women) or wear high-visibility clothing to create the impression of a public safety officer or other trusted figure.

Real-World Risk | Unescorted Visitors

Many companies' policies state that guests must be escorted by an employee at all times – often easier said than done. From delivery couriers, integrators, contractors, security personnel, janitors, and other professionals that regularly visit our workplaces, we tend to become complacent and trusting. In some work environments it may be an acceptable risk to allow regular/expected visitors to be unescorted, but what about total strangers?

It's important to encourage staff to ask and escort anyone they don't recognize – even if the visitor has a badge – and report unattended strangers they observe in restricted or sensitive areas.

Other physical security considerations to protect from prying eyes:

- **Always lock your workstation** to keep attackers from installing malware or stealing information or credentials.
- **Keep confidential information secure.** Use privacy screens and headphones if necessary and refrain from passwords on Post-it® notes displayed near computers.
- **Implement a clean desk policy** by removing business documents, notes, etc. to avoid sensitive information from being stolen from unlocked desk drawers or filing cabinets.

Physical Security Assessments and Penetration Tests

Physical security is essential in cybersecurity to prevent unauthorized access to sensitive systems and data. By addressing physical vulnerabilities through measures like penetration tests, utilities can ensure that physical and cyber defenses work together to protect critical resources. Conducting physical penetration tests helps identify and address physical security weaknesses, ensuring comprehensive protection. Penetration testing is valuable for discovering physical security gaps that may have been overlooked or lapsed over time.

For Consideration

Utilities are encouraged to perform physical security assessments, penetration tests, or ethical "hacks" of the physical security perimeter at all facilities. Physical penetration tests can be performed alone or in concert with any network-based penetration test engagements as an attempt to breach defenses through on-site physical access. Physical penetration tests are not just to test physical security, but to identify where a physical security breach could also lead to direct IT or OT system or other restricted access.

Physical security assessments evaluate an organization's physical security measures to identify potential risks and vulnerabilities that could compromise the safety and security of its people, assets, and facilities. The assessment typically involves a combination of physical inspections, lockpicking or other lock bypass methods, piggybacking/tailgating, and access control abuse. These methods assist in assessing the effectiveness of existing security measures and identifying areas for improvement. Utilities can use the results of physical penetration tests as part of security training to increase staff situational awareness of physical, environmental, and human vulnerabilities that contribute to physical security gaps.

While social engineering methods prove effective, there are also a lot of inexpensive tools and simple tricks that don't require social engineering humans to gain unauthorized physical access.

Testing Physical Security: Tools and Tradecraft

Hardware vulnerabilities and human error are arguably the most common physical security gaps. Most break-ins are enabled by a combination of both. Physical security is fairly mature today – with things like card readers, cameras, locks, guards, etc. However, physical security controls can still be compromised by social engineering, ineffective installation, a cheap piece of metal, or a can of compressed air.

Real-World Vulnerability | REX (Request-to-Exit) Sensors

These simple, passive, infrared thermal sensors are one of the most common devices seen in buildings all over the world. If you are walking out of a badged area, and you hear a click as you approach the door, can hit a button to exit the door, or do not have to swipe your badge to exit, your environment probably has REX sensors installed.

Vulnerability: Technicians typically install REX sensors in a way to maximize the area in which movement can be detected. While there are several things to keep in mind, such as building code and Americans with Disabilities Act (ADA) regulations, REX sensors are often found to be insecurely installed. The problem is that REX sensors are often installed too close to a door frame, which leads to the ability to activate the sensor from the wrong side of the door. We have seen some that could be activated by pushing a thin item (printer paper, envelopes, etc.) through a gap in the door. The most common method is a can of compressed air. Turn it upside down and spray some cold air toward the sensor. Your $200 REX sensor/magnetic lock setup can be bested by an inexpensive can of compressed air.

Remediate: This one is, admittedly, a bit tricky. Turning the sensor so that it is not directly accessible from the wrong side of the door is a good way to mitigate this issue. The addition of static charge push bars or installing a pressure-sensitive mat on the secured side of the door is another way to add additional security.

Further details on this example and several more can be found at TrustedSec.[2]

[2] https://www.trustedsec.com/blog/three-most-common-physical-security-flaws-and-how-to-fix-them/

Environmental Considerations

Awareness of the environment around the physical security perimeter is crucial. Being aware of the environment could be the *key* for not needing a *key* or other tool to gain unauthorized physical access. In other words, just look at what it is you are assessing for clues.

Real-World Vulnerabilities | Environmental

More information on these examples is available at Black Hills Information Security.[3]

Sebaceous Oils. Sebaceous oils are simply oils from your fingers that could cause discoloration on a keypad. Anyone could use this to guess the correct combination.

I'm Snow Excited! Another use case is simply looking around your environment for a way In. Here is an interesting edge case where the snowbank was high enough to clear a barbed wire fence. *This doesn't apply to just snow. It could be new construction with dirt or even pallets that are high off the ground.*

Traveler Hook. Also known as a shrum tool, this tool is capable of bypassing dead latched locks. If not set properly, an attacker could simply insert the traveler hook in the door gap and push the locking mechanism in, opening the door in a matter of seconds.

Knife Bypass. A knife bypass tool is another simple bypass that could be used on certain padlocks. It's as simple as sticking the bypass tool into the lock, thus bypassing the locking mechanism.

Wafer Key Bypass. Warded locks, often located outside of a facility to secure power generators and other valuable assets, can be picked with a wafer key.

Double Door Tool. The double door tool allows an attacker to engage push bars located on double doors from the outside.

Thumb Turn Tool. Otherwise known as a J-Tool, this tool can fit in between door gaps and twist the handle that twists the bypass mechanism, allowing an attacker to open the door from the outside simply by turning the knob.

Under Door Tool. One of the oldest bypass tools, an under door tool can be leveraged by placing it under a door, rotating the hook, and pulling the door lever down.*Further details on this example and several more can be found at TrustedSec.*[3]

[3] https://www.blackhillsinfosec.com/tales-from-the-pick-intro-to-physical-security-tools/

Protection of Hardware

Gaining physical access to control rooms or other sensitive areas often implies gaining access to IT or ICS/OT equipment, but this need not be the case if utilities apply additional physical security measures.

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.

Computers used for ICS functions should never be allowed to leave the ICS area, lest they be compromised when in less secure environments. Electronic devices that *must* be taken out of secured areas, such as laptops, portable engineering workstations, and handhelds should be tightly controlled and returned to secured areas when not in use.

Malicious actors are not the only threat to IT and ICS/OT hardware; natural disasters can threaten this equipment as well. Therefore, organizations should implement measures that protect hardware from events like earthquakes, hurricanes, and floods which can damage equipment directly or have indirect impacts through the loss of power.

Practical Application

To protect critical systems and equipment from unauthorized physical access, consider the following measures:

- Affixing hard drives and portable media drives with locks when not in use.
- Removing and store hard drives and portable media drives in secured containers when not in use.
- Disabling USB ports to prevent uploading/downloading of data.
- Disabling buttons that control important functions such as power.
- Using physical protection devices that prevent unauthorized use.
- Storing keys and fobs in locked areas when not in use.

Unattended Equipment

Computing equipment, including storage media, should never be left unattended. Regardless of current storage state, computing equipment, hard drives, portable media drives, etc., can be affixed with locks or removed and stored in secured containers when not in use.

For Consideration

Unidentified USBs. USBs, those innocuous looking little portable storage devices, while useful in utility can contain malicious content. While hey are practical for transferring legitimate files and documents, they are equally functional for transferring malware into and sensitive files out of production networks – including air-gapped environments. Attackers often plant portable USBs to lure employees to install malware on corporate computers. Even advanced threat actors have used USBs to attack businesses. *In January 2022, the FBI reported on several packages containing malicious USB devices sent by the FIN7 advanced persistent threat (APT) group to U.S. businesses in the transportation, insurance, and defense industries.*[4] *The packages were sent using the United States Postal Service (USPS) and United Parcel Service (UPS). Along with the malicious USBs, some packages were accompanied by decorative gift boxes, letters, and counterfeit gift cards.*

Options for blocking or limiting USB usage:

- Disable USB ports to prevent the ability to upload or download data.
- Install USB locking port blockers that physically prevent devices from being plugged in.
- Establish and communicate clear USB security policies. USB policies should include at the very least additional scrutiny on files, documents, and other digital content.

[4] https://therecord.media/fbi-fin7-hackers-target-us-companies-with-badusb-devices-to-install-ransomware

- **Decommissioned equipment.** Computing equipment and storage media such as hard drives, back-up tapes, USB drives, CD-ROMs, DVDs, may contain sensitive data. Decommissioned equipment awaiting destruction should be placed in locked containers. Likewise, all data must be properly erased before disposal. *Simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools or services may be required to securely erase data prior to equipment disposal.*
- **New equipment.** If not properly secured, even new equipment without any data could be stolen and have malware placed on them – like a USB – and returned.

Protecting Design and Configuration Documents

If a threat actor cannot gain direct access to a control system, their next best option is to procure design and configuration documents. This type of information facilitates, and perhaps even guarantees, a successful campaign by a threat actor. Ways to protect these digital and paper documents include encrypting digital copies, keeping physical paper copies in a locked office and cabinet, limiting control room tours, and preventing visitor photography.

Likewise, it is important to limit the availability of sensitive documents during open procurements. Document access can be restricted through non-disclosure agreements, background checks, two-step procurement process with limited information provided during the qualification stage, secure file sharing with encryption, and document review only under supervision while onsite at the utility.

The importance of protecting control system design and configuration documentation was underscored by the North American Electric Reliability Corporation (NERC) in 2016. NERC fined one of its electric utility members $2.7 million for not properly protecting its critical cyber asset documentation, thereby unintentionally enabling a contractor to expose the documents on the internet.[5]

Reconnaissance Techniques Used by Threat Actors

Threat actors use various methods to gather information about critical infrastructure design and configuration:

Open Source Intelligence (OSINT). Attackers collect publicly available information about the target organization's infrastructure, including:

- Technical documentation
- Job postings revealing technology used within the environment
- Public records and regulatory filings
- Social media posts from employees

Network Scanning. Threat actors probe networks to identify:

- Active systems and open ports
- Software versions and potential vulnerabilities
- Network architecture and segmentation

Social Engineering. Malicious actors may use tactics like phishing or pretexting to:

- Extract sensitive information from employees
- Gain unauthorized access to internal systems
- Obtain credentials for accessing design documents

Targeting of Specific Documents. Threat actors often focus on acquiring:

- Network diagrams and topology maps
- System configuration files
- Software and hardware inventories
- Security policies and procedures
- Operational technology (OT) documentation

[5] https://www.nerc.com/pa/comp/CE/Enforcement Actions DL/Public_CIP_NOC-2569 Full NOP.pdf

RECOMMENDED RESOURCES

SANS ICS Site Visit Plan | SANS Institute

Cyber Assurance of Physical Security Systems (CAPSS) | National Protective Security Authority (UK)

Understanding the Importance of Physical Security for Industrial Control Systems (ICS) | Applied Risk

Tales From the Pick: Intro to Physical Security Tools | Black Hills Information Security

If You Don't Ruse, You Lose: A Simple Guide to Blending in While Breaking In | Black Hills Information Security

Social Engineering Basics: How to Win Friends and Infiltrate Businesses | TrustedSec

2024 USB Threat Report | Honeywell Global Analysis, Research, and Defense

Technology Equipment Disposal Policy | SANS Institute

NERC Full Notice of Penalty regarding Unidentified Registered Entity | NERC

8 Install Independent Cyber-Physical Safety Systems

WHY THIS IS IMPORTANT: Despite the practical applications for automation in control systems environments, it's important to consider implementing non-digital solutions to limit the consequence of high-impact events from physical damage or destruction that could result from any intentional or accidental act or failure of critical components or processes.

If you can imagine a worst case cyber threat scenario that could cause physical damage to and impact safety of ICS/OT and SCADA equipment, so will the bad guys. By engineering solutions to limit physical damage that could occur due to a cyber attack – *or even an unintentional event/incident, or failure of a device, component, or process* – asset owners can significantly reduce the impact posed by dangerous conditions that could result in high-consequence events such as excessive levels of pressure or chemical additions.

Adversaries may compromise an IT or OT control system to seek monetary gain, perform reconnaissance, modify operations, weaken customer trust, injure people, or physically destroy equipment or infrastructure. Malicious cyber actors targeting the water sector may seek long-term physical service disruption by breaking pipes or damaging process equipment that have long replacement times. Cyber attacks resulting in physical impact represent a complex or blended threat and typically pose a risk to safety. To protect critical assets from these blended threats, utilities should consider non-digital, engineered solutions such as independent cyber-physical safety systems.

Engineering Can Limit Physical Consequences of a Cyber Incident

If we can protect our critical assets from physical damage, service disruption from a cyber attack may be limited to the time it takes to transition to manual operation. Blended/complex attacks with long-lasting impacts can be mitigated by physically preventing access to process equipment and by installing independent cyber-physical safety systems. Such purpose-built engineered cyber-physical systems could be implemented to prevent conditions such as excessive levels of pressure, chemical additions, vibrations, or temperature change from occurring due to malicious or unintentional acts against or failures of a control system.

Real-World Proof-of-Concept

In 2007, Idaho National Labs dramatically demonstrated an example of a cyber-physical vulnerability in its experimental AURORA[1] attack by remotely damaging a large diesel generator. During the demonstration, the generator's circuit breaker was rapidly opened and closed to force it out of phase with line power, which in turn created destructive electrical torque that physically damaged the unit.

Independent Protections from Worst Case Scenarios

Few utilities have cybersecurity experts readily available, but every utility already has staff and consultants who understand the intricacies of water or wastewater processes and infrastructure. Existing staff can collaborate to identify ways that physical damage or hazardous situations can be created either intentionally or accidentally through imagining worst case scenarios. For example, *assuming a threat actor has full knowledge and total control of the OT system, what could they do to cause injury or lasting system damage?*

[1] https://www.powermag.com/what-you-need-to-know-and-dont-about-the-aurora-vulnerability/

Practical Application

Examples of Cyber-Physical Safety Systems Solutions and Potential Precautions

In the same way that a large generator can be protected from an AURORA style attack with a properly designed protection relay, and a boiler can be protected from a low-water-explosion with an independent low-water trip switch, vital components of water systems can also be protected. The following are examples of dangerous conditions to water infrastructure and a corresponding independently engineered cyber-physical solution to protect the process from physical damage – the dangerous conditions could be caused by an attack (cyber or physical), equipment failure, or accident:

- Attempts to break pipes by valve water hammer or harmonics can be mitigated with appropriately slow mechanical gearing of valve actuators.
- Attempts to break pipes by turning on too many pumps within a pressure zone can be handled by independent pressure switches wired to pump controllers, or by increasing tank overflow capacity.
- Dangerous overdosing of treatment chemicals can be mitigated by careful pump sizing and/or, as shown in Figure 1, hardwired shutdown interlocks between the chemical analyzer and pump control circuit.
- Attempts to damage large rotating equipment through variable frequency drive manipulation can be countered with independent vibration monitoring and thermal interlocks.
- Attempts to run wastewater pumps dry for extended periods by falsely presenting high wet-well levels to the control system might be managed by creating a combined high RPM and low electrical current triggered interlock.

Figure 1 depicts a simplified example of a cyber-physical safety system designed to prevent an overdose of Sodium Hydroxide into a drinking water system. In this example, a 'hi-hi' pH alarm contact is taken directly from an output contact of the pH analyzer/transmitter, wired via a relay panel, to halt the NaOH metering pump. When this system is engaged, it notifies the operator via an alarm to the primary control system as well as independently to the control room. Thus, this example covers both an independent alarming strategy as well as a cyber-physical safety shutdown. A cyber-physical safety system such as this could prevent an advanced ICS/OT cyber attack from resulting in harm to the consumer.

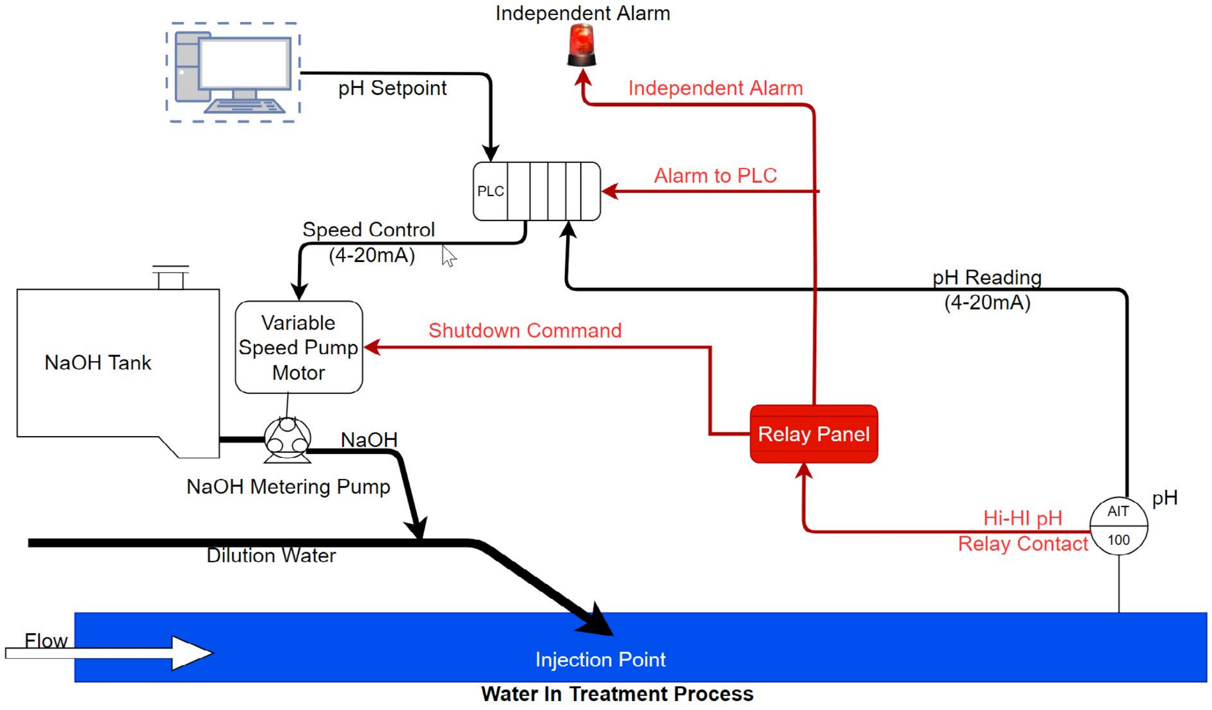


Figure 1 - Hardwired Hi-pH Shutdown and Independent Alarm Example

The independent and isolated aspects of a cyber-physical safety system are essential to its success. For example, in 2017, the TRITON/TRISIS[2] attack against a Saudi Arabian petrochemical plant demonstrated what could happen when a safety system is connected to a control system. In this case, the rigorous Safety Instrumented System (SIS) required for a petrochemical facility was compromised, presenting the potential for serious damage and injury if the control system had been subsequently attacked.

Likewise, while we carefully protect against adverse conditions, if the protection comes from logic built into the control system, the system can still be compromised. In other words, if the same PLC or digital controller contains both the normal process control logic and the process safety logic, then there is potential for both process manipulation and bypass of safety functions with the compromise of a single device. This potential exists even if there are two independent devices performing the function, but they are accessible with the same level of network access. Where consequences and risk require, it is critical to design and implement independent protections.

It is very important not to reduce the overall reliability of water and wastewater service because of the design, implementation, or maintenance of a cyber-physical safety system. Achieve simplicity and lower risk by using mechanical safety systems, such as a rupture disk. Use independent process monitoring alarms, as discussed in *Fundamental 4 | Implement System Monitoring for Threat Detection and Alerting*) and shown in Figure 2 in an initial, conservative approach. In some less time-sensitive cases, such as attempts to damage heat-sensitive electronic equipment by compromising an HVAC and building control system, use mechanical safety systems to reduce the likelihood of breach.

Figure 2 shows a simplified example of an independent alarming strategy. In this case, an analog copy of a critical system pressure is transmitted via an independent logging and telemetry system to the control center. The logger and associated logger server could generate an independent pressure reading and associated alarm. Ideally, a high-pressure alarm generated via the PLC (primary control system) would have a corresponding alarm generated via the logger and server. Any pressure value or alarms that were not within reasonable tolerances of one another would trigger further investigation and could help identify advance ICS/OT attacks that maliciously manipulate the process and primary control system.

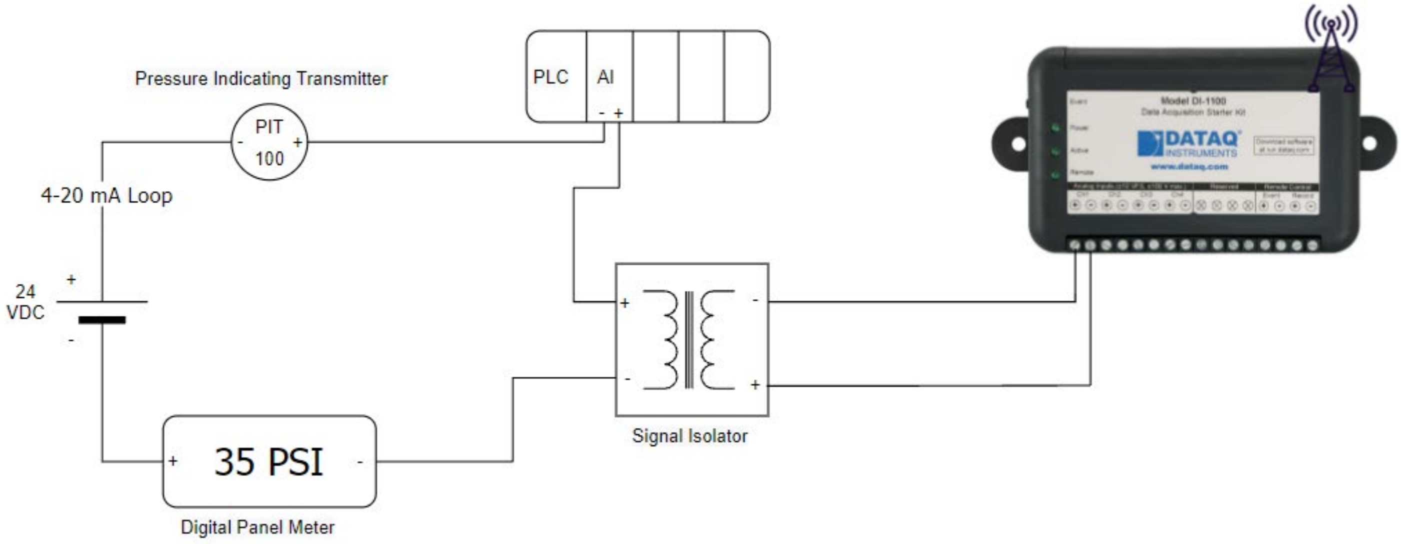


Figure 2 - Independent Pressure Alarm Example

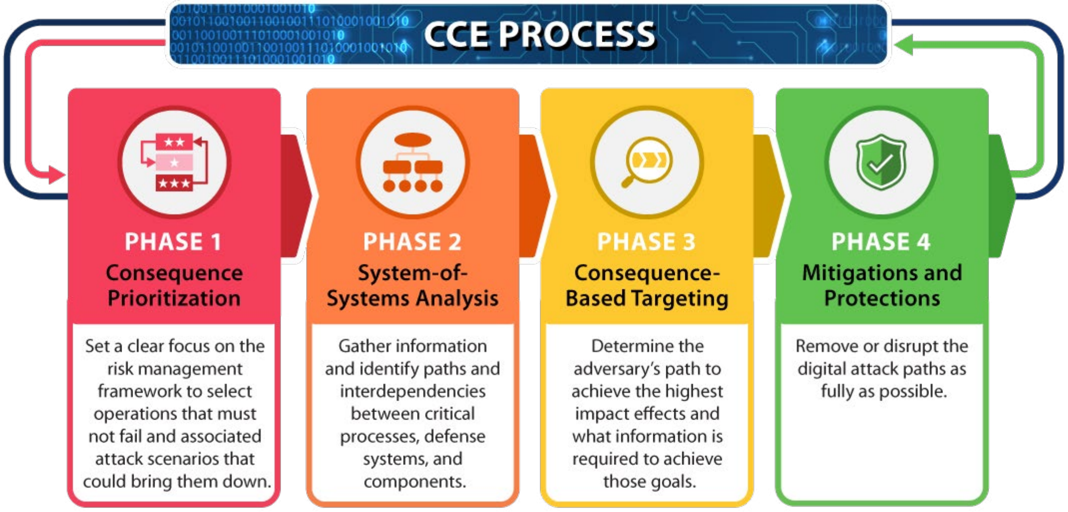
[2] https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf

Cyber Informed Engineering

Finally, to advance the effort of engineering cyber-physical safety systems to limit physical consequences and increase safety, Idaho National Laboratory (INL) developed the Cyber Informed Engineering (CIE) framework and Consequence-driven Cyber-informed Engineering (CCE) methodology focused on securing the nation's critical infrastructure systems. CIE and CCE have been incorporated into *NIST Special Publication 800-82r3.*[4]

Consequence-driven Cyber-informed Engineering (CCE)[3]

Developed at Idaho National Laboratory (INL), CCE begins with the assumption that if a critical infrastructure system is targeted by a skilled and determined adversary, the targeted network can and will be penetrated. This "think like the adversary" approach provides critical infrastructure owners and operators a four-phase process for safeguarding their critical operations.


CCE PROCESS
PHASE 1
Consequence Prioritization
PHASE 2
System-of-Systems Analysis
PHASE 3
Consequence-Based Targeting
PHASE 4
Mitigations and Protections

Set a clear focus on the risk management framework to select operations that must not fail and associated attack scenarios that could bring them down.

Gather information and identify paths and interdependencies between critical processes, defense systems, and components.

Determine the adversary's path to achieve the highest impact effects and what information is required to achieve those goals.

Remove or disrupt the digital attack paths as fully as possible.

RECOMMENDED RESOURCES

Cyber-Informed Engineering | Idaho National Laboratory (INL)

Consequence-Driven Cyber-Informed Engineering | Idaho National Laboratory (INL)

Countering Cyber Sabotage – Introducing Consequence-driven, Cyber-informed Engineering (CCE) | Andrew A. Bochman and Sarah Freeman

Cyber Informed Engineering – SANS ICS Concepts | SANS Institute

Engineering-Grade OT Security – A Manager's Guide | Andrew Ginter

Engineering Out the Cyber-Risk to Protect What Matters Most | Idaho National Laboratory at RSA Conference 2019

What You Need to Know (and Don't) About the AURORA Vulnerability | Power Magazine

Triton/Trisis Attack was More Widespread Than Publicly Known | Dark Reading

TRISIS Malware – Analysis of Safety System Targeted Malware | Dragos

[3] https://inl.gov/national-security/cce/
[4] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

9 Embrace Risk-Based Vulnerability Management

WHY THIS IS IMPORTANT: Vulnerability management across OT and IT is essential for water and wastewater utilities in maintaining operational continuity, protecting critical infrastructure, and mitigating the risks associated with cyber threats in increasingly interconnected industrial systems.

Vulnerability management is a foundation of every cybersecurity program. Like asset inventory (Fundamental 5 | Account for Critical Assets) and risk assessments, it is a continuous process and completely dependent on and intertwined with those actions. **Vulnerabilities are present everywhere – hardware, software, firmware, configurations, supply chains, and staff practices.** Therefore, vulnerability management is an absolute necessity in every organization. While tasks like patching and antivirus are important in addressing some vulnerabilities, effectively managing vulnerabilities requires a holistic program that applies a risk-based approach across OT and IT environments.

The Five ICS Cybersecurity Critical Controls[1] | Control No. 5: Risk-based Vulnerability Management Program

A risk-based vulnerability management program focuses on those vulnerabilities that actually drive risk to the organization, especially those that map to the scenarios identified in ICS Critical Control No. 1. Often, the vulnerabilities that drive risk in ICS are those that help an adversary gain access to the ICS or introduce new functionality that can be leveraged to cause operational issues such as the loss of view, control, or safety. **The focus of the vulnerability management program is not simply to patch vulnerabilities but also, in many cases, to mitigate their impact or monitor for their exploitation.**

Address Vulnerabilities Before the Bad Guys Exploit Them

CPG[2] | 1.E Mitigating Known Vulnerabilities

All known exploited vulnerabilities (listed in CISA's *Known Exploited Vulnerabilities Catalog*[3] in internet-facing systems are patched or otherwise mitigated within a risk-informed span of time, prioritizing more critical assets first.

Operational Technology (OT): For assets where patching is either not possible or may substantially compromise availability or safety, compensating controls are applied (e.g., segmentation, monitoring) and recorded. Sufficient controls either make the asset inaccessible from the public internet, or they reduce the ability of adversaries to exploit the vulnerabilities in these assets.

With the sheer number of IT devices and internet-accessible ICS/OT devices, vulnerabilities present a significant opportunity for cyber attacks. Public resources like Shodan,[4] Censys,[5] and even Google enable the discovery of vulnerable devices by anyone with an internet connection. Combining data garnered from these discovery tools with vulnerability exploitation kit frameworks like Metasploit and Cobalt Strike, even novice threat actors are able to launch attacks with very little knowledge or understanding about the systems (IT or OT) they are targeting. Performing authorized scans and assessments, including penetration tests, will help identify exploitable vulnerabilities within your environment before the bad guys do.

[1] https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/
[2] https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog
[4] https://www.shodan.io/dashboard
[5] https://censys.com/

CPG[6] | 1.F Third-Party Validation of Cybersecurity Control Effectiveness

Third parties with demonstrated expertise in (IT and/or OT) cybersecurity should regularly validate the effectiveness and coverage of an organization's cybersecurity defenses. These exercises, which may include penetration tests, bug bounties, incident simulations, or table-top exercises, should include both unannounced and announced tests.

Exercises consider both the ability and impact of a potential threat actor to infiltrate the network from the outside, as well as the ability of a threat actor a within the network (e.g., "assume breach") to pivot laterally to demonstrate potential impact on critical systems, including operational technology and industrial control systems.

High-impact findings from previous tests are mitigated in a timely manner and are not re-observed in future tests.

Information on vulnerabilities is provided from various sources including vendors, cybersecurity firms, ISACs and federal agencies. To aid utilities in maintaining awareness of vulnerability disclosures, **WaterISAC regularly disseminates information on vulnerabilities and patches received from partners at CISA, other ISACs, vendors, cybersecurity firms, and others.** These curated advisories and bulletins are invaluable, but utilities need to have an internal program to further track, research, and effectively address disclosed vulnerabilities with a risk-based approach that is most appropriate and relevant to each networked environment.

REPORT | Dragos OT Cybersecurity The 2023 Year in Review[7]

According to the *OT Cybersecurity The 2023 Year in Review*, while Dragos Intelligence assessed 2,010 OT-related vulnerabilities, only 3% of vulnerabilities needed to be addressed immediately. Additionally, Dragos evaluates that the majority of vulnerabilities can be addressed through alternative means like monitoring and multi-factor authentication rather than urgent patching.

In 2023, 53% of the advisories Dragos analyzed were vulnerabilities that could cause both a loss of view and control of the process through a vulnerable OT system. A full 46% of all the vulnerabilities have no ability to impact the control or visibility of the industrial process. Of these vulnerabilities, 1% could only cause loss of view without impacting loss of control.

Remediate, Mitigate, or Accept Vulnerabilities

Once vulnerabilities are identified and prioritized using a risk-based approach, they should either be remediated, mitigated, or the associated risks must be accepted and documented. Ignoring a vulnerability that exists in your environment is not an option. Device vulnerabilities are frequently remediated through patches and software or firmware updates. However, even after patches and updates have been released by a vendor, many systems remain vulnerable because asset owners are either unaware of the patch or choose to not implement fixes due to lack of understanding or insufficient resources.

[6] https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
[7] https://www.dragos.com/ot-cybersecurity-year-in-review/

Furthermore, some products have design "features" that are inherently insecure-by-design and will never have a patch. In instances where patches are not or cannot be applied, vulnerabilities should be mitigated through compensating security control methods such as "hardening" to remove unnecessary services and applications, replacing devices when they are no longer supported by the vendor, enforcing policies and procedures (Fundamental 10 | Develop and Enforce Cybersecurity Policies and Procedures)[8], and providing cybersecurity awareness and technical training (Fundamental 3 | Create a Cyber Secure Culture and Protect from Insider Risks). Impacts can be further reduced by installing independent cyber-physical safety systems (Fundamental 8 | Install Independent Cyber-Physical Safety Systems), interrupting threat actors early in the attack cycle through successful threat detection (Fundamental 4 | Implement System Monitoring for Threat Detection and Alerting), and applying lessons learned post-incident response (Fundamental 1 | Plan for Incidents, Emergencies, and Disasters).

RESOURCE | ICS-Patch[9]

The ICS-Patch decision tree will lead to one of three results for each cyber asset/security patch pair.

Defer Do not apply or schedule to apply the security patch on the cyber asset for risk reduction. (The asset owner may choose to apply the security patch as part of cyber maintenance to keep the system under support.)

Scheduled The security patch should be applied on the cyber asset during the next scheduled patch window. For some ICS, this may be a scheduled outage that occurs annually or semiannually. For others they may choose a quarterly or monthly patching interval.

ASAP Apply the security patch on the cyber asset as soon as possible in a safe manner.

SMALL SYSTEMS GUIDANCE

Throughout this guide, the CISA CPG's that have been referenced for smaller systems and less cyber mature utilities have been denoted as requiring *little to no monetary investment with high impact toward risk reduction and low complexity to implement*. While **CPG 4.C Deploy Security.txt Files** meets that criteria, **CPG 1.E Mitigating Known Vulnerabilities** is an exception that is strongly recommended. Despite its medium complexity to implement, mitigating known vulnerabilities, especially on critical assets has a high impact on risk reduction that cannot be overstated. Mitigating vulnerabilities significantly reduces the attack surface available for exploitation.

CPG | 1.E Mitigating Known Vulnerabilities

All known exploited vulnerabilities (listed in CISA's *Known Exploited Vulnerabilities Catalog*[10] in internet-facing systems are patched or otherwise mitigated within a risk-informed span of time, prioritizing more critical assets first.

Operational Technology (OT): For assets where patching is either not possible or may substantially compromise availability or safety, compensating controls are applied (e.g., segmentation, monitoring) and recorded. Sufficient controls either make the asset inaccessible from the public internet, or they reduce the ability of adversaries to exploit the vulnerabilities in these assets.

CPG | 4.C Deploy Security.txt Files

All public-facing web domains have a security.txt file that conforms to the recommendations in RFC 9116.

Reference **security.txt**[11] to define the process for security researchers to securely disclose security vulnerabilities to your utility.

[8] Fundamental 10 | Develop and Enforce Cybersecurity Policies and Procedures will be released in December 2024
[9] https://dale-peterson.com/wp-content/uploads/2020/10/ICS-Patch-0_1.pdf
[10] https://www.cisa.gov/known-exploited-vulnerabilities-catalog
[11] https://securitytxt.org/

Don’t Assume Cybersecurity

The maintenance of traditional computers and SCADA equipment for business and operations at water and wastewater utilities can be overwhelming. As such, it’s common for small or less technically mature utilities to contract service providers or integrators for both IT and OT support. In many cases, that support does not provide adequate, if any, cybersecurity protections. Technology or managed service providers (TSPs or MSPs) may perform patching of and provide antivirus on Windows devices for IT and OT systems (if the OEM or maintenance agreement allows it), but that is typically the extent of protection unless the service contract or scope of work outlines further requirements.

Vulnerability Management Resources

As a starting point in identifying critical vulnerabilities on external facing systems, less resourced systems are highly encouraged to avail themselves to *CISA’s Free Vulnerability Scanning (VS) for Water Utilities*[12] service. CISA’s vulnerability scanning can help utilities identify and address cybersecurity weaknesses that an attacker could use to impact a system.

CISA’s *Known Exploited Vulnerabilities (KEV) Catalog*[13] is a highly recommended resource to help all organizations prioritize patching. **CISA’s KEV catalog includes vulnerabilities known to be exploited** – either attempted or successful – by cyber threat actors. The KEV catalog offers network defenders a starting point for prioritizing remediation efforts on the subset of vulnerabilities that are causing immediate harm based on adversary activity. Organizations should use the KEV catalog as an input to their vulnerability management prioritization framework. CISA and WaterISAC strongly **recommend all stakeholders include a requirement to immediately address KEV catalog vulnerabilities as part of their vulnerability management plan**. Doing so will build collective resilience across the cybersecurity community. Utilities and their service providers are encouraged to check the KEV catalog and the regular updates for potentially impacted components in your environment and address accordingly.

In addition to referencing CISA’s KEV catalog for prioritizing known exploited vulnerabilities, it is necessary for utilities and their integrators to be aware of and apply a risk-based approach to addressing industrial control systems vulnerabilities for OT and SCADA components used within your OT environment. While it’s best to track published updates and notifications directly from vendors or manufacturers, CISA also tracks and provides regular *ICS Advisories*.[14] The ICS Advisories found at CISA provide concise summaries covering industrial control system (ICS) cybersecurity topics primarily focused on mitigations that ICS vendors have published for vulnerabilities in their products.

RECOMMENDED RESOURCES

Industrial Control Systems Advisories | CISA

Known Exploited Vulnerabilities Catalog | CISA

ICS-Patch - What To Patch When In ICS? A Decision Tree Approach | Dale Peterson

The OT Vulnerability Management Handbook | Langner, Inc.

ICS Advisory Project | Dan Ricci

Cybersecurity Incident & Vulnerability Response Playbooks | CISA

National Vulnerability Database (NVD) | NIST

Common Vulnerabilities and Exposures (CVE) | MITRE

[12] **https://www.cisa.gov/resources-tools/resources/cisas-free-cyber-vulnerability-scanning-water-utilities**
[13] **https://www.cisa.gov/known-exploited-vulnerabilities-catalog**
[14] **https://www.cisa.gov/news-events/cybersecurity-advisories?f%5B0%5D=advisory_type%3A95**

WATER ISAC

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

in waterisac

𝕏 waterisac

waterisac.org/fundamentals