ENDEAVORB2B®

SPECIAL REPORT · 2026

Shutterstock AI

WATER SYSTEM CYBERSECURITY

The When Is Now

Numerous cyberattacks on water systems raise alarms across the US

REPORTING FROM

WaterWorld®

WASTEWATER DIGEST

SIW SECURITY INFOWATCH.COM®

CONTROL

control design

TechEDGE™

ABOUT THIS COLLECTION

Deep expertise with a broad lens

The cyberattacks that hit water and wastewater systems in at least 12 states beginning in late July 2026 do not belong to a single beat.

BY BOB CROSSEN

The vulnerabilities for water and wastewater systems lie with programmable logic controllers used to automate operations, primarily with pumps and valves. The danger of this is multi-fold for a utility. A bad actor could reduce or increase chemical dosage by changing pump speeds, could close or open vales in a distribution system to create water hammer to break pipes, or simply make enough of a scare to sow distrust with the local municipality.

EPA estimates 97% of the country's 145,000 water systems serve 10,000 people or fewer, and as you may imagine, that means resources are not something of abundance for nearly every system in the U.S. Utilities leverage the knowledge of consultants, integrators, and when possible, security professionals to ensure their systems are safe from cyber threats.

In this collection of articles, we've brought in the expertise from the security and electronics markets to provide the expertise and knowledge that can help them better understand the threats to their systems. And for security and electronics professionals, you'll gain a deeper and more clear understanding of the challenges involved in keeping public water systems safe.

We hope this broader lens across multiple markets also offers you the deeper expertise and knowledge that help your businesses succeed and stay safe as digitization and automation continue to evolve.

The question is no longer whether a determined foreign adversary can reach an American water system. It is why so many systems were reachable in the first place.

STEVE LASKY · SECURITYINFOWATCH.COM, PAGE 18

All articles appear as originally published by their reporting brand. Headlines link to the source story.

ENDEAVORB2B®

TIMELINE

What happened

April, 2026

Six federal agencies issued CISA advisory AA26-097A, confirming that Iranian-linked actors were actively exploiting internet-connected Allen-Bradley programmable logic controllers across U.S. water, energy and government facilities.

May, 2026

Security Business published Critical Infrastructure Under Siege, reporting that the campaign was the activation of a threat built over a decade of connectivity decisions made without matching security investment.

Early July, 2026

A *Control Global* column argued the sector was not solving the right problem: guidance remained network-focused while control system incidents that produce physical consequences went largely unexamined.

Late July, 2026

More than 30 community water systems in Minnesota were targeted during a two-day campaign, according to Minnesota IT Services. In Braham, attackers temporarily disabled computerized operating controls, shutting down the city's well and water treatment plant until operators restored service.

August, 2026

The incidents expanded beyond Minnesota. Michigan officials disclosed that nine water systems in the state also experienced cyberattacks; Rapid City, South Dakota reported an incident as well. Since mid-July, systems in at least 12 states have reported intrusions.

The target

Federal officials said the attackers targeted Allen-Bradley MicroLogix 1100 and 1400 PLCs from Rockwell Automation, changing IP addresses and passwords so that operators lost monitoring and operational control. Most utilities kept running by switching to manual control, and officials said drinking water remained safe. Some incidents resulted in boil-water notices.

Where it stands

The FBI, EPA and CISA are investigating alongside state agencies and have not formally attributed the attacks. Iranian-linked sources on Telegram have claimed responsibility on behalf of the CyberAv3ngers, a group associated with Iran's Islamic Revolutionary Guard Corps.

12	30+	6	0
STATES REPORTING INTRUSIONS	MINNESOTA SYSTEMS TARGETED	FEDERAL AGENCIES ON AA26-097A	REPORTED CONTAMINATION EVENTS

Compiled from the articles in this collection. Sources and links on page 30.

CONTENTS

Inside this collection

NEWS

01 **Cyberattacks targeting U.S. water systems prompt renewed focus on utility cybersecurity** — 05
WATERWORLD

02 **Water facilities in 12 states hit by cyberattacks. The real story is how attackers gained access.** — 07
TECHEDGE

COLUMN

03 **Not solving the right problem: Water and wastewater safety and availability depend on more than networks** — 09
CONTROL GLOBAL

EXPLAINER

04 **What is a programmable logic controller (PLC)?** — 13
WASTEWATER DIGEST

FEATURES

05 **What recent cyberattacks reveal about securing water utility OT** — 15
WATERWORLD

06 **America's water systems are still too exposed to cyberattack** — 18
SECURITYINFOWATCH.COM

07 **Critical infrastructure under siege** — 23
SECURITYINFOWATCH.COM

LISTEN & WATCH

08 **Related videos and podcast episodes** — 29
WASTEWATER DIGEST · CONTROL DESIGN · SECURITYINFOWATCH.COM

Sources, links & photo credits — 30

WATERWORLD NEWS · WATER UTILITY MANAGEMENT

Cyberattacks targeting U.S. water systems prompt renewed focus on utility cybersecurity

A series of cyberattacks targeting municipal water systems across the Midwest disrupted automated controls but maintained water safety, prompting federal and state investigations into potential nation-state involvement.

ALEX COSSIN · AUG. 3, 2026

A coordinated wave of cyberattacks targeting municipal water systems across the Midwest has renewed concerns about the cybersecurity of U.S. drinking water and wastewater infrastructure, even as utilities report that public health and water quality were not compromised.

More than 30 community water systems in Minnesota were targeted during a two-day campaign in late July, according to Minnesota IT Services. The attacks affected operational technology used to monitor and control water infrastructure, prompting state and federal agencies to launch a coordinated response.

Among the affected utilities, the city of Braham reported that attackers temporarily disabled computerized operating controls, shutting down its well and water treatment plant until operators restored service. Other communities, including Plymouth, South St. Paul and Maple Plain, reported disruptions to automated controls or communications but maintained water and wastewater operations through manual procedures. Officials in each community said drinking water remained safe and no contamination occurred.

The incidents have since expanded beyond Minnesota. Michigan officials recently disclosed that nine water systems in the state also experienced cyberattacks, although operators maintained safe service and no public health impacts were reported. The FBI, the U.S. Environmental Protection Agency and the Cybersecurity and Infrastructure Security Agency (CISA) are investigating the incidents alongside state agencies.

Operational technology remains a target

The attacks primarily targeted operational technology (OT) systems, including remote monitoring and programmable logic controllers (PLCs) used to manage pumps, wells, lift stations and water towers, rather than enterprise information technology systems. Federal officials have warned that internet-connected industrial control equipment continues to present an attractive target for nation-state actors and cybercriminals, particularly at smaller utilities with limited cybersecurity resources.

While investigators have not publicly attributed the attacks, federal officials are examining whether they are connected to previously identified Iranian-affiliated cyber activity targeting critical infrastructure. Authorities caution that the investigation remains ongoing and no official attribution has been announced.

Manual operations limit service disruptions

Although the cyberattacks disrupted portions of automated control systems, most affected utilities were able to continue operations by switching to manual control procedures. The incidents underscore the importance of maintaining operational redundancy and emergency response plans alongside investments in cybersecurity.

Federal agencies have advised water utilities to review remote access practices, disconnect unnecessary internet-exposed control systems, implement multifactor authentication and ensure operators can safely transition facilities to manual operation if automated systems are compromised.

The recent attacks are the latest reminder that cybersecurity has become a core component of utility resilience. As drinking water and wastewater systems continue adopting digital monitoring, automation and remote operations, utilities face growing pressure to strengthen cyber defenses while ensuring reliable service and protecting public health.

This piece was created with the help of generative AI tools and edited by our content team for clarity and accuracy.

The recent attacks are the latest reminder that cybersecurity has become a core component of utility resilience.

TECHEDGE NEWS · SECURITY

Water facilities in 12 states hit by cyberattacks. The real story is how attackers gained access.

Cyberattacks targeting water utilities in late July and early August demonstrate how exposed OT systems can disrupt physical operations. For CIOs, CISOs and infrastructure leaders, the incidents highlight growing risks from internet-connected industrial controls and the need to strengthen OT security.

THERESA HOUCK · AUG. 6, 2026

At least 12 states have reported cyberattacks targeting water and wastewater systems in late July and continuing into August, but the larger story extends far beyond the water sector. For CIOs, CISOs and CSOs, the most important takeaway isn't that water systems were attacked. It's how they were attacked.

According to the FBI, the Environmental Protection Agency (EPA) and the Cybersecurity and Infrastructure Security Agency (CISA), attackers gained access to internet-facing operational technology (OT) devices and disrupted physical operations by altering configurations, changing passwords and disabling monitoring capabilities.

Federal agencies warn that the same tactics could target industrial control systems across manufacturing, energy, transportation and other critical infrastructure sectors.

For water utilities, the attacks led to operational disruptions and, in some cases, boil-water notices. For manufacturers and infrastructure operators,

The lesson for technology and security leaders is straightforward: this isn't just a water-sector problem. It's a critical infrastructure problem.

similar attacks could halt production, damage equipment, create safety risks or disrupt supply chains.

CISA also warns that undocumented remote-access pathways, including vendor-installed connections and cellular modems, may be creating exposure that organizations don't fully understand.

Exposed PLCs gave attackers a path into water systems

According to an FBI and EPA public service announcement, water and wastewater utilities in at least seven states reported cyber incidents, with the number of affected states later reported to have grown to a dozen. In several cases, organizations were forced to switch to manual operations, and some incidents resulted in boil-water notices.

Minnesota was among the hardest-hit states, with officials reporting that more than 30 municipal water facilities were targeted between July 26 and 27. Michigan and Rapid City, South Dakota, also reported incidents. State officials said there was no evidence of water contamination and that affected systems continued operating safely.

Federal officials said the attackers targeted specific industrial control systems used by water utilities, including Allen-Bradley MicroLogix 1100 and 1400 programmable logic controllers (PLCs) from Rockwell Automation.

The FBI and EPA have not formally attributed the attacks. However, some officials and cybersecurity experts have suggested possible links to Iran based on similarities to previous campaigns and broader geopolitical tensions.

Federal agencies recommend restricting OT access and connectivity

Also, the decline of traditional air-gapped environments has increased exposure across critical infrastructure sectors, according to a Fortinet solution brief on its OT Security Platform.

Federal agencies are urging operators to remove critical OT assets from direct internet exposure, strengthen passwords, limit remote access and restrict communications to authorized systems. According to the FBI, attackers changed PLC IP addresses and passwords after gaining access, causing organizations to lose monitoring and operational control of affected devices.

While none of the reported incidents resulted in water contamination, they have renewed concerns about the cybersecurity of critical infrastructure nationwide. Investigations remain ongoing, and agencies continue to urge organizations with internet-connected industrial systems to review their OT security controls.

Why OT security is now a business resilience priority

The lesson for technology and security leaders is straightforward: this isn't just a water-sector problem. It's a critical infrastructure problem.

Organizations should identify internet-exposed OT assets, review remote-access pathways, strengthen IT/OT segmentation and validate their ability to continue operating when automated systems become unavailable.

These incidents demonstrate that OT security is increasingly a business resilience issue. Organizations best positioned to withstand future attacks will be those that understand and secure the connections between their digital and physical operations.

CONTROL GLOBAL COLUMN · UNFETTERED BLOG

Not solving the right problem: Water and wastewater safety and availability depend on more than networks

Organizations must understand how to limit the physical consequences when electronic information cannot be trusted and how to prevent compromise

JOE WEISS · JULY 6, 2026

Water and wastewater systems, like other industrial and manufacturing facilities, rely on electronically communicating control systems consisting of pumps, valves, motors, drives, relays, analyzers, process sensors, engineering workstations, operator displays and communication networks. Because these systems depend on electronic communications to monitor and control physical processes, control system cyber incidents occur whenever electronically communicated process information becomes corrupted, delayed, unavailable or untrustworthy, regardless of whether the cause is malicious, accidental or equipment-related, since each can compromise the safe operation of the physical process.

As Professor Ross Anderson stated in his seminal book, *Security Engineering: A Guide to Building Dependable Distributed Systems*, security engineering is about building systems that remain dependable in the face of malice, error or mischance. Consequently, organizations must understand not only how to prevent compromise but also how to limit the physical consequences when electronic information cannot be trusted.

A plethora of network cyberattacks and identified cyber vulnerabilities has prompted congressional hearings on various critical infrastructures, town hall meetings on critical infrastructure incident reporting and critical infrastructure cybersecurity conferences. The common thread across these discussions has been that these activities were network-focused, and they did not address process sensors or other control system cyber incidents that produce physical consequences.

The OT cybersecurity community's predominant emphasis on network security has caused a two-fold problem: First, a focus on network-related attacks or perceived attacks, and second, ignoring control system and unintentional incidents. The 2021 Oldsmar incident was widely characterized as a cyberattack even though subsequent reviews suggested that human error played a significant role

in the event. The result was a renewed emphasis on network security rather than an understanding of the engineering and human factors that led to of unsafe process behavior.

Federal cybersecurity guidance from agencies such as EPA, CISA and TSA, together with industry guidance from organizations such as AWWA and NERC, generally assumes that process sensors and actuators can be secured using approaches developed for networked IT assets, whenever those field devices are even explicitly discussed. This was illustrated by an EPA email recommending common IT security actions for process sensors and actuators, even though these devices lack the capabilities needed to implement such approaches. At the same time, the OT cybersecurity community continues to give comparatively little attention to control system incidents that have caused significant impacts because those incidents were not the result of network attacks. This narrow focus leaves a significant blind spot: incidents originating within the process environment.

The distinction between network cybersecurity incidents and control system cyber incidents is not merely semantic. It determines which incidents are investigated, reported, shared and ultimately mitigated. If only network intrusions are considered cyber incidents, a large class of events involving compromised electronically communicated process information, including failures involving process sensors, engineering defects and control-system interaction, remains outside the cybersecurity community's field of view despite producing the most significant physical consequences.

Identification of actual incidents and impacts

For more than three decades, Applied Control Solutions (ACS) has maintained a proprietary repository of control system cyber incidents spanning multiple critical infrastructure sectors. Unlike public cyber incident databases that primarily catalog network intrusions and malware events, this repository includes incidents resulting from automation failures, process measurement issues, engineering defects, control logic errors, human-machine interaction issues and malicious cyberattacks.

These incidents originate within the control process itself and therefore exist regardless of the degree of IT-OT convergence. Across critical infrastructures globally, these incidents have contributed to more than 30,000 fatalities and more than $100 billion in damages, demonstrating that major operational risk often originates within the control environment. Within the ACS repository, non-network incidents account for the overwhelming majority of fatalities and physical damage.

Given the current interest in water and wastewater cybersecurity, the water/wastewater portion of the repository was selected as the initial test case for this analytical capability. For water/wastewater, the repository spans 1994-2026 and contains more than 250 documented domestic and international control system cyber incidents involving loss of view, loss of control, equipment damage, environmental releases, boil water notices and injuries.

Because the ACS repository contains proprietary incident information, it has historically been difficult to systematically interrogate the data without exposing confidential information. A recently developed secure analytical tool now enables queries across the repository while protecting the underlying data, making it possible to identify previously unknown correlations and trends.

More than 35% involved process sensor problems, approximately 25% involved malicious cyber activity, more than 20 of the incidents resulted in boil water notices, and more than 150 public injuries were associated with those incidents. In many cases, the

PLCs operated exactly as designed. The physical damage occurred because the controllers received incorrect process measurements from field instrumentation rather than because the PLC software malfunctioned.

Incorrect sensor measurements disrupted normal closed-loop sensor-controller-actuator relationships, causing equipment to operate in potentially unsafe conditions. Consequently, even perfect PLC cybersecurity would not have prevented many of these incidents because the controllers acted on incorrect process information rather than compromised controller logic. Incorrect sensor data can result from manufacturing defects, installation errors, calibration problems, sensor drift, environmental influences, counterfeit components or malicious manipulation.

A preliminary review of other critical infrastructure sectors revealed similar patterns. Engineering personnel are generally not trained to recognize when failures of electronically communicated process information constitute cyber incidents, while cybersecurity personnel are generally not trained to investigate the engineering mechanisms through which those incidents produce physical consequences.

No trusted cross-sector mechanism currently exists for sharing control system cyber incidents involving process sensors, control logic interactions or electronically communicated process measurements. Although the Cyber Incident Reporting for Critical Infrastructure Act of 2022 was enacted to improve cyber incident reporting for critical infrastructure, it does not specifically address the distinctive characteristics of control system incidents involving process instrumentation and electronically communicated process measurements.

Proposed program

Consider a seven-point program that would help address these shortfalls:

01 Develop a taxonomy and common definitions for control system cyber incidents that distinguish them from traditional network cyber incidents while recognizing both malicious and non-malicious causes.

02 Integrate engineering, instrumentation and cybersecurity expertise into incident investigations involving physical process anomalies.

03 Educate executives, engineers, operators and cybersecurity personnel on control system cybersecurity and the role of field devices, particularly process sensors.

04 Train engineering and cybersecurity personnel to recognize, investigate and classify control system incidents that involve electronic communications, regardless of whether they are malicious or unintentional.

05 Develop mechanisms to collect and analyze control system incident data, including process sensor failures and sensor-actuator interactions, to identify recurring engineering and cybersecurity patterns.

06 Incorporate control system cybersecurity and process sensor integrity requirements into procurement specifications for field devices and automation systems.

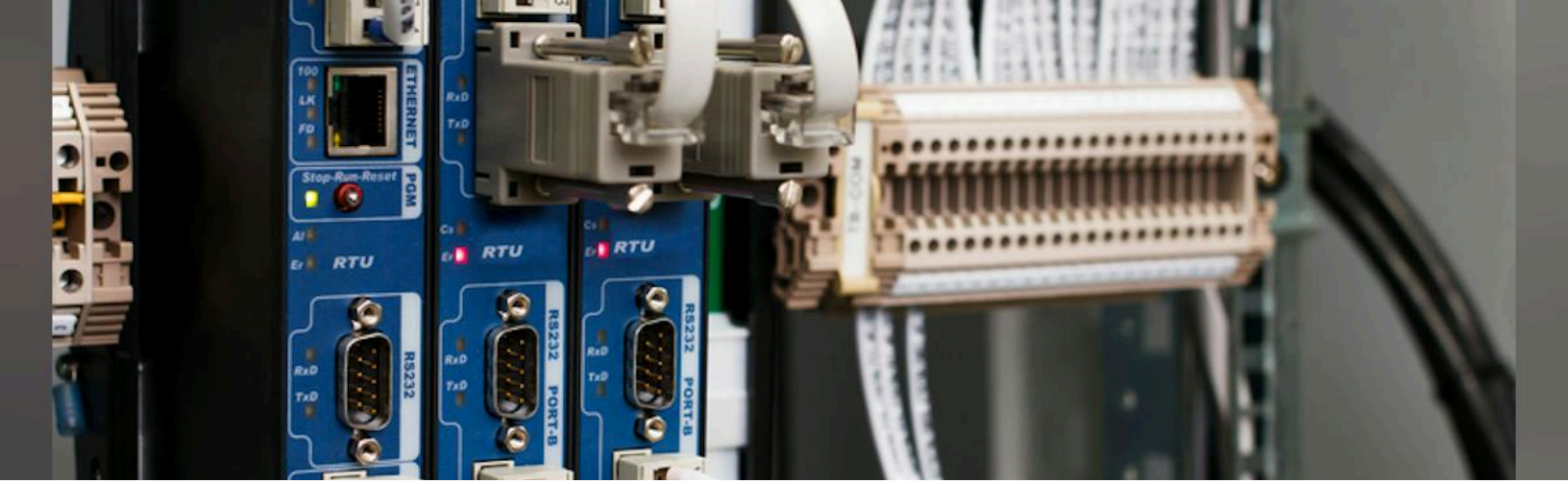
07 Establish a trusted, cross-sector information-sharing program focused specifically on control system cyber incidents, including process sensor failures and sensor-actuator interactions.

Summary

The incident data demonstrate that corrupted, delayed, unavailable or otherwise untrustworthy electronically communicated process information can produce physical damage, environmental releases, service interruptions and injuries.

Yet these incidents are generally investigated as equipment failures, instrumentation problems or operational errors rather than as control system cyber incidents. Until engineering and cybersecurity disciplines are jointly trained to recognize, investigate, classify and share information about these events, significant operational and public safety risks will remain outside the scope of current water-sector cybersecurity programs and regulations.

250+ Documented water and wastewater control system cyber incidents in the ACS repository, 1994-2026. More than 35% involved process sensor problems; approximately 25% involved malicious cyber activity.



WASTEWATER DIGEST EXPLAINER · WHAT IS SERIES

What is a programmable logic controller (PLC)?

A programmable logic controller is an industrial computer used to automate processes in facilities like a water or wastewater treatment plant.

CRISTINA TUSER · JULY 26, 2022

A programmable logic controller is "a small industrial computer originally designed to perform the logic functions executed by electrical hardware (relays, switches, and mechanical timer/counters)," as defined by The U.S. Department of Commerce National Institute of Standards & Technology (NIST).

PLCs have evolved to control complex processes and are used in supervisory control and data acquisition (SCADA) systems and Distributed Control Systems (DCS). PLCs are used in almost all industrial processes.

What are the benefits of PLCs?

According to NIST, PLCs have user-programmable memory for storing instructions for specific functions, including I/O control, logic, timing, counting, three mode (PID) control, communication, arithmetic, and data and file processing.

Unlike SCADA and DCS, PLCs usually do not have a central control server and HMI and, therefore, they "primarily provide closed-loop control without direct human involvement."

This kind of automation allows engineers with a limited knowledge of computers and computing languages to operate the systems easily, as PLCs are generally considered intuitive.

Other benefits noted by NIST are that PLCs "withstand vibrations, temperature, humidity and noise; and have interfacing for inputs and outputs already inside the controller."

What are the components of PLCs?

According to NIST, the components of the PLCs are:

PROCESSOR UNIT

The processor unit or central processing unit (CPU), or the unit containing the microprocessor that interprets the input signals and carries out the control actions.

PROGRAMMING DEVICE

The programming device, which is used to enter the required program into the memory of the processor.

INPUT AND OUTPUT SECTIONS

The input and output sections, where the processor receives information from external devices and communicates information to external devices.

POWER SUPPLY UNIT

The power supply unit, which converts the mains AC voltage to the low DC voltage.

MEMORY UNIT

The memory unit, where the program is stored that is to be used for the control actions to be exercised by the microprocessor and data stored from the input for processing and for the output for outputting.

COMMUNICATIONS INTERFACE

The communications interface is used to receive and transmit data on communication networks from or to other remote PLCs.

What are the main types of PLCs?

The main types of PLCs are compact PLCs and modular PLCs.

Compact PLCs

According to BasicPLC, the compact PLC input and output (I/O) are integrated into the microcontroller itself. Every type of input or output is fixed, so it does not have the capability to expand the modules.

Modular PLCs

A modular PLC generally looks like a rack in which multiple modules can be fitted. This allows multiple expansions of the system and gives the PLC additional features such as an increased number of I/O units. Modular PLCs are usually easier to use because each component is independent of each other, meaning operators can troubleshoot by isolating modules.

In addition to the I/O modules, these types of PLCs generally have an independent power supply as well as a communications module. As such, modular PLCs tend to offer more flexibility than compact PLCs.

Modular vs. compact PLC: Which is best?

Between modular and compact PLCs, the modular PLC is preferred, especially for large industrial systems because they often contain a lot of devices with I/O that also need to be controlled. Factors often considered when choosing a PLC include scalability, number of I/O, fault detection, downtime, module combinations, and memory.

WATERWORLD FEATURE · ROUNDTABLE

What recent cyberattacks reveal about securing water utility OT

Recent cyberattacks on U.S. water systems reveal critical vulnerabilities in operational technology, especially legacy PLCs and remote access methods.

ALEX COSSIN · AUG. 6, 2026

A wave of recent cyberattacks targeting U.S. water systems has highlighted persistent vulnerabilities in operational technology (OT) environments, prompting renewed discussion about how utilities – particularly smaller systems – can strengthen cybersecurity without sacrificing operational efficiency.

During a recent WaterWorld roundtable discussion, automation expert Jeremy Pollard, retired industrial automation specialist and columnist for *Control Design*, and Gabriel Collins, Baker Botts Fellow in Energy and Environmental Regulatory Affairs at Rice University's Center for Energy Studies, discussed what the attacks reveal about the current state of water utility cybersecurity and what utilities can do to reduce their risk.

While investigations into the attacks remain ongoing, both experts agreed the incidents should serve as a wake-up call for the industry.

Legacy OT remains a primary concern

According to Pollard, many water and wastewater utilities continue to rely on legacy programmable logic controllers (PLCs) and remote access methods that were designed long before cybersecurity became a central concern.

Pollard said many PLCs are internet-accessible because operators and integrators need remote access to monitor and maintain facilities. If attackers discover exposed devices or compromise remote communication methods, they may be able to gain access to control systems.

"If you use a tool like Shodan... PLCs show up all over the place," Pollard said, noting that internet-facing devices often exist because utilities require remote access for maintenance and operations.

Once inside, attackers may be able to change passwords, lock legitimate users out of controllers or manipulate operating parameters if sufficient protections are not in place. Pollard noted that some

reporting suggests the attackers demonstrated familiarity with PLC programming and industrial control systems.

He added that the widespread use of major automation platforms – including Schneider Electric, Siemens and Rockwell Automation – likely makes them attractive targets simply because of their prevalence throughout the water sector.

Smaller utilities face unique challenges

The discussion also focused on why smaller utilities frequently appear among publicly identified cyberattack victims.

Collins suggested that highly capable nation-state actors are likely probing many more systems than those ultimately reported.

"My suspicion is... these Iranian linked groups are probably attacking a lot more water systems," Collins said, adding that the publicly known incidents may simply represent systems where attackers successfully gained access or caused noticeable disruptions.

Pollard agreed, noting that smaller utilities often depend on third-party contractors for automation support and may lack dedicated OT cybersecurity expertise.

Many also rely on publicly accessible cellular networks for remote communications rather than private industrial networks, potentially increasing exposure if communication devices are compromised.

Simple security practices still matter

Although sophisticated nation-state attacks dominate headlines, both experts stressed that many vulnerabilities remain surprisingly basic.

Pollard recalled working with a municipality that used the password "password" across multiple devices, including cellular modems.

"It's easier to do that than to have different passwords," he said, acknowledging that operational convenience has often taken precedence over security in smaller organizations.

He also pointed to a recent report describing attackers targeting hotel Wi-Fi networks to steal credentials from traveling personnel who remotely access industrial systems.

Because many operators and contractors connect to facilities while traveling, compromised credentials can potentially provide attackers with legitimate access into operational networks.

Older equipment can still be secured

Replacing legacy PLCs is not always feasible, but Pollard said utilities can immediately improve security by reviewing how controllers are configured.

One recommendation is leaving controllers in "run mode" rather than remote programming mode whenever possible, preventing unauthorized online logic changes while still allowing systems to operate normally.

"It doesn't stop data changes," Pollard cautioned, noting attackers could still modify setpoints or timer values if they gain sufficient access.

He also referenced the industry's "Top 20 PLC Security" guidance, which outlines software and configuration practices intended to prevent unsafe parameter changes and establish operating boundaries for industrial control systems.

Why manual operations mattered

Most utilities affected by the recent attacks reported that drinking water remained safe because operators shifted facilities into manual operation after automated controls were disrupted.

While Pollard acknowledged those responses prevented more serious consequences, he argued the attacks were still successful in another sense.

"We're talking about it," he said. "The fact that it's got everybody on edge, I believe it's been very successful in that regard."

Collins added that cyberattacks do not necessarily need to cause catastrophic failures to achieve strategic objectives.

From his perspective, simply demonstrating the ability to access critical infrastructure can serve as a form of deterrence by reminding governments and utilities that vulnerabilities exist. He suggested that different nation-state actors may pursue different goals, ranging from signaling capability to causing operational disruption during future geopolitical conflicts.

Proactive testing over reactive response

Looking ahead, both experts advocated for greater use of proactive cybersecurity assessments.

Collins suggested federal agencies could conduct or fund penetration testing of utility systems to identify vulnerabilities before adversaries do.

"You can either adversarially test ourselves and find problems and fix them, or we can be tested by our adversaries," Collins said. "That's the fundamental security choice we're facing here."

Pollard agreed, saying the water sector should revisit remote access architectures that have become increasingly complex over time.

In his experience, some utilities now require numerous authentication steps involving jump servers, firewalls and demilitarized zones (DMZs), creating systems that are difficult to manage while not necessarily improving security.

"Anybody that's using remote access, you have to revisit that and make sure that it's as simple as it can be and have security as a focus," Pollard said.

As cyber threats against critical infrastructure continue to evolve, both experts emphasized that improving operational technology security will require a combination of modernized equipment, stronger cybersecurity practices and a proactive approach to identifying weaknesses before attackers do.

Credit: Wengen Ling

SECURITYINFOWATCH.COM FEATURE · CRITICAL INFRASTRUCTURE

America's water systems are still too exposed to cyberattack

The latest attacks on U.S. water infrastructure expose a deeper problem than vulnerable PLCs: an OT security gap that technology, regulation and resources have failed to close.

STEVE LASKY · AUG. 18, 2026

Since mid-July, water and wastewater systems in at least 12 states have reported cyber intrusions, putting a stark new face on a vulnerability security officials have warned about for years. Iranian-linked sources on Telegram have claimed responsibility on behalf of the CyberAv3ngers, a group associated with Iran's Islamic Revolutionary Guard Corps (IRGC), while the FBI and CISA have stopped short of publicly assigning definitive blame.

But attribution may ultimately be less important than what the attacks have exposed. The question is no longer whether a determined foreign adversary can reach an American water system. It is why so many systems were reachable in the first place.

That is the more consequential story emerging from the attacks. Beneath the headlines about Iranian hackers and compromised municipal systems is a far more systemic problem: critical water infrastructure is increasingly being operated on an industrial-control foundation that was never designed for today's cyber threat.

Legacy programmable logic controllers (PLCs) and other operational technology (OT) were built for reliability, availability and physical control; not internet-facing connectivity, remote administration, identity-based access or persistent cyber defense. Yet over decades, those systems have been connected to modern IT networks, remote-access platforms and, in some cases, the public internet.

The result is a dangerous collision between old technology and new adversaries.

Chuck Brooks, an internationally recognized cybersecurity expert, said the latest incidents should be viewed as part of a continuing campaign rather than isolated events.

"Instead of viewing this as a singular incident, security leaders should see it as part of an ongoing, opportunistic-to-directed campaign," Brooks said. He pointed to previous compromises of internet-exposed PLCs and human-machine interfaces (HMIs) and warned utilities to "anticipate ongoing scanning, credential attacks, and opportunistic exploitation of still-vulnerable interfaces," particularly as geopolitical tensions rise.

Maria Sumnicht, an OT, ICS and IoT cybersecurity expert and the National Director for Cybersecurity Task Force on National and Homeland Security, took the issue back to its roots: connectivity was a choice.

"The reason so many ICS and PLC environments are accessible from the public internet is that someone, somewhere, decided to do this," Sumnicht said. "Twenty-plus years ago, this was not the case. These systems were not connected to the public internet. To make changes, you had to go onsite."

Vendor remote access has become one justification for that exposure. As Sumnicht put it: "The best and worst answer I received at the same time was, 'Because the manufacturers need access to perform updates without sending a representative on site.'"

The policy response has been equally problematic. In 2023, the federal government attempted to require cybersecurity reviews as part of water-system risk assessments. Arkansas, Iowa and Missouri challenged the effort, a federal appeals court halted implementation, and the EPA ultimately withdrew the rule. Less than a week before the first highly publicized Minnesota attacks, CISA expanded its warnings to additional PLC manufacturers.

For smaller utilities, limited resources compound the challenge. The Water Watch Center, launched by DEF CON Franklin and the National Rural Water Association, was intended to help utilities serving fewer than 10,000 people strengthen detection and response capabilities. But the experts interviewed for this story emphasized that monitoring is only one piece of the solution.

The fundamentals still matter

Shane Barney, chief information security officer at Keeper Security, said the recent incidents demonstrate an access-control problem as much as a detection problem.

"When threat actors reached programmable logic controllers, changed passwords, and locked operators out of their own systems, the detection problem and the access problem arrived at the same moment," Barney said.

His prescription was straightforward: every operator and administrator should have a unique credential tied to an individual identity; contractor access should be time-limited and scoped; and changes to privileged accounts should be immediately visible to those responsible for the system. These controls, Barney said, do not require a dedicated security team and provide the foundation for more effective monitoring.

Matt Hartman, chief strategy officer at Merlin Group, agreed that detection cannot substitute for basic OT hygiene.

> *Legacy programmable logic controllers (PLCs) and other operational technology (OT) were built for reliability, availability and physical control; not internet-facing connectivity, remote administration, identity-based access or persistent cyber defense.*

“Traditional IT-focused monitoring may not detect direct interaction with a PLC,” Hartman said. For smaller utilities, he added, “detection isn't a substitute for the fundamentals: knowing what assets you have, securing remote access, segmenting networks, and eliminating unnecessary internet exposure.”

John Gallagher, vice president at Viakoo, put asset visibility at the top of that list.

“The true binding constraint for small water systems is basic asset discovery and vulnerability remediation,” Gallagher said. That means knowing which devices are connected, eliminating default passwords, updating firmware and enforcing secure access before sophisticated monitoring can deliver meaningful value.

The resource gap, however, cannot be ignored.

Kevin E. Greene, chief cybersecurity technologist, public sector, at BeyondTrust, described the situation bluntly: “Many small water systems are still operating below the cyber poverty line.”

A realistic national strategy, Greene said, must combine asset visibility, secure remote access, MFA where it can be enforced, privileged-access governance, tested manual operations, incident-response support and access to regional or shared technical expertise. It must also account for what happens when prevention fails: disaster recovery, continuity of operations, emergency management, and crisis communications.

“When a water utility loses operational control, it stops being only a cybersecurity problem very quickly,” Greene said. “It can become a public-safety and national security issue.”

Christopher Hills, chief security strategist at BeyondTrust, argued that the problem also reflects a longstanding OT priority.

“For many years, OT has prioritized uptime over security and threat actors know this,” Hills said.

Yet legacy technology does not eliminate the need for basic security. Hills pointed to default credentials and unnecessary public-facing access as fundamental weaknesses that can and should be addressed even when modern security controls cannot be deployed.

For environments that cannot easily adopt those controls, he argued that Zero Trust principles can establish a security boundary around OT and regulate access from both external and internal sources. The immediate priority, however, remains basic: manage or rotate default credentials and shut down direct public access that is not necessary.

Taken together, the experts pointed to a hierarchy of needs: know what is connected, remove unnecessary exposure, control access, secure remote pathways, segment OT networks and establish the visibility necessary to recognize abnormal activity.

The challenge is making those fundamentals sustainable for utilities that may lack the money, personnel or technical expertise to implement them independently.

OT is not IT

The industry has spent decades securing enterprise IT, but OT has lagged because the two environments present fundamentally different operational realities.

Industrial-control systems may be decades old, difficult to patch and unable to tolerate downtime. A security strategy designed around conventional IT assumptions — frequent updates, system replacement, and aggressive endpoint controls — cannot simply be transferred to an environment where availability and physical safety are paramount.

Sumnicht argued that the regulatory framework must recognize that distinction. USDA should incorporate industrial-control-system risk assessments into its regulations and establish cybersecurity controls tailored specifically to OT. USDA and CISA also need to address process-sensor security more explicitly

because those sensors can be critical to the safe and reliable operation of industrial environments.

Internationally, examples of a broader approach already exist. BSI 96:2026, British Standards Institution guidance on food defense, explicitly recognizes SCADA systems, PLCs, sensors and cold-chain monitoring as systems requiring protection against deliberate acts, including cyberattacks, sabotage and other threats.

“The broader lesson is that OT security must be addressed in the context of the physical processes those systems control, not simply through the lens of enterprise network security,” Sumnicht said.

That means defining control-system cybersecurity separately from enterprise IT security and building OT requirements into policies, procurement and workforce training. Organizations should also independently monitor critical process sensors using physics-based validation rather than relying solely on network security controls.

“Sensor cybersecurity should become part of existing safety and reliability programs,” Sumnicht said, “ensuring that anomalous readings or manipulated data can be identified before they translate into unsafe or unreliable physical outcomes.”

That requires cybersecurity, engineering and operations to work together rather than in separate silos. The objective is not simply to bolt another security layer onto legacy OT, but to incorporate security into the operational, engineering, safety and reliability processes already governing these systems.

Done correctly, the result can be more than improved cybersecurity. It can improve operational safety, reliability, predictive maintenance and resilience.

Cyber warfare's new target: Trust

The significance of these attacks extends beyond compromised PLCs, changed passwords or disrupted operations. Brooks said they reflect a broader evolution in cyber warfare; one in which disruption, public unease and declining trust in essential services can be as valuable to an adversary as stolen data or financial gain.

Water systems are particularly consequential targets because they sit at the intersection of public safety and public confidence. An attack can test an operator's preparedness, demonstrate an adversary's capabilities and impose operational and psychological costs without the escalation associated with a conventional kinetic attack.

That changes what water-system cybersecurity must accomplish.

The objective can no longer be simply to prevent a breach. Governments and operators must assume that scanning, credential attacks and exploitation of exposed systems will continue. They must also build the ability to absorb an intrusion without losing operational control.

The experts pointed to a hierarchy of needs: know what is connected, remove unnecessary exposure, control access, secure remote pathways, segment OT networks, and establish the visibility necessary to recognize abnormal activity.

As Brooks put it, critical-infrastructure cybersecurity must become “a fundamental component of both national and societal resilience.”

The action items are clear: remove unnecessary internet exposure; establish continuous visibility into OT assets; segment operational networks; secure remote access; strengthen privileged-identity controls; apply Zero Trust principles where appropriate; expand public-private threat intelligence sharing; exercise cross-sector incident response; and design systems for graceful degradation, manual operation and rapid recovery.

None of that can be accomplished through technology alone.

Cybersecurity must become part of how water systems are designed, procured, operated and maintained. That means investing in people, procedures and OT-specific expertise and providing smaller utilities with sustained federal support and shared capabilities rather than relying on temporary programs or philanthropic stopgaps.

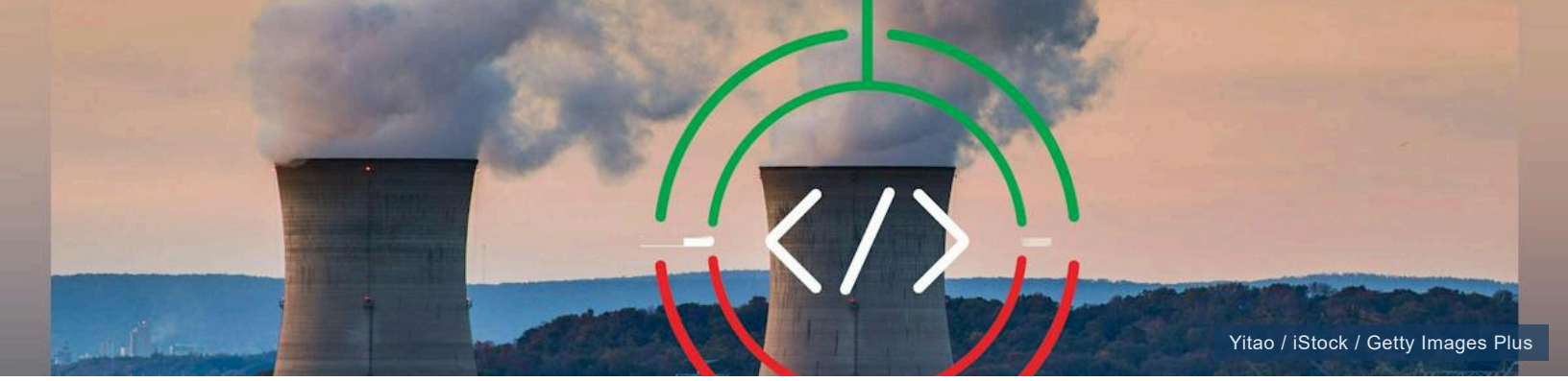
The lesson from this latest wave of attacks is not simply that America's water infrastructure is vulnerable. It is that adversaries increasingly understand how to turn that vulnerability into leverage.

The utilities best prepared for the next attack will not necessarily be those with the most sophisticated security technology. They will be the ones that know what is connected, control who can access it, eliminate unnecessary exposure, recognize when something is wrong, and critically know how to keep delivering safe water when their digital defenses fail.

The time for treating OT security as an IT problem is over. Water security is operational security, public safety and national resilience. The next phase of cyber warfare will test all three.

KEY HIGHLIGHTS · SECURITYINFOWATCH.COM

- Water systems in multiple states have experienced cyber intrusions, exposing vulnerabilities in legacy industrial-control systems not designed for today's cyber threats.
- Experts warn that connectivity choices made decades ago have left critical infrastructure exposed, necessitating fundamental security improvements and policy changes.
- Basic security practices such as unique credentials, network segmentation, and eliminating unnecessary internet exposure are essential to prevent and detect attacks.
- Small utilities face resource challenges, underscoring the importance of federal support, shared expertise, and comprehensive risk management strategies.
- Cyber warfare now targets trust and operational control, requiring utilities to build resilience through continuous visibility, manual operation readiness, and cross-sector collaboration.



SECURITYINFOWATCH.COM COVER STORY · SECURITY BUSINESS, MAY 2026

Critical infrastructure under siege

Iran's cyber campaign against U.S. operational technology is the activation of a threat that has been building for years. Security integrators and consultants have a central role in what happens next.

PAUL ROTHMAN · MAY 15, 2026

The valves that regulate chlorine levels in a municipal water supply. The relay switches on a transmission line serving a major metro grid. The programmable controllers governing pressure in a regional gas pipeline. These are the systems now in the crosshairs of Iranian-affiliated cyber actors, and according to a joint advisory issued April 7, 2026, by six U.S. federal agencies, the attacks are no longer theoretical. They are underway.

CISA Advisory AA26-097A, co-signed by the FBI, NSA, EPA, Department of Energy, and U.S. Cyber Command, confirms that Iranian-linked threat actors are actively exploiting internet-connected programmable logic controllers (PLCs) — specifically Rockwell Automation/Allen-Bradley systems — across U.S. critical infrastructure. Targeted sectors include water and wastewater systems, energy, and government facilities. The advisory documents actual operational disruptions and financial losses at victim organizations.

For security integrators and consultants serving utilities, municipalities, transportation authorities, and even manufacturing clients, the advisory represents a milestone: The question of whether OT security falls within their scope has been answered.

A problem built over decades

To understand why this moment arrived, security technology and management consultant Pierre Bourgeix, founder of ESI Convergent and one of the country's foremost OT security consultants, traced the exposure back to a decade of connectivity decisions made without commensurate security investment.

“As we have connected a lot of OT infrastructure in the last 10 years, what we've now connected are devices that do not have the technology to secure themselves,” Bourgeix explained. “There are hundreds of millions of connected devices where, back in the day, they were not. Over time, we started connecting them because the requirements shifted. These systems are in scope now — you have to know if they're online, if they're high, low, on, off, disabled.”

This article originally appeared as the cover story in the May 2026 issue of Security Business magazine.

The mandate came partly from government. Around 2018, the Government Accountability Office directed that all pipeline systems be connected to enable visibility and oversight. The intent was legitimate; however, the execution left critical systems exposed in ways that were predictable to those paying attention. Bourgeix wrote about the risk at the time, before the Colonial Pipeline attack made headlines, making the vulnerability undeniable.

COVID accelerated the exposure further. When facility operators had to manage industrial systems remotely, they connected those systems to the cloud without establishing the security architecture to protect those connections.

“What that has led to is even more attacks,” Bourgeix said, “because we haven't secured those connections and communication systems, nor have we secured the actual connector.”

What a PLC actually does, and why it matters

The term “operational technology” can obscure the physical reality at stake. PLCs are the switches that, among hundreds of functions, regulate flow valves in a water treatment facility, control transmission lines and transformers in a power grid, and manage ingredient ratios in a food manufacturing process. Their function is binary at the core — open and close, on and off — but the downstream consequences of unauthorized manipulation are not.

“If we put too much chlorine in water, it could kill people,” Bourgeix said flatly. “So it's everything. If you turn on your water, the things that support it are what causes this problem.”

In an energy environment, the stakes scale even further. A compromised switch in a transmission network can trigger what Bourgeix called a cascading effect — a chain reaction that takes out an entire regional power grid. Restoration requires days, not hours. Most energy companies lack the compensating controls and backup redundancy to recover quickly, and building that resilience costs millions.

The transit sector carries its own risks. The switching systems that route subway and rail traffic are embedded in the same OT environment. A manipulated signal switch is a collision waiting to happen.

The IT/OT boundary: Where the exposure lives

OT environments operate in a fundamentally different security architecture than IT systems. In IT, decades of open-standard development have produced a mature protection stack — layers three through seven in network architecture terms, with established tools from vendors like Juniper and a well-understood security model.

In OT and SCADA environments, the equivalent stack (layers zero through three) is proprietary, fragmented, and far less mature.

“There are over 74 different types of PLC and SCADA control systems, and they're all closed systems,” Bourgeix noted. “They don't talk to each other. We can't add security components without those vendors being part of it.”

Each manufacturer — Rockwell, Siemens, Schneider Electric, and dozens of others — has built its own security model. Each carries its own vulnerabilities, and each requires its own patching cadence.

CISA has issued hundreds of vulnerability advisories for Siemens PLC controllers alone.

Legacy code running on aging hardware compounds the problem. When IT departments inherit responsibility for OT systems, the result is rarely good.

“IT looks at OT going, ‘this is simple,’” Bourgeix said. “But isn't simple, because it's connected to

high-availability systems that are very secure and need to be protected. A lot of those systems are old. And old code on old computers means vulnerabilities."

The nominal separation between OT and IT — the DMZ, the firewall, the airgap — erodes in practice. Dual-hatted personnel who work across both OT and IT environments become potential attack vectors. Service technicians who dial in to repair an isolated system create a connection point, and any data traveling from a PLC through a DMZ to a dashboard creates a channel that a sophisticated attacker can exploit through a man-in-the-middle or side-channel approach.

Aras Nazarovas, Senior Information Security Researcher at Cybernews, described the core vulnerability plainly: "OT environments often don't have the same security controls as IT systems; instead, they rely much more on physical security and isolation. These systems are built to stay active 24/7, so a lot of standard protections like encryption or strong authentication aren't always in place. In some cases, traffic is unencrypted for simplicity, and default passwords are still used."

Nation-state actors: The long game

The Iranian campaign did not materialize from nothing. The groundwork was laid over years, by multiple state-sponsored actors probing and pre-positioning inside U.S. critical infrastructure.

Volt Typhoon — a Chinese state-supported cyber operation also known by the designations Vanguard Panda, Bronze Silhouette, and Voltzite, among others — spent years compromising thousands of internet-connected devices across U.S. aviation, water, energy, and transportation networks.

Western intelligence officials and CISA confirmed that Volt Typhoon's goal was pre-positioning: establishing persistent access that could be activated to disrupt critical communications infrastructure during a future conflict.

CISA director Jen Easterly told Congress that agency teams found and eradicated Chinese intrusions across multiple critical infrastructure sectors. The hackers had maintained that access for approximately five years. Bourgeix connected the dots directly. "We knew they were already in. We think Volt Typhoon was part of it. This was not something people weren't aware of for the last 10 months."

The Iranian actors named in AA26-097A — operating as CyberAv3ngers under the IRGC's Cyber Electronic Command — have been active since at least 2023. A prior CISA advisory from December 2023 documented the same group targeting U.S. PLCs across multiple sectors including water and wastewater systems. The current campaign is an escalation, not an inauguration.

> *"If one of the systems has already been penetrated, something may be lying in wait that could attack another system from within. Anything interconnected has to be evaluated."*
>
> **PIERRE BOURGEIX, ESI CONVERGENT**

“Nation-state syndicates are organizations hired to create these vulnerabilities,” Bourgeix said. “They go to work every day. They share what they've done and piggyback onto each other's effects. The misnomer is that this is a guy in his underwear in a basement. These guys all work for a living.”

Iran, he noted, learned from being a victim. The Stuxnet attack on Iranian centrifuges — widely attributed to U.S. and Israeli intelligence — gave Iranian actors a detailed education in OT vulnerability. They absorbed those lessons. They built relationships with Chinese and North Korean hacking syndicates. They waited.

What a competent response looks like

When the AA26-097A advisory dropped, Bourgeix's immediate protocol was triage. “The first thing we do is assess the client's systems if we haven't already,” he explained. “We evaluate every automated control system — not just Rockwell and Siemens, but all of them — and look at what vulnerabilities have been identified in the last year that should have been patched or changed.”

That assessment drives the next phase: isolation and quarantine of affected or at-risk systems, evaluation of the kill chain to understand where and how an intrusion may have progressed, and a determination of what can safely be taken offline versus what must remain operational. For systems that cannot be shut down, Bourgeix's team implemented immediate communication controls — temporarily halting any traffic from inside the OT environment to the outside while the vulnerability is being evaluated.

The hardest truth in OT incident response is that a simple patch rarely resolves the problem. “You can't just roll out a patch,” Bourgeix said. “Especially in OT infrastructure, because you're dealing with so many different layers. You're shutting down, isolating, triaging, repairing, then mitigating the root problem so you can get back up and running.”

Validation after remediation requires testing in a sandboxed environment — a duplicate of the production system that can absorb a patch test without risking operational continuity. “Most organizations don't have sandboxes of their own,” Bourgeix acknowledged. “The first thing I would do is build one within an organization that mimics how their system is working. You have to test and validate that your fix actually solves the problem before it touches the live system.”

He also warned against assuming that isolation equals safety. “If one of the systems has already been penetrated, something may be lying in wait that could attack another system from within. Anything interconnected has to be evaluated.”

The integrator's role: Larger than they think

Most security integrators working in industrial, utility, or municipal environments have not positioned themselves as OT security advisors. That positioning needs to change.

Bourgeix is direct about the risk of deploying physical security technology into an OT environment without understanding the architecture. “If you're dealing with work within OT infrastructure and there are vulnerabilities that could arise if you deploy cameras incorrectly — or if you don't understand the cloud vs. hybrid environment — then you are potentially risking your client's security.”

Camera systems, access control, sensor networks, fence detection — all of these, when deployed inside an OT environment, become part of that environment's attack surface. An integrator who installs a cloud-connected camera system in a utility substation without understanding the network segmentation model may have created an entry point.

The architecture question extends to the choice between cloud, on-premises, and hybrid deployments. Bourgeix described working with an energy company that wanted to move toward cloud-based management. His counsel was precise: bidirectional cloud communication inside an OT environment is dangerous. Outbound-only, directional communication to a DMZ domain controller — for visibility and alerting — can be done safely. The difference requires an understanding that the integrator sitting across the table often does not have.

The path forward, Bourgeix argued, runs through the consultant relationship that too many integrators treat as adversarial. “Our biggest challenge right now with integrators is they treat consultants like they are their enemy,” he said. “If they started working with us instead of trying to design things they shouldn't be designing, they would end up being more successful. They'd sell more because we'd be able to have these conversations with IT and OT together and build systems that are much more accurate and secure.”

The integrator who walks into a utility or manufacturing client's office with OT architecture awareness — who understands segmentation, who knows what a PSP is in a SIP environment, who can speak to NERC governance alongside physical security technology — earns a seat at a different table. “They'd go, ‘You've done your due diligence; you understand our problems, and you are willing to work with us hand in hand,'” Bourgeix said. “That grows a relationship.”

The board problem

Underneath every underfunded, underprotected OT environment is a board of directors that never treated OT security as a budget priority. Bourgeix has sounded that alarm for years. “If the board doesn't understand the challenge and the problem, they're the ones who prevent the money and the funding and the requirements.”

That is where integrators and consultants carry their most underutilized leverage. They are often the only outside voices in front of a board or senior leadership team with firsthand knowledge of the physical infrastructure at risk. The ability to connect an OT vulnerability to a business continuity failure — to translate “compromised PLC” into “regional grid outage lasting days, with no backup system in place” — is a conversation that changes budget allocations.

Nazarovas reinforced the foundational argument for making that case: “This is not just a one-off campaign — it's a repeatable attack model. The same kind of attack can be repeated again and again until the systems are properly secured.”

The current Iranian campaign, whatever its geopolitical trajectory, has exposed the structural vulnerability of OT infrastructure to state-sponsored cyberattack. That exposure does not resolve with a ceasefire. It resolves with architecture, segmentation, governance, redundancy, and the kind of cross-disciplinary expertise that security integrators and consultants are positioned — when they are at their best — to deliver.

The outcome imperative

Bourgeix closed with a frame that will resonate with every integrator who has followed the industry's evolution over the past decade. “That's how you create value — showing the outcomes and the business problems. Because if you don't, you're simply seen as somebody who just hangs stuff. And if the stuff you hung becomes the problem, you're probably not going to keep that customer.”

In OT security, the stakes for that calculus are higher than anywhere else in the integrator's portfolio. Critical infrastructure has no tolerance for a mistake born of incomplete architecture knowledge or an eagerness to sell the wrong system. “In critical infrastructure, there isn't a next day once you screw up,” Bourgeix said.

The integrators who build OT competency now — who develop the consultant relationships, learn the segmentation principles, understand the governance frameworks, shows up to client conversations with architecture awareness rather than product catalogs, and who treat this moment as a strategic inflection point — will define the next generation of the trusted advisor role in critical infrastructure.

Coordinated incident response: Who does what

When an OT environment is compromised or at risk, effective response requires every stakeholder in the room and a clear division of responsibilities. Pierre Bourgeix outlined the framework, below, stressing that the integrator's value in a response event is physical layer assurance. When the software layer is compromised, the physical security layer becomes the fallback. Integrators who understand that dynamic — and show up prepared to fill that role — become indispensable partners.

THE CONSULTANT / OT SECURITY LEAD

- Conduct immediate forensic triage: what happened, when, and what is still at risk
- Isolate and quarantine compromised or vulnerable systems
- Evaluate the kill chain across all interconnected systems
- Coordinate with Rockwell, Siemens, or relevant vendors on available patches
- Build or activate a sandbox environment to test remediation before deployment
- Validate all security controls before systems return to operation

THE IT DEPARTMENT

- Provide visibility into any IT/OT boundary exposure or dual-hatted user accounts
- Support network segmentation hardening at the IT layer
- Coordinate on any cloud or remote access connections that may create reentry points

THE SECURITY INTEGRATOR

- Confirm that all physical security systems (access control, cameras, sensors) are fully operational and not themselves connected to compromised OT segments
- Identify any monitoring gaps created by systems taken offline — and provide physical or temporary coverage for those gaps
- Advise on whether guard services or additional physical presence is warranted at high-risk system locations
- Validate that camera and access control systems in OT environments are appropriately segmented from compromised infrastructure

THE END USER / FACILITIES OWNER

- Confirm backup power and redundancy status across affected systems
- Execute business continuity protocols while remediation is underway
- Ensure board and executive leadership are briefed and empowered to authorize spending

LISTEN & WATCH

More on the attacks

Three places to keep following the story, from the newsrooms covering it.

PODCAST WASTEWATER DIGEST

What we know about the cyberattacks on water systems

Recent coordinated cyberattacks targeting water and wastewater system PLCs across Minnesota and several other states raised alarm bells for water systems across the U.S. In this episode, learn what happened, why it matters, and what utilities can learn from the incident.

Listen Now

VIDEO CONTROL DESIGN

Connect your PLCs to the Internet: What could possibly go wrong?

The Cybersecurity & Infrastructure Security Agency (CISA) issued an alert on July 30 regarding a significant increase in cyber threat actors targeting programmable logic controllers (PLCs) in the water/wastewater sector. While the U.S. government has not at this point made a public attribution of the activity, CISA has urged all critical infrastructure owners, operators and integrators to remove publicly exposed PLCs and other OT devices from the internet ASAP.

Watch Now

PODCAST SECURITYINFOWATCH.COM

Security DNA Podcast

Security DNA Podcast covers security news, trends and analysis as well as technology solutions, policy risk analysis and management, and more for industry professionals. The podcast hosts, along with industry experts and consultants, fill each episode with information that is of value to security professionals serving multiple industries.

Listen Now

SOURCES & CREDITS

References

ARTICLES IN THIS COLLECTION

1. Cossin, A. “Cyberattacks targeting U.S. water systems prompt renewed focus on utility cybersecurity.” *WaterWorld*, Aug. 3, 2026. waterworld.com/55395154
2. Houck, T. “Water Facilities in 12 States Hit by Cyberattacks. The Real Story Is How Attackers Gained Access.” *TechEDGE*, Aug. 6, 2026. tech.endeavoredge.com/55396121
3. Weiss, J. “Not solving the right problem: Water and wastewater safety and availability depend on more than networks.” *Control Global*, July 6, 2026. controlglobal.com/55388935
4. Tuser, C. “What is a Programmable Logic Controller (PLC)?” *Wastewater Digest*, July 26, 2022. wwdmag.com/21016258
5. Cossin, A. “What recent cyberattacks reveal about securing water utility OT.” *WaterWorld*, Aug. 6, 2026. waterworld.com/55396350
6. Lasky, S. “America's Water Systems Are Still Too Exposed to Cyberattack.” *SecurityInfoWatch.com*, Aug. 18, 2026. securityinfowatch.com/55398609
7. Rothman, P. “Critical Infrastructure Under Siege.” *SecurityInfoWatch.com*, May 15, 2026. securityinfowatch.com/55372352

AUDIO & VIDEO

“What we know about the cyberattacks on water systems,” *Talking Under Water* podcast, Wastewater Digest. “Connect your PLCs to the Internet: What could possibly go wrong?” video with Jeremy Pollard, Control Design. *Security DNA* podcast, SecurityInfoWatch.com.

PHOTOGRAPHY

Cover: Shutterstock AI. This content was generated by Shutterstock AI by an Artificial Intelligence (AI) system. Cyberattack concept: ID 133946276 © Shmeljov / Dreamstime.com. Wastewater plant aerial: ID 222664021 © Photovs / Dreamstime.com. Treatment plant at sunrise: Shutterstock. Valve and pressure gauge: ID 69956183 © Henrique Silva / Dreamstime.com. OT security concept: Wengen Ling. Critical infrastructure: Yitao / iStock / Getty Images Plus.

THE BRANDS IN THIS COLLECTION

WaterWorld serves the municipal drinking water industry.

Wastewater Digest covers municipal wastewater news, trends and regulations.

SecurityInfoWatch.com reports on physical and cybersecurity for security professionals.

Control Global serves technical and managerial professionals in the process industries.

Control Design serves machine builders and system integrators.

TechEDGE covers strategy, security and infrastructure for technology decision-makers.

ABOUT ENDEAVORB2B

EndeavorB2B operates the largest B2B newsroom in North America, serving industry professionals across water, energy, automation, security and technology.

ENDEAVORB2B®

KEEP READING

Six newsrooms. One critical infrastructure story.

Follow the reporting where it continues: in the plant, in the control room, and on the network.

WaterWorld waterworld.com

VISIT SITE

Wastewater Digest wwdmag.com

VISIT SITE

SecurityInfoWatch securityinfowatch.com

VISIT SITE

Control Global controlglobal.com

VISIT SITE

Control Design controldesign.com

VISIT SITE

TechEDGE tech.endeavoredge.com

VISIT SITE

© 2026 EndeavorB2B · All rights reserved