

September 2026

From IT breach to grid impact

What the Iran-linked PLC campaign means for utilities, and how to respond

Critical infrastructure risk is shifting from data exposure toward operational disruption. An ordinary IT compromise can now become a physical incident, and the distance between the two is shorter than most boards assume. Recent federal advisories and independent threat research point to a specific, achievable set of actions utilities can take now to limit exposure.

The PLC campaign is real, and it's expanding

In April 2026, CISA, the FBI, NSA, EPA, DOE, and U.S. Cyber Command warned that Iranian-affiliated actors were exploiting internet-exposed programmable logic controllers, initially concentrated on Rockwell Automation and Allen-Bradley devices. The July 22 update, which also involved the Treasury Department, expanded confirmed targeting to Schneider Electric and Siemens controllers. The confirmed targeting underscores the fact that this is no longer a single-vendor problem.

The pattern is not confined to one incident, or to water. More than 30 Minnesota water systems were disrupted in late July, with similar activity since confirmed across at least seven states. A separate December 2025 attack disrupted OT and communications systems at more than 30 wind, solar, and combined heat and power facilities in Poland. What stands out is not sophistication, but repeatability: shared third-party network configurations across victims may explain why the same technique kept working, a procurement and integrator problem as much as a technical one.

Independent researchers, including SentinelLABS, assess this activity as consistent with known Iran-affiliated patterns, but caution that consistency is not confirmed attribution. That distinction matters: regardless of who is behind any individual incident, the underlying exposure is well documented and addressable today.

What attackers actually did

Following one US attack, the FBI found a modified PLC project file that preserved normal ladder logic, so the device kept functioning and looked unremarkable while quietly overriding the instruction sets responsible for maintaining safe operating parameters. Attackers didn't shut anything down. They removed a safety guardrail while the system looked normal.

Priority actions

The following actions can be taken now to reduce risk, no matter where the threat comes from:

- Eliminate direct internet exposure for PLCs and other field controllers.
- Harden remote access and vendor/remote monitoring and management connectivity, especially shared integrator configurations.
- Restrict and monitor programming-mode changes, including reusable code modules.
- Preserve known-good configuration backups and rehearse manual operation cutovers.
- Map and restrict IT-to-OT trust pathways explicitly as part of the OT attack surface, not a separate conversation.
- Inventory AI touchpoints across engineering workflows and build governance early.

These actions map directly to NERC Critical Infrastructure Protection (CIP) obligations around remote access, configuration management, and incident response. The openings attackers are leveraging are largely ones utilities already have the ability to close.

The overlooked path: IT compromise becomes OT compromise

Utilities have historically treated IT and OT as separate risk domains, with separate teams and separate incident response plans. That separation made more sense when the two environments didn't talk to each other.

Independent research into the broader Iran-linked threat landscape finds that many intrusions don't begin with a novel OT exploit. They begin with something ordinary: a compromised remote monitoring tool, a trusted service-provider relationship, or an administrative credential that was never meant to carry this much authority. The question boards need to ask is no longer just how well OT is segmented; they must consider what IT-side access or vendor relationship could reach it.

AI is compressing timelines, not inventing new attacks

In widely reported incidents, AI agents operating in a testing environment escaped its intended constraints, used exposed credentials across multiple services, and chained several vulnerabilities together within a single session. The lesson: tasks that once took skilled teams days or weeks to complete can now be compressed into hours. This isn't hypothetical for the actors already discussed. Researchers assess that at least one recent destructive script used by an Iran-linked persona was likely AI-assisted, and these operators are already using generative tools to accelerate reconnaissance and execution.

There's a second side to this. Federal guidance published this year recognizes real operational value from AI inside OT environments. The utilities that get this right will inventory where AI already touches engineering workflows, establish governance early, and fold AI-specific failure modes into incident response planning.

Questions boards and management teams should be asking

Boards and management teams should focus on whether exposures are known, ownership is clear, and response capabilities are tested. Questions should include:

- Do we have a current inventory of internet-accessible PLCs and other field controllers, with accountable owners and time-bound remediation plans?
- Which IT credentials, remote-access tools, and third-party relationships can reach engineering workstations or OT systems, and when were those pathways last tested?
- Can we quickly detect and investigate unauthorized programming-mode changes or PLC logic changes, and compare them against known-good configurations?
- Have we rehearsed operating through a loss of remote access, including manual-operation cutovers, escalation thresholds, and decision rights?
- Does AI already touch engineering or OT workflows? And, if so, are incident-response expectations defined?

These questions move the discussion to whether controls exist to whether the utility can demonstrate that critical pathways are understood, monitored, and resilient under realistic operating conditions.

How CRA can help

CRA's Energy and Cybersecurity & Incident Response Practices work jointly with utilities and IPPs on both sides of this problem - responding to active OT-adjacent incidents and proactively assessing exposure before an incident happens. Two representative engagements illustrate our range:

1 Incident response (details anonymized)

A mid-size electric utility engaged CRA experts after detecting anomalous activity on a maintenance vendor's remote access account. An investigation traced the intrusion from a compromised third-party credential into the utility's engineering workstation network, with early signs of reconnaissance toward PLC-adjacent systems. CRA's incident response team contained the access, validated that no PLC logic had been altered, and worked with the client to rebuild vendor remote access controls and segment engineering networks from corporate IT before restoring normal operations.

2 Security hygiene assessment (details anonymized)

An independent power producer engaged CRA experts for a proactive OT security hygiene assessment ahead of a planned generation asset expansion. The review identified internet-reachable field devices and shared administrative credentials across multiple vendor-managed systems, exposures consistent with patterns seen in recent Iran-linked PLC campaigns. CRA worked with the client's engineering and IT teams to prioritize remediation, tighten remote access governance, and stand up a recurring external exposure review as part of their ongoing security program.

Sources: CISA Advisory AA26-097A (updated July 22, 2026); FBI public statements on multi-state water/wastewater PLC activity; SentinelLABS, "Iran War Cyber Threat Landscape: A Midyear Assessment on What Matters" (July 21, 2026); CISA, "Principles for the Secure Integration of Artificial Intelligence in Operational Technology"; CERT Polska energy-sector incident report; public reporting on the OpenAI/Hugging Face incident. Engagement examples are representative composites with anonymized and altered details; they do not describe a specific client or matter.

Contacts

To discuss how CRA's Energy and Cybersecurity & Incident Response Practices can help assess and strengthen your organization's OT resilience, contact:

Aniket Bhardwaj

Vice President
Dallas, Toronto
+1-416-323-5574
abhardwaj@crai.com

Andrew Dressel

Vice President
Salt Lake City
+1-801-536-1500
adressel@crai.com

Bill Hardin

Vice President, Practice Leader
of Forensic Services
Chicago
+1-312-619-3309
bhardin@crai.com

Kirsten Maw

Associate Principal
Salt Lake City
+1-801-536-1518
kmaw@crai.com



The views expressed in this paper are the views and opinions of the authors and do not reflect or represent the views of Charles River Associates or any of the organizations with which the authors may be affiliated. Detailed information about Charles River Associates, a trade name of CRA International, Inc., is available at www.crai.com.

Copyright 2026 Charles River Associates