Two Clocks Are Running on Utility Networks

> *Adversaries are already inside operational technology (OT), and a second, quieter deadline is arriving behind them. Research by TORII's Adv. RD&E Lab accepted for the IEEE International Conference on Quantum Computing and Engineering (QCE) 2026 examines whether both can be addressed within the determinism, bandwidth, and auditability constraints imposed by OT.*

By Theresa Melvin, JD, PhD
TORII Technology | TORII Defense | TORII Holdings (TORII)

Utility operators have spent the period since late 2023 absorbing a difficult lesson: the operational technology (OT) that runs water, power, and gas is reachable, and adversaries have learned to reach it.

In December 2023, a joint advisory led by the Federal Bureau of Investigation (FBI), with the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), the Environmental Protection Agency, and international partners, documented actors affiliated with the Islamic Revolutionary Guard Corps compromising internet-exposed programmable logic controllers (PLCs) at United States water and wastewater facilities. The technique required no exploit. The devices were internet-facing on default ports, and they carried either default passwords or no password at all. A December 2024 update to that advisory placed the count at no fewer than 75 devices, at least 34 of them in the U.S. water and wastewater sector.

In May 2024, a joint fact sheet on pro-Russia hacktivist activity described what happens once an adversary is past the door. Actors reached human-machine interfaces (HMIs) using default credentials, then drove water pumps and blower equipment beyond normal operating parameters, drove setpoints to maximum values, and turned off alarm mechanisms. Some victims experienced minor tank overflow events, though most reverted to manual control and restored operations promptly. The constraint on consequence, in other words, was operator response rather than adversary access. A December 2025 joint advisory extended that record, reporting that the most common operational impact was a temporary loss of view that forced operators to manage processes manually.

TORII HQ
7280 N.W. 87th Terrace,
Suite C-210, Kansas City,
Missouri 64153

TORII LABS
311 W. 22nd St – #222
Kansas City, Missouri
64108

TORII FEDERAL
Washington, D.C.
211 N Union St, Suite #100
Alexandria, VA 22314

(833) GOTORII · 468-6744 | engage@toriitechnology.us | torii.technology
TORII Holdings Group, LLC · TORII Technology Corp. · TORII Defense Inc.

The pattern sharpened again in 2026. A joint advisory on Iranian-affiliated exploitation of PLCs, first issued in April and updated in July, described actors modifying controller project files and manipulating what appeared on HMI and supervisory control and data acquisition (SCADA) displays. The July update added the finding that matters most to anyone responsible for safety systems: the changes "disabled critical shutdown and alarm logic, allowing systems to enter unsafe conditions without notifying operators of the anomalies."

THE SECOND CLOCK

Those advisories all describe a threat with the same kind of clock, one measured in hours. An adversary gains access to an OT device, and within hours the equipment begins to behave differently. There is a second clock, however; it runs much longer, and critical infrastructure is particularly exposed to it.

Operational telemetry is long-lived. Process data, setpoints, network topology, and the relationships between assets remain sensitive across asset lifecycles measured in decades. Traffic captured today can be stored and decrypted later, once the public-key cryptography protecting it fails. CISA, NSA, and the National Institute of Standards and Technology (NIST) named this directly in their August 2023 quantum-readiness guidance, describing adversaries who use a "catch now, break later" operation. That same guidance calls for a cryptographic inventory offering visibility into how an organization uses cryptography across both information technology (IT) and OT systems, and it gives explicit priority to industrial control systems and to systems with long-term confidentiality needs. A 2022 national security memorandum was blunter about the stakes for this sector, warning that a cryptographically relevant quantum computer (CRQC) could "undermine supervisory and control systems for critical infrastructure."

The timeline is no longer speculative. NIST published its first post-quantum standards — Federal Information Processing Standards (FIPS) 203, 204, and 205 — in August 2024. Draft NIST guidance proposes that today's RSA and elliptic-curve public-key algorithms be deprecated after 2030 and disallowed after 2035. Executive Order 14412, signed June 22, 2026, requires federal high-value assets and high-impact systems to transition to post-quantum key establishment by the end of 2030 and to post-quantum digital signatures by the end of 2031, and it directs the Sector Risk Management Agencies (SRMAs) to assist critical infrastructure owners and operators in developing their own migration plans. Utilities that assume this remains a federal-systems problem should read that last provision closely, because the SRMAs for energy and for water are the agencies utilities already work with.

TORII HQ
7280 N.W. 87th Terrace,
Suite C-210, Kansas City,
Missouri 64153

TORII LABS
311 W. 22nd St – #222
Kansas City, Missouri
64108

TORII FEDERAL
Washington, D.C.
211 N Union St, Suite #100
Alexandria, VA 22314

(833) GOTORII · 468-6744 | engage@toriitechnology.us | torii.technology
TORII Holdings Group, LLC · TORII Technology Corp. · TORII Defense Inc.

WHY UTILITIES CANNOT SIMPLY TURN ENCRYPTION ON

The obvious response — encrypt everything — collides with how OT actually works. A joint guide on adapting zero trust principles to operational technology, published in April 2026 by CISA, the Department of War, the Department of Energy, the FBI, and the Department of State, states the constraint plainly: most OT networks operate without authentication or encryption, and because many OT applications are time-sensitive, adding encryption without consideration of system constraints could disrupt operations. Where secure protocol support is unavailable, the same guide identifies the next best solution as wrapping legacy protocols in secure tunnels "so that encryption and authentication occur outside the control devices themselves." It also calls for encryption on all data flows into and out of the control network, with particular emphasis on flows traversing untrusted or third-party networks.

That is the design problem: protection strong enough to matter, bounded enough to field, and terminated somewhere other than the controller.

WHAT THE RESEARCH SHOWS

Research by TORII's Adv. RD&E Lab, accepted for the Quantum Networking and Communications track at the IEEE International Conference on Quantum Computing and Engineering (QCE) 2026, to be held in Toronto, September 13–18, treats this as an architectural question rather than solely an algorithm-selection question. Three coordinated layers sit at an industrial demilitarized zone (DMZ) gateway — the layer practitioners call Purdue Level 3.5 — where sessions terminate cryptographically and only evidence passes upward to enterprise governance.

The first layer is an always-on baseline built on a module validated to FIPS 140-3, with per-client tunnel selectors enforcing cryptographic isolation as policy rather than as general reachability. Each flow therefore retains a minimum protection level even when the adaptive layer is unavailable.

The second layer selects post-quantum session protection based on measured link conditions. Constrained cellular or remote edge devices receive a lower-overhead profile; plant local area network (LAN) and cloud nodes receive a stronger one. Cryptographic agility is treated as a bounded policy decision among approved profiles, not as unconstrained negotiation — a distinction that matters when a substation link and a control-center link cannot tolerate the same overhead.

The third layer treats the quality of the randomness feeding key establishment as a security control in its own right, measured continuously against an estimator modeled on NIST Special Publication (SP) 800-90B and exported as time-correlated evidence.

A live multi-node demonstration carried real SCADA traffic across both 10 Gb/s and 1 Gb/s link profiles. The demonstration reported post-quantum handshakes completing in single-digit

TORII HQ
7280 N.W. 87th Terrace,
Suite C-210, Kansas City,
Missouri 64153

TORII LABS
311 W. 22nd St – #222
Kansas City, Missouri
64108

TORII FEDERAL
Washington, D.C.
211 N Union St, Suite #100
Alexandria, VA 22314

(833) GOTORII · 468-6744 | engage@toriitechnology.us | torii.technology
TORII Holdings Group, LLC · TORII Technology Corp. · TORII Defense Inc.

milliseconds while estimated min-entropy held near the theoretical maximum, at approximately 7.9 of 8.0 bits per byte. Nuclear reactor telemetry — reactor power, generator output, coolant-loop temperatures, and pressurizer pressure — was modeled, carried within the protected channel, and bound per stream to a specific secured client. These results come from a software reference implementation exercised across both higher- and lower-capacity nodes. On more constrained field hardware, further limits on processing, memory, and cryptographic acceleration may reduce handshake speed and the strength of the profile in use.

THE EVIDENCE MODEL

The performance results are less consequential for utilities than the evidence model that accompanies them.

Electric utilities are audited against mandatory standards such as North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) 005, and utilities across sectors benchmark themselves against voluntary frameworks including International Electrotechnical Commission (IEC) 62443-3-3 and NIST SP 800-82 Revision 3. All of them are effective at establishing that a security control was configured correctly on the day an assessor looked. They are weaker at establishing that it has functioned continuously since. The 2026 advisory on Iranian-affiliated PLC exploitation describes adversaries who disabled alarm logic without notifying operators, and joint logging guidance warns that in some cases it can take up to 18 months to discover a cybersecurity incident, with malware dwelling on a network for 70 to 200 days before causing overt harm. Point-in-time attestation does not survive contact with that adversary.

The architecture exposes negotiated cryptographic posture, entropy health, and continuity of protection at runtime, through a dashboard and a restart-persistent audit trail. Neither packet capture nor privileged access to a live safety-critical system is required. An assessor can evaluate posture from exported evidence rather than by touching production, which is intended to reduce the operational disruption associated with assessing a live control environment. The architecture also defines a source-agnostic keying interface. External key material, including material delivered by future quantum key distribution services, can be consumed without redesigning the layered design. The intent is that utilities procuring gateway infrastructure on long replacement cycles need not commit, at the time of purchase, to either post-quantum cryptography or quantum networking to the exclusion of the other.

THREE QUESTIONS WORTH ASKING

First, does the cryptographic inventory include OT? Federal quantum-readiness guidance calls for visibility into cryptography across both IT and OT systems, and it names industrial control systems as a priority. An inventory that stops at the enterprise boundary does not meet that description.

TORII HQ
7280 N.W. 87th Terrace,
Suite C-210, Kansas City,
Missouri 64153

TORII LABS
311 W. 22nd St – #222
Kansas City, Missouri
64108

TORII FEDERAL
Washington, D.C.
211 N Union St, Suite #100
Alexandria, VA 22314

(833) GOTORII · 468-6744 | engage@toriitechnology.us | torii.technology
TORII Holdings Group, LLC · TORII Technology Corp. · TORII Defense Inc.

Second, can suppliers demonstrate posture at runtime, or only at configuration time? That question separates suppliers who have addressed assessment from those who have addressed documentation alone.

Third, is cryptographic agility a procurement requirement? Equipment purchased in 2026 will still be in service when NIST's proposed 2035 disallowance takes effect for federal and FIPS-validated use, and when procurement and insurance expectations have followed it. Whether that equipment can accept a new algorithm profile without an on-site field visit is decided at the purchase order, not afterward.

The threat advisories and the quantum timeline are usually treated as separate conversations. They are the same conversation. Both describe long-lived infrastructure protected by assumptions that no longer hold, and both are answered by the same discipline: protection that is layered, bounded by measured operating conditions, and provable while it runs.

Theresa Melvin, JD, PhD, is a Quantum Researcher and TORII's Founder. She can be reached at theresa@torii.technology (www.torii.technology)

The architecture described in this article is the subject of research conducted by the author's organization and of pending patent applications. Public references are limited to official standards, government guidance, and openly published research.