QCE26 · QNET · IEEE QUANTUM WEEK 2026

Securing Today's Industrial Traffic Against Tomorrow's Quantum Threat

Theresa Melvin, JD, PhD · Quantum Researcher & Founder, TORII

Most quantum-networking research looks years ahead. Our QNET-track poster paper for **IEEE Quantum Week 2026 (QCE26)** in Toronto examines a nearer-term question: how can industrial traffic that is **already being generated, stored, and moved today** be protected against future quantum attack?

1 The problem

Operational technology (OT) runs power grids, water utilities, pipelines, and nuclear plants, and it lives on long asset lifecycles. That makes it a prime target for **harvest-now, decrypt-later (HNDL)** attacks. Adversaries capture encrypted traffic now and decrypt it once quantum computers break today's public-key cryptography. For OT, the exposed data (operational state, set-points, system relationships) stays sensitive for years. Because these networks were engineered first for continuity and safety, any defense must coexist with existing transport and segmentation rather than replace them.

2 Approach and demonstration

The paper, *Quantum-Safe Edge-to-Cloud Communications for Constrained Operational Technology Networks*, describes **Q-Haven©**, a three-layer, defense-in-depth architecture mapped to the Purdue model at the Level 3.5 Industrial DMZ:

- **Baseline:** always-on FIPS 140-3 IPsec/IKEv2 protection.
- **Adaptive post-quantum sessions:** NIST-standardized ML-KEM and ML-DSA, with strength selected by measured link conditions.
- **Entropy assurance:** continuous validation from our QPP-RNG, exported as time-correlated evidence.

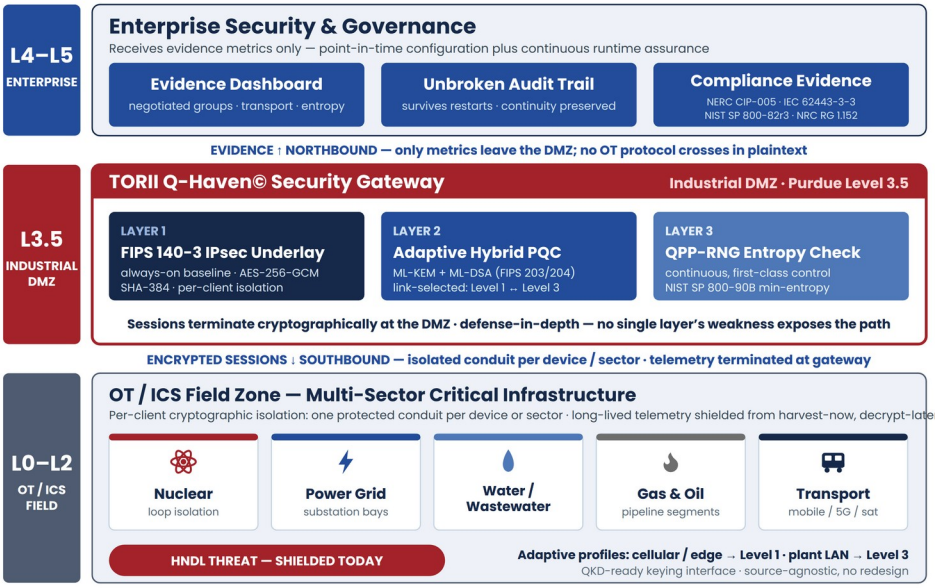


Fig. 1. Q-Haven© integrates three coordinated layers at a Purdue Level 3.5 Industrial DMZ gateway. Profile names illustrative; implementation internals omitted.

In a 1-server / 2-client demonstration carrying nuclear SCADA telemetry, we observed:

< 10 ms	**~7.9 / 8.0**	**NORMAL**
post-quantum handshakes	validated min-entropy, bits per byte (PASS)	SCADA telemetry status, end to end

3 Contributions and open questions

- **Quantum-safe protection as an observable property:** negotiated posture, entropy health, and telemetry continuity are measured at runtime rather than assumed from configuration.
- **Crypto-agility as bounded policy:** post-quantum strength adapts to measured link capacity, within a set of approved profiles.
- **A source-agnostic keying interface:** the same layered design can accept QKD-delivered keys as quantum networks mature.

Limitations. These results come from a software reference implementation. Constrained field hardware, with limited CPU, memory, and cryptographic acceleration, may bound achievable handshake rates and profile strength. Characterizing that boundary is a priority for our next phase.

Presenting at a peer-reviewed venue invites exactly this kind of scrutiny, and we welcome discussion from the QCE community. The design aligns with the following standards and guidance:

FIPS 140-3 | FIPS 203/204 | NIST SP 800-90B | NIST SP 800-82r3 | NSA CNSA 2.0 | NERC CIP-005 | IEC 62443-3-3 | NRC RG 1.152

FUTURE WORK

- Additional ML-KEM / ML-DSA parameter sets, plus alternative PQC families such as HQC and SLH-DSA for crypto-agile fallback.
- Live QKD key delivery through the source-agnostic keying interface.
- Extended NIST SP 800-90B validation of QPP-RNG entropy.

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

TORII Technology® Q-Haven© and QPP-RNG. Portions of this work are the subject of a pending patent application; implementation details are intentionally omitted.

PARENT

AUTHORING ENTITY

AFFILIATE

Theresa Melvin, JD, PhD
Quantum Researcher & Founder, TORII
theresa@torii.technology
www.torii.technology
IEEE Quantum Week 2026 · Toronto

www.torii.technology