JUNE 2026
APPLIED QUANTUM

# THE APPLIED QUANTUM PQC MIGRATION FRAMEWORK

## CRITICAL NATIONAL INFRASTRUCTURE & OPERATIONAL TECHNOLOGY EXTENSION

***Energy, Utilities, Water, Transportation, and Industrial Control Systems*** *— Industry-Specific Challenges and Framework Adaptations*

Version 2.1 — June 2026

**Marin Ivezic**

CEO, Applied Quantum

Author, PostQuantum.com

**PQCFramework.com | PQCMigrationBrief.com | PostQuantum.com | SecureQuantum.com | AppliedQuantum.com | QuantumReady.com**

*"Start while it's a project, before it's a crisis."*

# COPYRIGHT AND LICENSE



# DISCLAIMER

This extension is provided as professional guidance based on the author's and Applied Quantum's practitioner experience and publicly available standards, regulations, and industry research. It does not constitute legal, regulatory, financial, or compliance advice. This document does not contain or reference any classified information. Organizations should consult appropriate classification authorities, legal counsel, and regulatory bodies for guidance specific to their jurisdiction, classification level, and operational context.

The regulatory timelines, vendor capabilities, algorithm parameters, and tool categories referenced in this document reflect the state of the PQC landscape as of March 2026. This landscape evolves rapidly. Readers should verify current status against primary sources (NIST, NSA, CISA, IEC, NERC, national agencies, vendor documentation) before making implementation decisions.

References to specific vendors, products, or tools are for illustrative purposes and do not constitute endorsement.

NIST IR 8547, referenced throughout for deprecation and disallowance timelines, was an Initial Public Draft as of November 2024 with final publication expected in 2025–2026. Federal agencies and their contractors should reference the final published version when available.

# ABOUT THIS DOCUMENT

| | |
|---|---|
| **Document type** | Enterprise methodology and practitioner framework |
| **Parent Document** | The Applied Quantum PQC Migration Framework — Universal — v2.1 (June 2026) |

| | |
|---|---|
| **Intended audience** | CISOs, OT security managers, control system engineers, compliance officers, and program managers in energy, utilities, water, transportation, and industrial organizations |
| **Assumed knowledge** | Familiarity with the Universal PQC Migration Framework and its 8-phase lifecycle; working knowledge of ICS/SCADA architectures, Purdue Model, and OT security principles |
| **Scope** | Industry-specific challenges and phase-by-phase framework adaptations for OT-operating critical national infrastructure. Not a standalone document — intended to be used alongside the Universal Framework. |

# VERSION HISTORY

| Version | Date | Changes |
|---|---|---|
| 1.1 | March 2026 | Initial publication as a companion to the Universal Framework v1.1. |
| 2.1 | June 2026 | Major alignment release tracking Universal Framework v2.1 (June 2026), adopting the v2.0 structural foundations and the v2.1 positions in a single release. New Alignment with Universal Framework v2.1 section (two-track model with Track B leading, FIPS validation gap compounded by safety certification, Merkle Tree Certificates relevance, and six v2.1 position subsections). New Challenge 11 (Process Historians and Long-Horizon Operational Data); Challenge 10 extended with the EU coordinated roadmap dates and the COM(2026) 13 NIS2 proposal. Algorithm-specific vulnerability weighting added to Phase 3 risk scoring. Regulatory map gains the CISA OT guidance and updated EU timelines; Further Reading updated. Section title corrected. Companion book (Quantum Ready) cross-reference added. |

# HOW TO USE THIS EXTENSION

This document is a companion to the Applied Quantum PQC Migration Framework (Universal). It does not replace the Universal Framework but extends it with

telecommunications-specific guidance. For each topic, this extension identifies unique sector challenges and then maps specific adaptations to the relevant Universal Framework phase. Readers should have the Universal Framework open alongside this document and cross-reference its phase definitions, maturity indicators, and templates.

## WHAT'S NEW IN V2.1

Version 2.1 of the CNI/OT Extension is a major alignment release tracking Universal Framework v2.1 (June 2026). Because the extension moves directly from v1.1, it adopts the Universal v2.0 structural foundations and the v2.1 positions in a single release:

**Alignment with Universal Framework v2.1.** A new alignment section maps the two-track migration model (with the OT inversion: Track B leads), the FIPS validation gap compounded by safety certification, and the Merkle Tree Certificates position onto OT estates, followed by six v2.1 position subsections: hybrid and composite signatures under OT constraints; algorithm weighting and why modern OT is the early target; machine identity in industrial networks; SP 800-208 firmware signing as the deploy-now OT action; CBOM protection as sabotage-targeting data; and verification, decommissioning, and the decades-long tail. The remaining Universal v2.1 additions are sector-neutral and apply as written; the alignment section introduction lists them and the governing cross-references.

**New and extended challenges.** Challenge 11 (Process Historians and Long-Horizon Operational Data) brings the Universal data-at-rest decision framework to the OT data estate. Challenge 10 gains the EU coordinated roadmap dates (national strategies end-2026, high-risk and critical use cases by 2030, the rest by 2035) and the COM(2026) 13 proposal to write PQC transition planning into NIS2.

**Currency and corrections.** The regulatory alignment map gains the CISA/DHS OT guidance and updated EU timelines; Further Reading reflects the June 2026 state. The opening section title, which incorrectly carried the Government & Defense wording, was corrected. A cross-reference to the companion book, Quantum Ready, was added.

## ACCOMPANYING RESOURCES

Every aspect of this framework (from executive business cases and cryptographic inventory methodologies to CBOM architecture, hybrid deployment patterns, and vendor governance) has been analyzed in detail on PostQuantum.com over the past 10+ years through practitioner-grounded articles, deep dives, and sector-specific analyses.

The best starting point is the curated Quantum Readiness Starting page: https://postquantum.com/quantum-readiness-starting/, but readers should also use PostQuantum.com's Search function to surface additional relevant posts that may not be included in that curated list.

Key framework resources, templates, and supporting materials are also published on PQCFramework.com, a dedicated companion site for this framework, drawing on relevant content from PostQuantum.com.

# TABLE OF CONTENTS

# WHY CNI AND OT REQUIRE A SECTOR EXTENSION

The Universal PQC Migration Framework provides a comprehensive 8-phase methodology applicable to any enterprise. Critical national infrastructure operators can and should follow that methodology. However, organizations with significant OT environments face a different set of constraints that make PQC migration slower, riskier, and more dependent on compensating controls than in IT-centric enterprises. These constraints do not invalidate the Universal Framework: they add urgency to some phases, extend timelines for others, and introduce safety considerations that most enterprises never encounter.

## Safety-Critical Operations Where Failure Has Physical Consequences

The defining characteristic of OT environments is that cryptographic failure can cause physical harm. Unlike IT systems where a compromise primarily threatens data confidentiality or business continuity, a compromise in OT can cause equipment damage, environmental contamination, service outages affecting millions of people, or loss of human life. A forged firmware signature on a safety instrumented system (SIS) could disable safety interlocks. A compromised VPN key on a SCADA link could enable unauthorized control commands to a dam, a gas pipeline, or a power grid substation.

This safety dimension changes the risk calculus for PQC migration. Every cryptographic change must be evaluated not just for technical correctness but for its impact on safety cases, process integrity, and regulatory safety certifications (IEC 61508, IEC 61511, ISA 84). The Universal Framework's Phase 5 (Pilots) and Phase 6 (Infrastructure) must incorporate safety assessment processes that are foreign to most IT migration programs.

## Trust Now, Forge Later (TNFL) as the Primary Threat

While most quantum risk discussions focus on Harvest Now, Decrypt Later (HNDL) (the confidentiality threat), OT environments face a more dangerous quantum threat: Trust Now, Forge Later (TNFL). TNFL targets digital signatures and authentication, not encryption. A quantum adversary who can forge signatures could inject malicious

firmware into PLCs, impersonate authorized engineering workstations, forge safety system certificates, or manipulate code-signing chains.

In OT, integrity is more critical than confidentiality. A plant operator can tolerate some data exposure far more easily than unauthorized modification of control logic. This means the Universal Framework's risk scoring (Phase 3) must weight signature and authentication functions more heavily than encryption in OT environments.

## Extreme Equipment Lifecycles and Constrained Hardware

OT equipment routinely operates for 15–30 years, with some installations exceeding 40 years. Many devices run on processors with limited memory (sometimes measured in kilobytes), no operating system patches available, and fixed cryptographic implementations burned into firmware or hardware. PQC algorithms impose significant overhead: ML-KEM public keys are approximately 1,200 bytes (vs. 32 bytes for X25519), ML-DSA-65 signatures are approximately 3,300 bytes (vs. 64 bytes for ECDSA). Many OT devices simply cannot handle these sizes and must be protected through network-layer compensating controls rather than endpoint upgrades.

## Limited Patching Windows and Rigid Change Control

OT environments operate under strict change management regimes. Firmware updates on safety-critical systems may require factory acceptance testing, site acceptance testing, safety validation, and regulatory re-certification. Patching windows may be limited to planned annual shutdowns. PQC migration cannot follow the IT model of rolling updates: cryptographic changes must be planned around maintenance windows that may be 12–18 months apart, and each change must pass through safety and reliability validation processes.

## Weak Cryptographic Visibility

Many OT environments have poor visibility into what cryptography is actually in use. Legacy industrial protocols (Modbus, DNP3, older PROFINET) were designed without cryptographic protection. Where cryptography exists, it is often embedded in vendor firmware and not documented. The asset discovery problem that underpins the entire framework is amplified in OT by shadow devices, undocumented protocol converters, and equipment where the vendor's documentation does not disclose the cryptographic libraries in use.

### Heavy Vendor Dependency with Fragmented Markets

OT operators depend on specialized vendors (Siemens, ABB, Schneider Electric, Honeywell, Emerson, Rockwell/Allen-Bradley, GE Vernova, Yokogawa) for their control system hardware and software. Unlike IT, OT cryptographic implementations are deeply embedded in vendor products and cannot be changed without vendor cooperation. A single plant may have equipment from 10–20 different vendors across different generations of technology.

### Converging IT/OT Architectures Creating Expanded Attack Surface

Modern OT environments are no longer air-gapped. The convergence of IT and OT through industrial IoT, cloud-based SCADA, remote monitoring, and enterprise integration has expanded the cryptographic attack surface dramatically. Every IT-to-OT connection point uses quantum-vulnerable cryptography. The IT/OT boundary protections (DMZ firewalls, jump servers, VPN concentrators) must be among the first systems migrated to PQC.

# INDUSTRY-SPECIFIC CHALLENGES

This section details the technical and operational challenges unique to PQC migration in OT-operating critical infrastructure. Each challenge is presented with its technical basis, real-world context, and the Universal Framework phases it most directly impacts.

## CHALLENGE 1: FIRMWARE SIGNING AND SECURE BOOT VULNERABILITY

OT devices rely on digital signatures to verify firmware authenticity at boot and during updates. Vendor firmware is typically signed with RSA-2048 or ECDSA keys. A quantum adversary who can forge these signatures could craft malicious firmware that passes verification, establishing persistent compromise of control systems. This is the TNFL threat in its most dangerous form. Remediation is complicated because the signature verification logic is embedded in boot ROM or firmware. Updating the trust anchor requires a firmware update, which itself must be verified using the existing quantum-vulnerable mechanism.

> **Framework Impact:** Phase 1 must inventory all firmware signing mechanisms and trust anchors across the OT estate. Phase 5 must include firmware signing migration pilots with key OT vendors. Phase 7 must require vendors to publish PQC firmware signing roadmaps.

## CHALLENGE 2: SAFETY INSTRUMENTED SYSTEM CERTIFICATION CONSTRAINTS

Safety instrumented systems operate under rigorous certification frameworks (IEC 61508/61511, ISA 84) that govern how changes can be made. Any modification to the cryptographic stack of a SIS may trigger re-certification requirements, expensive (potentially hundreds of thousands of dollars per device type) and time-consuming (months to years). This creates a perverse incentive: the most safety-critical systems are the hardest and slowest to migrate. Compensating controls become essential interim measures.

> **Framework Impact:** Phase 3 must flag SIS-certified systems as highest-risk/lowest-agility. Phase 4 must model safety re-certification timelines. Phase 5 must use boundary-protection approaches for SIS zones while native PQC migration is pending.

## CHALLENGE 3: INDUSTRIAL PROTOCOL CRYPTOGRAPHIC POVERTY

Many widely-deployed OT protocols (Modbus, DNP3, BACnet, early PROFINET) transmit data in plaintext with no authentication or integrity protection. More modern protocols (OPC UA, IEC 62351, Secure DNP3) do incorporate TLS and X.509 certificates, all quantum-vulnerable. The result is a bimodal challenge: some OT communications have no cryptography to migrate, while others have quantum-vulnerable cryptography that must be upgraded.

> **Framework Impact:** Phase 1 must categorize OT protocols as “no cryptography,” “quantum-vulnerable,” or “symmetric-only.” Phase 5 must prioritize adding PQC-protected overlay encryption to currently unprotected critical OT links.

## CHALLENGE 4: REMOTE ACCESS AND VPN DEPENDENCY

Critical infrastructure operators increasingly rely on remote access VPNs for monitoring, diagnostics, vendor support, and emergency response. These use IPsec or TLS-based VPNs with quantum-vulnerable key exchange. Remote access VPNs to OT networks are among the highest-value targets for both HNDL and future real-time quantum attack. The good news is that VPN concentrators are typically IT-managed equipment, making them the most accessible early-migration target.

> **Framework Impact:** Phase 3 must weight OT remote access VPNs as Tier 1 priority. Phase 5 should target VPN concentrators as the first production PQC deployment. Phase 7 must track VPN vendor PQC timelines.

## CHALLENGE 5: SUBSTATION AUTOMATION AND GRID PROTECTION

Electrical grid operators face a unique combination of scale, criticality, and protocol complexity. IEC 61850 relies on TLS and X.509 certificates for GOOSE message authentication and MMS communications. Grid protection relays (devices that detect faults and trip circuit breakers within milliseconds) are among the most time-critical

devices in any OT environment. Any PQC-related latency increase could compromise protection coordination, potentially leading to cascading grid failures.

> **Framework Impact:** Phase 1 must inventory IEC 61850/62351 deployments and protection relay firmware. Phase 6 must benchmark PQC overhead against protection relay timing requirements. Phase 7 must engage grid equipment vendors.

## CHALLENGE 6: SCADA WIDE-AREA NETWORK EXPOSURE

SCADA systems monitoring geographically distributed assets (pipelines, water distribution, transmission lines, railway signaling) communicate over WANs that traverse public infrastructure. These links use IPsec, TLS, or proprietary encryption with quantum-vulnerable key exchange. Pipeline SCADA, water utility SCADA, and rail signaling SCADA all transmit commands with direct physical safety implications.

> **Framework Impact:** Phase 1 must map SCADA WAN encryption endpoints. Phase 3 must score SCADA WAN links for both HNDL and TNFL exposure. Phase 6 must test PQC overhead against SCADA polling and response time requirements.

## CHALLENGE 7: LONG-LIVED CERTIFICATES AND PKI IN OT

OT environments commonly use certificates with validity periods of 10–20 years because the operational cost and risk of renewal on deployed field devices is high. These certificates will be quantum-vulnerable well within their validity period. Rotating certificates in OT is not routine: many field devices lack automated certificate management and renewal may require physical access and planned outages.

> **Framework Impact:** Phase 2 (CBOM) must capture certificate validity periods and renewal mechanisms. Phase 4 must plan certificate migration campaigns aligned with maintenance windows. Phase 6 must address OT-specific PKI automation gaps.

## CHALLENGE 8: VENDOR LOCK-IN AND PROPRIETARY CRYPTOGRAPHIC STACKS

OT vendors frequently use proprietary cryptographic implementations, proprietary protocols, and closed firmware. The operator's PQC migration timeline for embedded OT

devices is entirely determined by the vendor's product roadmap. Some OT vendors do not even document which algorithms are used in their products.

> **Framework Impact:** Phase 2 must include vendor disclosure requests and CBOM generation through passive network observation. Phase 7 must include PQC-upgradability clauses in all new OT procurement contracts.

## CHALLENGE 9: PHYSICAL SECURITY AND ENVIRONMENTAL CONSTRAINTS

OT equipment operates in environments ranging from offshore platforms and underground mines to nuclear facilities and Arctic pipelines. Physical access for hardware upgrades is expensive, dangerous, and sometimes impossible without planned shutdowns. Equipment in hazardous environments may require ATEX/IECEx certification, adding certification dependency to any hardware change.

> **Framework Impact:** Phase 4 must model physical access and environmental constraints for each OT zone. Phase 6 must assess which devices require hardware replacement vs. firmware update vs. compensating controls.

## CHALLENGE 10: REGULATORY FRAGMENTATION ACROSS CNI SECTORS

Critical infrastructure regulation varies dramatically by sector, jurisdiction, and asset class. Energy operators face NERC CIP, EU NIS2, and nuclear-specific requirements. Water utilities face EPA requirements and the Drinking Water Directive. Transportation operators face TSA directives and sector-specific railway/aviation safety standards. Organizations operating across multiple CNI sectors must navigate overlapping regulatory requirements.

> **Framework Impact:** Phase 0 must map all applicable CNI regulations and their quantum/cryptographic requirements. Phase 4 must align with the most demanding regulatory timeline.

The EU clock is now explicit. The NIS Cooperation Group's Coordinated Implementation Roadmap (June 2025) sets dates: Member States start national transitions with strategies by the end of 2026, high-risk and critical use cases migrate by the end of 2030, and the remainder by 2035 where practically feasible. COM(2026) 13, proposed in February 2026, would write PQC transition planning into NIS2 itself as a named component of national cybersecurity strategy, converting what was an interpretive argument about "state-of-the-art" cryptography into an explicit obligation flowing from directive to national strategy to supervisory expectation. For EU critical infrastructure operators, "the most demanding regulatory timeline" in this challenge now has numbers attached: plan critical use cases to 2030.

## CHALLENGE 11: PROCESS HISTORIANS AND LONG-HORIZON OPERATIONAL DATA

OT programs treat data at rest as an IT problem, and the OT data estate proves them wrong. Process historians hold years to decades of time-series telemetry; engineering repositories hold PLC logic, control narratives, and P&IDs; alarm and event archives record how the plant behaves under stress. Exfiltrated and decrypted later, these archives are HNDL against industrial intellectual property, plant and grid topology, and operational patterns an adversary can study at leisure. The exposure is widening, not shrinking: historian replication to corporate data lakes and cloud analytics platforms moves decades of operational data across exactly the boundaries an adversary can reach.

The confidentiality horizon for this data is driven by the life of the asset, not the age of the record: a plant's topology remains sensitive for as long as the plant operates. The Universal Framework's data-at-rest decision framework (Activity 5.6) applies per store: PQC key-wrap for archives too large to re-encrypt, re-encryption for active tiers, and deletion only with records-retention sign-off, with backup generations aging out under a documented schedule while new generations are written under PQC-protected keys.

**Framework Impact:** Phase 1 data classification must include historian estates, engineering repositories, and their replication paths, with confidentiality horizons set from asset life. Phase 5 applies the Activity 5.6 strategy choice per data store and records it in the CBOM. Phase 6 capacity planning must account for re-encryption at historian scale, which is a throughput problem before it is a cryptographic one.

# ALIGNMENT WITH UNIVERSAL FRAMEWORK V2.1

The Universal Framework v2.0 (June 2026) introduced structural changes with specific implications for OT-operating critical infrastructure, and v2.1 added positions and sections that operators need to map onto their programs. Because this extension moves directly from v1.1 to v2.1, this section covers both: the v2.0 foundations below, followed by the v2.1 positions that require OT-specific adaptation. The remaining Universal v2.1 additions (the data-at-rest decision framework in Activity 5.6, the AI-assisted migration position in 5.7 with its Phase 1 tool category, cloud and SaaS shared responsibility in 7.7, the risk-weighted coverage KPI, algorithm sovereignty and standards fragmentation, crisis communications, the skills matrix, and Appendices G and H) apply as written, with three notes. The data-at-rest framework lands on the OT data estate through Challenge 11 (historians and engineering data). The counterparty coordination pattern in Activity 7.6 is the general case of interconnected-operator coordination: grid interties, shared pipelines, and rail interchanges connect operators who exchange live telemetry and commands but cannot compel each other, and the pattern's dual-stack windows and deprecation protocol apply to those interconnects directly. And the Accelerated Execution Profile (Activity 4.7) meets a hard OT boundary: compression is bounded by maintenance windows and safety approvals, so the OT version of the profile pre-approves accelerated compensating-control deployment (segmentation, gateway insertion, key-lifetime reduction) rather than compressed device migration that the safety case will not permit.

## Two-Track Migration Model in OT: Track B Leads

The Universal Framework's two tracks map onto OT with the priorities inverted. Track B (Integrity / Signatures / PKI) leads, because TNFL is the primary OT threat: firmware signing and secure boot, control-command authenticity, device identity certificates, and configuration signing protect the property that matters most in OT, which is that the system does only what its operators intend. Track A (Confidentiality / Key Exchange) covers remote access VPNs, vendor support tunnels, and SCADA wide-area backhaul; the

HNDL exposure on telemetry is real (topology and operational patterns are valuable, as Challenge 11 details) but secondary to forged commands and counterfeit firmware. Where the Universal default sequences Track A first for most sectors, OT programs should run Track B's first move (SP 800-208 firmware signing) at the front of the program, alongside rather than after the Track A VPN work.

## FIPS Validation Gap Compounded by Safety Certification

The Universal Framework's deployment environment classification meets a second gate in OT. Most OT estates classify as FIPS-aware at best, but safety-certified systems form a class of their own: even a CMVP-validated cryptographic module waits for safety recertification (IEC 61508 SIL levels, sector safety cases) before it can be deployed, and the safety authority's clock does not care about NIST's. Sequence accordingly: pilot on non-safety systems and on gateways in front of safety systems now, and treat safety-system cryptographic changes as the long pole whose vendor and certification lead times Phase 4 must carry explicitly. The documented-risk-acceptance route exists in OT, but a risk acceptance never overrides a safety case.

## Merkle Tree Certificates: Limited OT Relevance

The Universal position on Merkle Tree Certificates concerns the public Web PKI. OT touches that world only at its edges: vendor cloud portals, browser-based remote HMIs, and corporate-side dashboards will follow the browser ecosystem's fork on the browser ecosystem's schedule. Private OT PKIs (device identity hierarchies, IEC 62443-style zone certificates) are operator-controlled and unaffected by MTC; their fork is the long-validity certificate problem this extension already covers in Challenge 7. Do not let Web PKI developments distract OT planning, and do not assume they exempt the browser-facing edge.

## Hybrid and Composite Signatures Under OT Constraints

The Universal v2.1 default is composite or dual signatures, with solo deployment recorded as a risk decision. In OT the default holds where size and compute allow: firmware images can usually carry dual signatures, and gateway TLS can run hybrid. It breaks at the constrained edge: protocol-level signatures on field devices and legacy serial-attached equipment often cannot fit a second signature at all. Record those as documented solo decisions per the Universal position, pair them with compensating controls (segmentation, gateway termination), and note that for firmware signing the hash-based route (SP 800-208) sidesteps the lattice-implementation-maturity concern

that motivates composites in the first place; conservative hash-based cryptography suits OT safety culture.

## Algorithm Weighting: Modern OT Is the Early Target

The Universal v2.1 weighting position (quantum attack cost tracks key size, not classical strength) produces a counterintuitive OT result: the newest equipment is the most quantum-urgent. Modern OT and IIoT devices adopted ECC precisely because it is constrained-device-friendly, so greenfield device identity and secure-channel deployments sit on 256-bit curves while legacy estates sit on RSA-2048 or on no cryptography at all. At equal criticality, weight the ECC-based modern estate at least as early as the RSA legacy, and resist the instinct that newer equals safer; in quantum resource terms the opposite ordering applies.

## The Identity Stack: Machine Identity in Industrial Networks

The Universal v2.1 identity-stack addition translates in OT to machine identity: device certificates in IEC 61850 substations and OPC UA deployments, 802.1X on industrial LANs, engineering workstation and jump-host authentication, and the PAM credentials that gate remote access. All of it is Track B, all of it depends on the OT PKI whose long-validity certificate problem Challenge 7 describes, and re-enrollment of device estates rides maintenance windows like every other OT change. Inventory the machine-identity estate explicitly; it is where TNFL meets the network.

## SP 800-208 Firmware Signing: The Deploy-Now OT Action

Challenge 1 of this extension is firmware signing; the Universal v2.1 makes SP 800-208 stateful hash-based signatures (LMS/XMSS) the deploy-now component of Track B, and the two meet. The standards are final, validated implementations ship, and hash-based signatures carry none of the lattice novelty that makes conservative OT engineering hesitate. The operator's lever is procurement: firmware signing migrates at the vendor, so the new OT procurement requirements in this extension's Phase 7 adaptations should require LMS/XMSS-signed firmware with verifier support in new equipment now. The state-management caveat (stateful schemes must never reuse a signing state) argues for vendor HSM-backed signing services rather than ad hoc key handling.

## Securing the CBOM: Targeting Data for Physical Consequences

Universal Activity 2.5 treats the CBOM as a high-value intelligence target. The OT version is sharper: a CBOM that maps which controllers accept which signatures, which firmware is forgeable, and which compensating controls exist is sabotage targeting data with physical consequences. Treat the OT CBOM as sensitive operational information (in some regimes, handling akin to critical energy infrastructure information applies), partition access by site and role, log access, and design the SOC integration so that machine-readable does not become broadly readable.

## Verification, Decommissioning, and the Decades-Long Tail

The Universal v2.1 closure standard (evidence of migration, destruction of classical material, formal transition to business-as-usual) meets OT's defining constraint: a tail of non-migratable devices measured in decades. The OT closure artifact is therefore twofold. For migrated systems, the standard evidence applies, and decommissioning classical material includes vendor-escrowed keys and recovery material, not only operator-held copies. For the non-migratable tail, the compensating-control registry is itself a closure artifact: each entry carries the control, the residual risk acceptance, and a re-evaluation date, so that "closed" means accounted for under a documented control regime rather than migrated. Both evidence streams feed the safety case and the regulator.

# PHASE-BY-PHASE FRAMEWORK ADAPTATIONS FOR CNI AND OT

This section specifies the adaptations required for OT-operating critical infrastructure. Implement these alongside the Universal Framework's phase guidance.

## Phase 0 — Executive Mandate & Business Case

### Additional Business Case Arguments

- **Safety case:** Frame quantum risk in terms of physical safety consequences. A forged firmware signature on a safety system is not a data breach; it is a potential industrial accident.
- **Critical infrastructure designation:** Position PQC readiness as proactive compliance with the trajectory of NIS2, NERC CIP, TSA Security Directives, and sector-specific regulations.
- **TNFL-specific urgency:** Emphasize TNFL over HNDL. The board message: "The signatures protecting our safety systems will be forgeable by quantum computers. The devices most at risk are the ones we cannot easily update."
- **Insurance and liability:** Cyber insurance for CNI operators now asks about cryptographic modernization plans. Failure to demonstrate quantum readiness planning may affect coverage.

### Governance Adaptation

Establish a Quantum Readiness Steering Committee that includes OT Engineering, IT Security, Process Safety, Regulatory Compliance, and Procurement. OT engineering and process safety must have co-equal status with IT security. Include the Chief Engineer or Director of Operations, not just the CISO.

## Phase 1 — Discovery & Inventory

### OT-Specific Inventory Tracks

- **Control system inventory:** PLCs, RTUs, DCS controllers, SIS controllers, protection relays, IEDs, by vendor, model, firmware version, and cryptographic capabilities.
- **SCADA/HMI inventory:** SCADA servers, HMI workstations, historian servers, data concentrators. Identify TLS/SSH configurations and authentication mechanisms.
- **Network infrastructure:** OT firewalls, VPN concentrators, data diodes, protocol converters, serial-to-IP gateways. Primary targets for early PQC migration.
- **Field device communications:** Map which OT protocols are in use and which have cryptographic protection enabled.
- **Vendor firmware catalog:** Document the firmware signing mechanism, vendor's public key, and key algorithm for each OT vendor/product.
- **Certificate inventory:** All X.509 certificates in OT, including validity periods, key algorithms, and renewal mechanisms.

### The Asset Discovery Problem in OT

OT asset discovery is fundamentally harder than IT. Shadow devices, undocumented protocol converters, legacy serial devices bridged to IP, and decades-old equipment all contribute to incomplete inventories. Passive network monitoring can help identify communicating devices but will not reveal cryptographic implementation details. Active scanning is often prohibited due to device fragility. The framework must accept that OT cryptographic inventory will be incomplete and use risk-driven scoping.

## Phase 2 — CBOM & Documentation

### OT CBOM Challenges

Generating CBOMs for OT is harder than IT because vendor disclosure is limited and cryptographic implementations are embedded in proprietary firmware. Apply the Minimum Viable CBOM approach: document what can be observed and tag the rest as "vendor-opaque — disclosure requested." Prioritize boundary devices and devices with known firmware signing mechanisms.

### Purdue Model Alignment

Organize CBOM documentation by Purdue Model level. Tag each entry with its Purdue level (0–5) and its zone/conduit classification per IEC 62443. This facilitates zone-by-zone migration planning.

## Phase 3 — Risk Scoring & Prioritization

### Adapted Risk Scoring Model

For CNI/OT, add three dimensions to the Universal Framework's risk scoring:

- **Safety impact:** Could compromise lead to physical harm, environmental damage, or loss of life? SIS, protection relays, and emergency shutdown systems score highest.
- **TNFL exposure:** Is this a signature/authentication function (high TNFL) or encryption (HNDL)? In OT, TNFL generally scores higher.
- **Upgrade feasibility:** Can this device's cryptography be updated in the field, or does it require hardware replacement or safety re-certification?

**Algorithm-specific weighting:** Apply the Universal Framework v2.1 vulnerability weighting in OT scoring: quantum attack cost tracks key size rather than classical strength, so modern ECC-based device identity and secure channels weigh at least as urgent as legacy RSA at equal criticality. See the alignment section's Algorithm Weighting subsection.

### CNI/OT Priority Tiers

| Priority | System Category | Rationale |
|---|---|---|
| Tier 1 | IT/OT boundary: VPN concentrators, jump servers, DMZ firewalls, remote access gateways | Highest external exposure. Operator-controlled IT equipment. Can migrate without OT vendor dependency. |
| Tier 2 | SCADA WAN encryption, historian/enterprise integration TLS, OPC UA server certificates, cloud SCADA | High WAN exposure. Mix of IT-managed and vendor-managed. Migration possible with vendor firmware updates. |
| Tier 3 | Firmware signing trust anchors, secure boot chains, DCS/PLC device identity certificates | Highest TNFL risk. Requires vendor cooperation and potentially safety re-certification. Plan now, execute when ready. |
| Tier 4 | Legacy field devices (no crypto), serial endpoints, devices in hazardous environments | Cannot be natively migrated. Apply compensating controls: segmentation, overlay encryption, physical isolation. |

## Phase 4 — Roadmap & Governance

### Maintenance Window Alignment

OT migration roadmaps must be aligned with planned maintenance windows. Cryptographic changes to safety-critical devices cannot be deployed during normal operations. Map each activity to the next available maintenance window and build the roadmap around these windows.

### Recommended Year-1 Plan

- **Q1:** Secure joint CISO/Chief Engineer sponsorship. Begin Tier 1 inventory. Issue PQC readiness RFIs to top-5 OT vendors. Begin regulatory pre-engagement.
- **Q2:** Complete IT/OT boundary inventory. Begin hybrid PQC VPN pilot on non-production link. Map maintenance windows for next 24 months.
- **Q3:** Complete SCADA WAN encryption inventory. Begin OT CBOM generation. Initiate vendor firmware signing roadmap discussions.
- **Q4:** Deliver first board report with TNFL risk assessment. Publish internal OT PQC policy. Begin Tier 2 planning.

## Phase 5 — Pilots & Migration Execution

### OT Pilot Sequence

- **Pilot 1 — IT/OT boundary VPN:** Migrate a remote access VPN concentrator to hybrid PQC IPsec. IT equipment, operator-controlled, lowest risk.
- **Pilot 2 — SCADA WAN link:** Deploy hybrid PQC on a non-critical monitoring-only telemetry link. Test latency against SCADA polling requirements.
- **Pilot 3 — OPC UA server:** Enable PQC-TLS on OPC UA in a staging environment. Verify client compatibility and throughput.
- **Pilot 4 — Firmware signing (lab):** Test PQC firmware signing (LMS/XMSS or ML-DSA) on a representative device in a lab.
- **Pilot 5 — Certificate migration:** Migrate certificates on non-safety OT devices to hybrid PQC. Test renewal and revocation.

### Compensating Controls for Non-Migratable Devices

- **Quantum-safe VPN gateways:** Deploy PQC-capable VPN appliances at zone boundaries to encrypt all traffic regardless of endpoint capability.
- **Network segmentation hardening:** Strengthen IEC 62443 zones and conduits to limit blast radius of any quantum-enabled compromise.

- **Out-of-band firmware validation:** For critical devices where firmware signing cannot be upgraded, implement out-of-band PQC signature validation using a separate appliance.
- **Physical isolation:** For the most critical legacy devices, maintain or restore true air gaps where operationally feasible.

## Phase 6 — Infrastructure Modernization & Performance

### OT-Specific Performance Constraints

- **Protection relay timing:** Grid relays must operate within single-digit millisecond latency. Benchmark PQC overhead against these requirements.
- **SCADA polling cycles:** 1–10 second cycles. PQC key exchange must not cause polling timeouts.
- **Real-time control loops:** Sub-second DCS control loops. PQC must not introduce destabilizing jitter.
- **Constrained device memory:** Test PQC library footprint on representative OT hardware. Consider lightweight implementations (LMS/XMSS).

### HSM and Key Management

OT environments often have separate or minimal key management infrastructure. PQC migration requires establishing quantum-safe key management for OT certificate issuance, firmware signing keys, and VPN pre-shared keys. Engage HSM vendors early.

## Phase 7 — Vendor & Supply Chain Governance

### OT Vendor Classification

- **Tier A — Timeline-blocking:** PLC/RTU/DCS vendors (Siemens, ABB, Schneider, Honeywell, Emerson, Rockwell), SIS vendors, protection relay vendors. Engage at executive level.
- **Tier B — Timeline-influencing:** SCADA software, historian vendors, OPC UA stack providers, OT network equipment. Standard vendor management.
- **Tier C — Operator-controlled:** IT/OT boundary equipment, internally developed integration applications, custom HMI configurations.

### New OT Procurement Requirements

- **PQC-upgradability clause:** Vendor must demonstrate a PQC roadmap or provide firmware-upgradable cryptographic modules.
- **CBOM disclosure:** Vendor must provide a Cryptographic Bill of Materials for all products.

- **Hybrid mode support:** Vendor must support hybrid classical+PQC operation during the transition period.

# CNI/OT REGULATORY ALIGNMENT MAP

| Authority / Standard | Requirement | Timeline | CNI/OT Implication |
|---|---|---|---|
| NIST / CNSA 2.0 | Deprecate classical asymmetric; adopt ML-KEM, ML-DSA | 2030 deprecation, 2035 disallowance | Affects all TLS/IPsec. Mandatory for operators serving US government or defense. |
| EU NIS2 Directive | Essential entities must implement state-of-the-art security | Transposition Oct 2024; EU roadmap: national strategies end-2026, high-risk and critical use cases by 2030, remainder by 2035; COM(2026) 13 proposes PQC as a named NIS2 obligation | Energy, transport, water are essential entities. PQC increasingly expected. |
| NERC CIP | Critical infrastructure protection for bulk electric system | CIP-013, CIP-005, CIP-007 updates | Supply chain risk (CIP-013) and electronic security perimeters (CIP-005) must incorporate quantum risk. |
| IEC 62443 | Industrial automation and control systems security | Series ongoing | Zone/conduit security requirements. PQC expectations will evolve. |

| | | | |
|---|---|---|---|
| TSA Security Directives | Pipeline and rail cybersecurity mandates | SD-02D, rail directives ongoing | Requires cybersecurity implementation plans. Quantum risk increasingly relevant. |
| IEC 62351 | Security for power system protocols | Parts published, evolving | Defines TLS/cert profiles for DNP3, IEC 61850. PQC updates will drive grid migration. |
| Nuclear regulators | Cyber security for nuclear facilities | 10 CFR 73.54 (US), national variants | Most restrictive change management. PQC for nuclear OT will be slowest. |
| CISA / DHS | Post-Quantum Considerations for Operational Technology; quantum-readiness migration guidance for ICS | Published November 2024; ongoing | First dedicated federal OT PQC guidance. Anchors segmentation, crypto-agile procurement, and gateway expectations for ICS; cite it in business cases and vendor requirements. |

# CNI/OT MATURITY MODEL SUPPLEMENT

The Universal Framework's 5-level maturity model with sector-specific indicators:

| Level | Universal Indicator | CNI/OT-Specific Indicator |
|---|---|---|
| Level 1: Aware | Executive sponsorship; quantum risk acknowledged | Joint CISO/Chief Engineer sponsorship. TNFL risk communicated to safety governance. Regulatory pre-engagement initiated. |
| Level 2: Assessed | Inventory complete for priority systems; CBOM initiated | IT/OT boundary inventory complete. Firmware signing cataloged. SCADA WAN mapped. Purdue-aligned CBOM initiated. |
| Level 3: Planning | Risk-scored roadmap approved; pilots designed | Multi-track roadmap approved. Maintenance window alignment complete. Compensating control plan defined. |
| Level 4: Migrating | Hybrid PQC in production; CBOM maintained | Tier 1 boundary migrated. SCADA WAN PQC rollout in progress. Compensating controls deployed for Tier 4. |
| Level 5: Resilient | Crypto-agile; all crypto remediated or compensated | All accessible OT crypto PQC-protected or compensated. Safety-certified devices migrated. CBOM maintained across Purdue levels. |

# CNI/OT KPI SUPPLEMENT

## Board-Level KPIs (Quarterly)

- **Boundary protection PQC coverage:** Percentage of IT/OT boundary connections protected by PQC or hybrid cryptography.
- **TNFL exposure index:** Number of safety-critical systems with quantum-vulnerable firmware signing, weighted by safety impact score.
- **Vendor PQC readiness:** Percentage of Tier A OT vendors with confirmed PQC firmware delivery dates within 24 months.
- **Compensating control coverage:** Percentage of non-migratable OT devices protected by compensating controls.
- **Regulatory compliance trajectory:** Gap analysis score against NIS2, NERC CIP, IEC 62443, and sector-specific mandates.

## Operational KPIs (Monthly)

- **OT cryptographic inventory coverage:** Percentage of Purdue levels (0–5) with completed cryptographic inventory.
- **CBOM freshness:** Percentage of CBOM entries verified within last 90 days.
- **PQC pilot progress:** Number of pilot phases completed vs. planned. Safety validation results.
- **Firmware signing migration readiness:** OT vendor product lines with PQC firmware signing capability / total in estate.
- **Certificate migration progress:** OT certificates migrated to PQC or hybrid / total OT certificates.

# RECOMMENDED IMMEDIATE ACTIONS

- **1. Secure joint CISO/Chief Engineer mandate.** Frame quantum readiness as a safety and integrity issue. Use the TNFL threat to firmware signing as the urgency metric.
- **2. Inventory your IT/OT boundary immediately.** Catalog every VPN concentrator, jump server, DMZ firewall connecting IT to OT. Document TLS/IPsec configurations. These are Tier 1 targets.
- **3. Catalog firmware signing mechanisms for critical OT devices.** For SIS controllers, protection relays, critical PLCs: who signs firmware, what algorithm, where is the verification key, can it be updated?
- **4. Issue PQC readiness RFIs to top OT vendors.** Ask for PQC firmware timelines, hybrid mode support, and trust anchor update procedures for deployed devices.
- **5. Deploy a hybrid PQC VPN pilot on a non-production OT link.** Select a monitoring-only telemetry link. Deploy hybrid ML-KEM + X25519 IPsec. Measure latency and compatibility.
- **6. Map maintenance windows for the next 24 months.** Every planned outage and turnaround is a migration opportunity. Missing them means waiting another 12–18 months.
- **7. Engage your sector regulator proactively.** Brief them on your quantum readiness planning. Solicit guidance on how PQC migration intersects with safety certifications.

# FURTHER READING

- **Upgrading OT Systems to PQC: Challenges and Strategies** — https://postquantum.com/post-quantum/ot-pqc-challenges/
- **Trust Now, Forge Later (TNFL) — The Overlooked Quantum Threat** — https://postquantum.com/post-quantum/trust-now-forge-later/
- **The Challenge of IT and OT Asset Discovery** — https://postquantum.com/post-quantum/asset-discovery-challenge/
- **Harvest Now, Decrypt Later (HNDL) Risk** — https://postquantum.com/post-quantum/harvest-now-decrypt-later-hndl/
- **PQC Is Necessary, But Not Sufficient** — https://postquantum.com/post-quantum/pqc-not-everything/
- **Mitigating Quantum Threats Beyond PQC** — https://postquantum.com/post-quantum/mitigating-quantum-threats-pqc/
- **Hybrid Cryptography for the Post-Quantum Era** — https://postquantum.com/post-quantum/hybrid-cryptography-pqc/
- **Introduction to Crypto-Agility** — https://postquantum.com/post-quantum/introduction-crypto-agility/
- **Infrastructure Challenges of Dropping In PQC** — https://postquantum.com/post-quantum/infrastructure-challenges-pqc/
- **PQC and Network Connectivity: Challenges and Impacts** — https://postquantum.com/post-quantum/pqc-network-impacts/
- **Common Failures in a Quantum Readiness Program** — https://postquantum.com/post-quantum/common-failures-quantum-readiness/

CISA’s Post-Quantum OT Guidance: Key Takeaways and Next Steps for CISOs — https://postquantum.com/quantum-policy/dhs-cisa-pqc-ot/ — Analysis of the first dedicated federal OT PQC guidance.

NIS2, DORA, and the EU Post-Quantum Roadmap — https://postquantum.com/quantum-policies/nis2-dora-pqc-quantum/ — The EU regulatory chain from the coordinated roadmap to entity-level obligations.

Quantum Ready (companion book) — https://quantumready.com — The executive and governance dimensions of quantum readiness, complementing this framework’s technical methodology.

# ABOUT

## ABOUT THE AUTHOR

Marin Ivezic is a former Fortune Global 500 CISO/CTO, the Editor-in-Chief of PostQuantum.com, and the founder and CEO of Applied Quantum. He previously held cybersecurity partner and practice lead roles, including regional and global leadership positions, at IBM, Accenture, PwC, and KPMG. He is also the former CEO of Cyber Agency and the founder of Cryptosec, a cryptography advisory and engineering firm.

Marin has been involved in quantum technologies for over 25 years, having advised governments on the quantum threat since the early 2000s. He previously founded Boston Photonics and PQ Defense. He has led real-world quantum readiness programs for telecoms, financial institutions, and critical infrastructure operators, including programs exceeding 120,000 discrete migration tasks.

PostQuantum.com, his personal blog, reaches over 1 million monthly readers and is recognized as the premier quantum security publication for CISOs, CTOs, and security architects worldwide.

## QUANTUM READY: THE COMPANION BOOK

*Quantum Ready* (QuantumReady.com) is the book-length companion to this framework, written by the same author. Where this document is deliberately methodology-grade (prerequisites, activities, outputs, decision logic). The book provides the complete treatment: the reasoning behind each phase, extended case examples from real migration programs, sector narratives, and guidance for leading the program from the first board conversation through closure. The two are maintained in alignment: the framework is updated as the field moves, and the book supplies the depth that a methodology document omits by design.

## ABOUT APPLIED QUANTUM

Applied Quantum (AppliedQuantum.com) is a research-driven professional services firm focused entirely on quantum technologies and post-quantum security. Its dedicated security practice, Secure Quantum (SecureQuantum.com), focuses on quantum security

advisory and PQC migration. Services span Quantum Security & PQC Migration, Quantum Strategy & Sovereignty, Quantum Engineering & Implementation, and Quantum Commercialization.

If you need help: Applied Quantum provides advisory, program design, and hands-on migration execution support. Contact: contact@appliedquantum.com