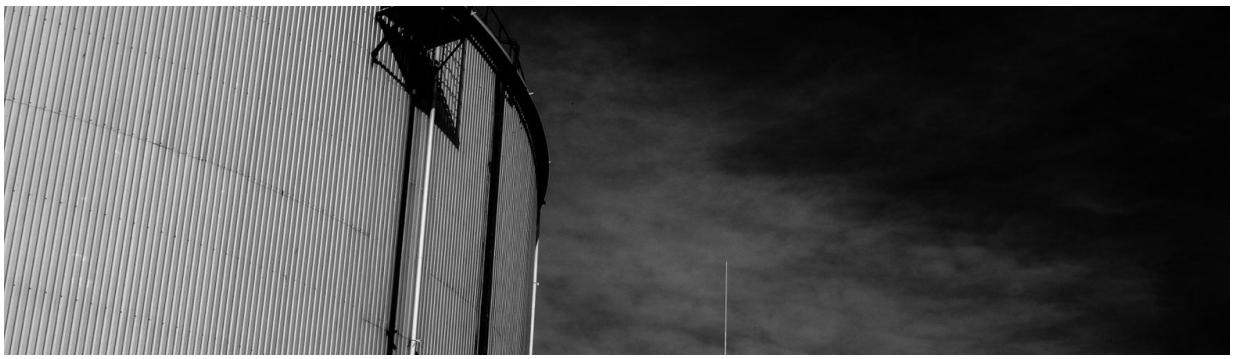
SEPTEMBER 2026

APPLIED QUANTUM

THE APPLIED QUANTUM PQC MIGRATION FRAMEWORK

OT & CRITICAL INFRASTRUCTURE EXTENSION



Industrial control systems, utilities and critical national infrastructure – *sector-specific challenges and framework adaptations*

Version 3.0 – September 2026

Marin Ivezic

CEO, Applied Quantum

Author, PostQuantum.com

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

COPYRIGHT AND LICENSE

DISCLAIMER

This framework 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. Organizations should consult qualified legal counsel, auditors, and regulatory authorities for guidance specific to their jurisdiction, sector, and circumstances.

The regulatory timelines, vendor capabilities, algorithm parameters, and tool categories referenced in this document reflect the state of PQC as of September 2026. These references may become outdated quickly. Readers should verify current status against primary sources before making implementation decisions; movement between editions is published through the PQC Migration Brief.

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, remains an Initial Public Draft at the date of this edition; the deprecation and disallowance dates it proposes are cited as anchors and re-checked at each release. Federal agencies and their contractors should reference the final version when it publishes.

ABOUT THIS DOCUMENT

Document type	Enterprise methodology and practitioner framework
Parent document	The Applied Quantum PQC Migration Framework – Universal – v3.0 (September 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 v3.0 and its 8-phase lifecycle; working knowledge of ICS/SCADA architectures, the Purdue Model, IEC 62443 zones and conduits, and OT safety-certification processes
Scope	Industry-specific challenges and phase-by-phase framework adaptations for OT-operating critical national infrastructure, including

	the facilities estate inside every enterprise. Not a standalone document – intended to be used alongside the Universal Framework.
Status	Version 3.0 - published September 2026

VERSION HISTORY

Version	Date	Changes
2.0	June 2026	Major version. Three methodological changes: (1) two-track migration model separating key exchange (HNDL) and signature/PKI (TNFL) as parallel tracks; (2) PKI architecture fork with definitive position on Merkle Tree Certificates for public Web PKI; (3) FIPS 140-3 validation gap as hard deployment constraint with environment classification. New Program Foundation sections: SOC Implementation (five detection use cases, four incident response playbooks, five tabletop exercises, three-horizon quantum CTI model), GRC Implementation (17-indicator cascading KRI framework, risk appetite statements, regulatory intelligence process, audit and assurance, GRC-SOC handoff). Expanded Program Foundations: Governance (program leadership, board oversight, three lines of defense), Crypto-Agility (five-dimensional operational discipline with four-year implementation roadmap), Skills & Team Structure (team sizing, build/borrow/buy framework, crypto champion program). Also added: cost estimation methodology, NIST CSWP 39 crypto-agility alignment, 2026–2030 regulatory deadline convergence analysis, multinational hybrid navigation framework, deployment ecosystem status data, algorithm pipeline update (9 additional signature candidates, FN-DSA/HQC status, CNSA 2.0 requirements), objection-handling appendix (Appendix F). All sector extensions updated to v2.0.
2.1	June 2026	Targeted update. Activity 3.3 sequencing harmonized with the two-track model; explicit position on hybrid/composite signatures; algorithm-specific vulnerability weighting added to Phase 3 risk scoring (ECC/RSA quantum resource analysis); SP 800-208 hash-based signatures foregrounded as the deploy-now component of Track B. New: Activity 2.5 (Secure the CBOM and Program Artifacts), Migration Verification & Program Closure section, identity and authentication stack in Track B scope. Added: reference program economics (0.2c), confidentiality-horizon method (1.1), evidence dossier as litigation defense, M&A due diligence, procurement model-

Version	Date	Changes
		language references, additional common failures and benefit arguments. Web PQC adoption datapoint corrected to F5 Labs mid-2025 attribution. Companion book (Quantum Ready) cross-references added. Also added: data-at-rest decision framework (5.6); AI-assisted migration position (5.7) with a Phase 1 tool category; counterparty coordination (7.6); cloud shared responsibility and SaaS (7.7); Accelerated Execution Profile (4.7); risk-weighted coverage KPI; algorithm sovereignty and standards fragmentation; crisis communications and industry information sharing (GRC); skills matrix; role-based reading paths and right-sizing profiles; Appendix G (framework crosswalk); Appendix H (protocol coverage matrix).
3.0	September 2026	Major version, published with Universal v3.0. Crypto-agility as the program's method read for OT estates: the agility objective stated for the sector (algorithms changed on a date the operator can plan, at the gateway layer the operator controls without reopening a certified boundary), the agility criterion and a rehearsal per wave on the gateway, issuer and firmware-signing service, "migrated with agility debt" as the expected recorded state for the vendor-locked population, and closure at zero unaccepted agility debt with the compensating-control registry as the home of the accepted exceptions. Two artifacts the Universal cites by name: the cryptographic ownership register (Phase 1; The Cryptography Nobody Owns as a new sector characteristic) and the Encapsulate strategy (Phase 5; permanent and bridge enclosure, what the pattern does not cover, agility-debt state per entry). The facilities estate as a sector characteristic and its own discovery scope; the Modbus payload arithmetic in Challenge 3; four execution failure modes in Phase 5; the OT tender template as the deploy-now procurement action in Phase 7, requirement categories agility first. Alignment section rebuilt on v3.0: validation decided per product (CMVP #5247) with the safety case as a decision per change; three new subsections (the agility criterion and rehearsal; evidence grades and the coverage denominator; vendor dates and questions). Phase adaptations mirror the v3.0 method: dual-outcome charter and named owners (Phase 0); evidence grades and the enumerated denominator (Phase 1); the minimum record with the Profile as informative carriage (Phase 2); the OT factors restated inside Dimensions 2 and 3

Version	Date	Changes
		with the arithmetic and a delivery-state column (Phase 3); two results per gate record and the Re-Baseline Protocol (Phase 4); the four-field register with entropy references (Phase 6); questionnaire order, certificate-authority questions, the one-afternoon test and firmness grades (Phase 7). Challenge 10 restructured under E1 with the ANSSI qualification gate (2027) as the sector's procurement-gate example; the regulatory map restructured with status and enforcement-tier columns and the jurisdiction roster replaced by the Global PQC Migration Clock pointer. Corrections: CISA OT guidance dated October 2024 (was November); COM(2026) 13 dated January 20, 2026 (was February). Control-system vendor names moved to Tool and Vendor References. Maturity supplement on the Universal's 0 to 5 scale; four agility KPIs; three immediate actions added. Requirements register generated as Appendix J. About block aligned to the Universal.

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 guidance specific to OT-operating critical infrastructure: industrial control systems, safety-instrumented systems, grid and SCADA estates, and the facilities estate inside every enterprise. 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 V3.0

Version 3.0 of the OT & Critical Infrastructure Extension publishes with Universal Framework v3.0 (September 2026). Crypto-agility is the program's organizing method and measured end state, and this extension states the ruling for OT: crypto-agility in OT means changing algorithms on a date the operator can plan, and the gateway layer is where that property is achievable, so the agility criterion and the rehearsal per wave run on the gateway, the OT issuer and the firmware-signing service, "migrated with agility debt" is the expected recorded state for the vendor-locked device population, and closure requires zero unaccepted agility debt with the compensating-control registry as the home of the accepted exceptions. Regulatory content states the mechanism and the sector's own instruments with status and enforcement tier; the jurisdiction roster is in the Universal's Regulatory Timeline Context and on the Global PQC Migration Clock page.

This is the substantive content release among the extensions. Two sector characteristics are added: The Cryptography Nobody Owns (in OT, certificates, keys and embedded credentials arrived inside equipment nobody in the operator's organization chose, and they have to be claimed before they can be migrated) and The Facilities Estate (every enterprise operates OT inside its own buildings). Two

artifacts the Universal already cites by name are written: the cryptographic ownership register (Phase 1), which maps every embedded credential, certificate store and signing dependency to a named owner with a RACI and is the program's first contact with OT operations and engineering; and the Encapsulate strategy (Phase 5), grown from the compensating controls of the June 2026 edition, with the criteria for permanent and bridge enclosure, what the pattern does not cover, and an agility-debt state on every entry. Challenge 3 states the payload arithmetic: an ML-DSA-44 signature of 2,420 bytes against a Modbus protocol data unit of at most 253 bytes, which forces the placement decision to the session layer, the gateway or the conduit. Challenges 3, 5 and 6 state where each secured industrial protocol runs its asymmetric cryptography: OPC UA over `opc.tcp` on its own SecureChannel per SecurityPolicy, with the RSA policies' RSA key transport and its absence of forward secrecy scored on Dimension 1 and Pilot 3 restated as a SecurityPolicy change; IEC 61850 with GOOSE and Sampled Values under the symmetric MAC of IEC 62351-6:2020 and the substation's exposure in the IEC 62351-9 key management layer and the TLS-protected MMS flows; and DNP3 Secure Authentication as a predominantly symmetric application-layer mechanism whose standard, IEEE 1815-2012, has been Inactive-Reserved since March 30, 2023 with its successor unpublished. Phase 5 adds four execution failure modes (the reconnect storm; testing without an outage; bricking and rollback; the dual-stack decade). Phase 7 adds the OT tender template as the deploy-now procurement action, its requirement categories ordered agility first. Challenge 10 is restructured under the three deadline archetypes, with the EU chain matched to the Universal's wording and ANSSI's 2027 qualification gate as the sector's procurement-gate example; the June 2026 Forescout Research – Vedere Labs device-class measurement is cited as a data source to calibrate the OT gap.

Alignment section and adaptations. The alignment section is rebuilt on v3.0: the validation subsection states the per-product, per-operation, per-certificate rule, with CMVP certificate #5247 (Go Cryptographic Module, Level 1 software, April 2026, ML-KEM-768 and ML-KEM-1024) and #5497 (Crypto4A QASM, Level 3 hardware, August 2026, carrying ML-DSA and LMS), states the FIPS 140-2 Historical transition of September 21, 2026 as CMVP's permission for existing systems, and makes safety-case recertification a decision per change rather than a blanket rule; the SP 800-208 subsection narrows the availability claim to the one LMS parameter set #5497 evidences, with state safety as an acceptance item and CNSA 2.0's recommendation of LMS and XMSS beside its approval of ML-DSA-87 for firmware signing; the verification subsection is rewritten to the four verification dispositions and closure at zero unaccepted debt, with the closure proof run on the gateway layer and the firmware-signing service; and three subsections are added: the agility criterion and rehearsal in OT; evidence grades and the coverage denominator in OT; vendor dates and questions in OT. The phase adaptations mirror the v3.0 method where this extension already adapts the element: the dual-outcome charter and the Crypto-Agility and Cryptographic Record owners (Phase 0), evidence grades and the enumerated denominator on the inventory tracks (Phase 1), the minimum record with the Applied Quantum CBOM Profile as informative carriage (Phase 2), the OT factors restated inside Dimensions 2 and 3 with the Universal's arithmetic, verifier updatability as the strongest agility-debt indicator, the priority tiers re-derived from the Universal's ordered test (firmware signing, safety functions and non-updatable device identity at Tier 1 with their bridging patterns named) and a delivery-state column (Phase 3), two results per gate record and the Re-Baseline Protocol for dates the operator does not control (Phase 4), the rehearsal per wave and the wave-exit criterion (Phase 5), the four-field HSM and KMS register with entropy references and the SP 800-208 section 8 conditions on the signing module (Phase 6), and the questionnaire order, the certificate-authority questions for vendor-issued device certificates, the one-afternoon test against proprietary stacks and firmness grades on every date (Phase 7).

Supplements, corrections and currency. The maturity supplement is re-based on the Universal's 0 to 5 scale with the Universal's level names, and the KPI supplement gains the four agility KPIs measured on the gateway layer, with the non-updatable-verifier population as the burn-down denominator. Three immediate actions are added: open the cryptographic ownership register, name a Crypto-Agility owner in engineering, and schedule the first rehearsal on the pilot concentrator. Two dates are corrected in the open: CISA's Post-Quantum Considerations for Operational Technology was published in October 2024, not November; COM(2026) 13 was tabled on January 20, 2026, not in February. Control-system vendor names move from the body to Tool and Vendor References. The regulatory map gains status and enforcement-tier columns and points to the maintained roster. Further Reading adds the July 2026 HNDL analysis, the June 2026 device-class data, the ANSSI and NIS2 analyses and the Global PQC Migration Clock. Appendix J lists the extension's own requirements.

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.

TOOL AND VENDOR REFERENCES

This framework references specific tools, products, and vendors as illustrative examples to help practitioners understand the categories of capability available. A mention does not constitute an endorsement, recommendation, or assessment of fitness for any particular environment. The PQC tooling market is evolving rapidly; products mentioned may have changed in capability, licensing, or availability since publication. Organizations should conduct their own evaluation based on their specific requirements, regulatory environment, and procurement constraints.

The body of this edition names categories and capability requirements. Commercial vendors appear in the body only where a dated public fact is itself the evidence (a measurement, an announcement, a published roadmap). The references below carry the names the body relied on in the June 2026 edition, verified September 2026, and are maintained on PQCFramework.org between editions.

Control-system vendors (sector characteristics; Phase 7, Tier A): the June 2026 edition named Siemens, ABB, Schneider Electric, Honeywell, Emerson, Rockwell Automation (Allen-Bradley), GE Vernova and Yokogawa as the timeline-blocking class of the installed base. As of September 2026 the list describes the installed base this extension was written against; it is not an assessment of any vendor's PQC readiness, which is established per product through the questionnaire in Phase 7 and graded for firmness.

Device-population measurement used as a data source (sector characteristics; Phase 5): Forescout Research – Vedere Labs, "PQC Adoption Gaps: 90% of Systems Are Still Not Quantum-Safe", June 24, 2026, an internet-wide and enterprise-network measurement of PQC-capable SSH and TLS by device class.

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 Getting Started with Quantum Security and PQC Migration page: https://postquantum.com/starting-pqc-quantum-security/, 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.org, a dedicated companion site for this framework, drawing on relevant content from PostQuantum.com.

Two sibling Applied Quantum properties carry work this framework cites rather than repeats. The Applied Quantum CBOM Profile, the property taxonomy layered on CycloneDX that Phase 2 cites by minimum version, publishes at CBOMProfile.org. The Cryptographic Concentration Framework, which measures cryptographic concentration beneath the vendor layer and consumes a Profile-conforming CBOM, publishes at CCFramework.org. Both are open under CC BY 4.0 and follow this framework's sector taxonomy.

This framework is the execution methodology. For the complete treatment (the reasoning behind each phase, extended case examples, and guidance for leading the program from the first board conversation through closure), see the companion book, *Quantum Ready* (QuantumReady.com). Quantum Academy (QuantumAcademy.com), founded by the author, offers trainings and certifications on the topics this framework covers, for the roles and training levels described in Skills & Team Structure.

The PQC Migration Brief (pqcmigrationbrief.com) carries corrections, standards and regulatory movement between editions, and the current jurisdiction roster is maintained on the Global PQC Migration Clock page on PostQuantum.com; the framework itself remains free and ungated.

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 requires assessment against safety cases, process integrity, and regulatory certifications (IEC 61508, IEC 61511, ISA 84) alongside its technical correctness. Phase 5 (Pilots) and Phase 6 (Infrastructure) must incorporate assessment processes that most IT migration programs never encounter.

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 algorithm outputs dwarf their predecessors: ML-KEM public keys are approximately 1,200 bytes (vs. 32 bytes for X25519), ML-DSA-65 signatures 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 (the Encapsulate strategy, Phase 5). Software updates will not close the gap on their own. One dated measurement calibrates how wide it is: the June 2026 internet-wide and enterprise-network measurement by Forescout Research – Vedere Labs, used here as a data source, found PQC-capable SSH on 16% of OT devices in enterprise networks against 50% of IT devices, PQC-capable TLS on 0.8% of OT devices against 8% of IT devices, and two-thirds of OT devices both high-risk and not PQC-capable on TLS; at the observed pace the measurement projects no asset class fully migrated by 2029. The figures describe capability in an observed population, not a migration rate.

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, with patching windows sometimes 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, and the largest message the most widely deployed of them permits is smaller than a post-quantum signature (Challenge 3). 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.

The Cryptography Nobody Owns

In IT, cryptographic assets have owners because the security organization deployed them. In OT, certificates, keys and embedded credentials arrived inside equipment purchased by engineering, commissioned by integrators and maintained by vendors. No function in the operator's organization chose them, and the ability to change them is often held by the vendor or the integrator, not the operator. Before OT cryptography can be inventoried, prioritized or migrated it has to be claimed, an organizational act the IT-derived phases assume has already happened. This extension introduces the cryptographic ownership register (Phase 1) and makes the register conversation the program's first contact with OT operations and engineering.

Heavy Vendor Dependency with Fragmented Markets

OT operators depend on a small set of specialized control-system vendors for their hardware and software. The vendors named in the June 2026 edition are listed in the front-matter Tool and Vendor References. 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.

OT in Every Enterprise's Facilities Estate

The OT estate this extension covers is not confined to plants, grids and pipelines. Every enterprise operates an OT estate inside its own buildings: access control, building management, elevators, fire and life-safety panels, CCTV and the controllers behind them, almost none of it owned by the security team or present in the CMDB. In one corporate head office, a walkdown identified more than 160 distinct categories of connected device, most of them provisioned by facilities management or the building owner.

That count is engagement experience, not a published statistic, and the population differs by building. What transfers is that the facilities estate is a discovery scope of its

own (Phase 1), with its own owners to engage before the walkthrough and its own gateway and encapsulation patterns (Phase 5). An enterprise with no plant still has this estate, and the Universal's Phase 1 points it here.

INDUSTRY-SPECIFIC CHALLENGES

Each challenge below states its technical basis, real-world context, and the Universal Framework phases it most directly affects.

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, with a firmness grade on every date.

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. A modification to the cryptographic stack of a SIS may trigger re-certification, 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.

Whether a given change reopens the safety case is decided per change, with the safety authority, against the change's effect on the safety function. The decision is recorded

with the change: a gateway inserted in front of the SIS zone, a key-lifetime reduction or a certificate renewal outside the certified boundary usually does not. A firmware change to the SIS controller usually does. The per-change record is what the safety authority and the auditor ask for. Compensating controls are the interim measure, and for some SIS populations the permanent one (the Encapsulate strategy, Phase 5).

Framework Impact: Phase 3 must score SIS-certified systems Critical on physical consequence, which places them at Tier 1 under the ordered test, with the change path scored per device from the recertification decision (Hard where the change reopens the safety case or needs a hardware replacement; Medium where the safety authority accepts it as a firmware campaign inside a maintenance window) and the delivery state blocked until the vendor's certified release exists where one is required. Phase 4 must model safety re-certification timelines and record the recertification decision per change. Phase 5 must use the Encapsulate strategy 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. The more modern protocols use quantum-vulnerable public-key cryptography, and each uses it in its own place. OPC UA over the binary `opc.tcp` mapping runs OPC UA's own SecureChannel rather than TLS. Its SecurityPolicy decides whether the session keys are established by RSA key transport with no forward secrecy, or by ephemeral ECDH; TLS applies only to the `opc.https` and `opc.wss` mappings (Phase 3, OPC UA and forward secrecy).

IEC 62351 protects station-bus MMS traffic with TLS and X.509 certificates and secures GOOSE and Sampled Values with a symmetric MAC whose keys a certificate-based key management layer distributes (Challenge 5). DNP3 Secure Authentication is an application-layer mechanism, predominantly symmetric, separate from any TLS on the transport, and the standard behind it is inactive (Challenge 6). The result is a bimodal challenge: some OT communications have no cryptography to migrate, while others have quantum-vulnerable cryptography that must be upgraded. The second class is migrated where its asymmetric operation actually runs.

For the first class the arithmetic settles where a signature cannot go. The Modbus application protocol limits a protocol data unit to 253 bytes. An application data unit is 256 bytes on serial lines and 260 bytes over TCP (Modbus Application Protocol Specification V1.1b3). An ML-DSA-44 signature is 2,420 bytes (FIPS 204), roughly ten times the largest message the protocol permits. An FN-DSA-512 signature of about 666 bytes (the Falcon-512 round-3 value; FIPS 206 is under development with no published draft and no published date, and the size may move) still exceeds it several times over.

A post-quantum signature therefore does not fit inside the protocol data unit, and that is all the arithmetic shows: it does not rule out a secure encapsulation or a gateway design that carries the unmodified protocol inside a post-quantum-protected conduit. The program places the protection instead: at the session layer where a secure protocol variant exists, at a gateway in front of the zone (the Encapsulate strategy, Phase 5), or in segmentation that keeps the unauthenticated traffic inside a conduit the gateway controls.

Each segment and each endpoint is modeled separately and recorded in the CBOM as native, tunneled or terminated, with the component that bears the post-quantum processing load and the classical leg that remains named on the entry. A device behind a terminating gateway does not process the gateway's post-quantum handshake. Its own session, buffers and polling are untouched by the gateway's algorithm. The gateway's outward leg is where the handshake sizes and timings are measured (Phase 6).

Framework Impact: Phase 1 must categorize OT protocols as "no cryptography," "quantum-vulnerable," or "symmetric-only," and for a quantum-vulnerable protocol record where the asymmetric operation runs and whether its key establishment has forward secrecy. Phase 5 must prioritize adding PQC-protected overlay encryption to currently unprotected critical OT links and must record the placement decision per protocol class and per segment in the CBOM: native, tunneled or terminated, the component that bears the processing load, and the classical leg that remains.

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. VPN concentrators are typically IT-managed equipment, making them the most accessible early-migration target.

Framework Impact: Phase 3 must score OT remote access VPNs Critical on Dimension 1 as internet-facing entries, which places them at Tier 1 under the ordered test, with the delivery state available. 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.

In IEC 61850 the station-bus MMS traffic runs over TCP/IP and is protected by TLS and X.509 certificates under IEC 62351-3 and -4. GOOSE and Sampled Values are Layer 2 Ethernet multicast publish/subscribe services on the process and station bus, not TCP/IP flows, so TLS does not apply to them.

Their timing budget is read per flow rather than assumed. IEC 61850 defines distinct transfer-time classes, and the roughly 3 to 4 millisecond figure quoted for substation protection belongs to the fastest of them, the class used for trip signaling. It does not belong to every GOOSE and Sampled Values application. Record the message type and the performance class with each flow, and test against that flow's budget.

IEC 62351-6:2020 secures the frames with HMAC or AES-GMAC, carried in a security extension in the reserved fields defined in IEC 61850-8-1. The 2020 edition moved off the digital signatures of earlier editions (RSASSA-PKCS1-v1_5, later RSASSA-PSS) for that reason.

The quantum-vulnerable asymmetric dependency in a substation is therefore in two places:

- The TLS-protected MMS and other station-bus flows.
- The key management layer under IEC 62351-9: the certificates and PKI that distribute the symmetric keys the MAC consumes.

An adversary who forges the certificates that authenticate key management controls the keys the MACs depend on. The substation's TNFL exposure is therefore scored on the key management layer and the MMS certificates, not on the GOOSE frame.

Grid protection relays, the devices that detect faults and trip circuit breakers within milliseconds, are among the most time-critical devices in any OT environment. The MAC on a GOOSE frame is symmetric, so moving the asymmetric key-management dependency to post-quantum algorithms need not change the frame at all. A grid operator benchmarks the PQC overhead on the key-management exchange and the MMS session. Any latency increase there is tested against protection coordination before the substation's key management is changed.

Where the vendor release that delivers post-quantum key management also changes the MAC algorithm, the tag size or the framing, the operator runs a timing and bandwidth test on that change, at the performance class of the affected flows. A symmetric MAC makes the frame indifferent to the algorithm change, not to a change in the frame itself.

Framework Impact: Phase 1 must inventory IEC 61850/62351 deployments and protection relay firmware, recording per substation which flows run under TLS (station-bus MMS, IEC 62351-3 and -4), which run under the IEC 62351-6 MAC (GOOSE and Sampled Values), and the IEC 62351-9 key management that distributes the MAC keys, with the certificates and trust anchors that layer depends on. Phase 3 scores the key

management layer and the MMS certificates on Dimension 2 and the MMS flows on Dimension 1. The MAC itself is symmetric and is not a Shor target.

Phase 6 must benchmark PQC overhead against protection relay timing requirements on the flows that carry it, the key-management exchange and the MMS session. Phase 7 must engage grid equipment vendors on the PQC revision of the IEC 62351 profiles and on the firmware path that delivers it to deployed relays.

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, and that transport layer is the Track A entry.

Where the link carries DNP3, Secure Authentication (SAv5, IEEE 1815-2012) is a separate mechanism at the application layer. It authenticates the master, the outstation and the named user per critical operation, by challenge and response over the critical ASDU with HMAC-SHA-256 or AES-GMAC. Session keys are distributed under a pre-shared Update Key by AES-256 Key Wrap. It runs with or without TLS on the transport.

That core is symmetric and is not a Shor target. Asymmetric cryptography enters SAv5 only through the optional remote Update Key change (RSAES-OAEP, with RSA or DSA signature options beside the symmetric AES-256 Key Wrap method). A deployment using that option records it as its one quantum-vulnerable DNP3 element.

The standards status is graded like every other date in this extension:

- IEEE 1815-2012 has been Inactive-Reserved since March 30, 2023.
- The successor work, now named DNP3 Security Layer (DNP3-SL) and formerly SAv6, remains unpublished, with the Authorization Management Protocol under project P1815, extended to December 2027.
- No IEEE 1815-2020 exists.

That status is a firmness signal about future revisions of the standard. What applies to equipment already in service is read from the operator's own contractual and regulatory references.

The DNP Users Group's 2026 update states the successor's position per component. The security-layer draft is complete. The Authorization Management Protocol's authority work is near completion, and its device work is still in development. A vendor date that names the successor is graded per component, not as one delivery.

Pipeline, water utility, and rail signaling SCADA all transmit commands with direct physical safety implications.

Framework Impact: Phase 1 must map SCADA WAN encryption endpoints and, for DNP3, record whether Secure Authentication is enabled and whether the asymmetric Update Key option is in use. 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: EXTENDED-VALIDITY 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. Whether the device's trust store can accept a new signature algorithm at all is the verifier-updatability factor of Dimension 2 (Phase 3), and it decides the path. A device whose verifier cannot be updated is re-keyed to a new algorithm only by replacement, or enclosed behind a gateway.

Framework Impact: Phase 2 (CBOM) must capture certificate validity periods, renewal mechanisms and verifier updatability. 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. A proprietary algorithm offered as a product's quantum-safe claim is checked against the Universal's one-afternoon test (Activity 7.3): public specification with test vectors, public cryptanalysis by parties other than its designers, a standards-body track, and a validated or CAVP-tested implementation. A stack that fails the first two tests is excluded from approved-mode use. The exclusion is a line in the tender template (Phase 7).

Framework Impact: Phase 2 must include vendor disclosure requests and CBOM generation through passive network observation. Phase 7 must issue this extension's tender template for all new OT procurement, agility requirements first.

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 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 railway and aviation safety standards. An organization operating across several CNI sectors plans against the most demanding of them. Three deadline archetypes cover every instrument the sector meets (Universal, Regulatory & Standards Alignment Map): plan-by, procure-by and migrate-by, each with an enforcement tier that Phase 3 Dimension 4 reads.

The plan-by and migrate-by archetypes reach EU operators through the NIS Cooperation Group's Coordinated Implementation Roadmap (June 2025): 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 (January 20, 2026) proposes to write PQC transition policy into NIS2 itself as a named component of national cybersecurity strategy. The obligation is on the Member State and is conditional on adoption, and entity-level transition-plan requirements would follow through transposition and supervisory practice. For EU critical infrastructure operators, "the most demanding regulatory timeline" in this challenge now has numbers attached: plan critical use cases to 2030.

The procure-by archetype has a national example in the sector. ANSSI's published position (FAQ on post-quantum cryptography, October 8, 2025; restated at France Quantum on June 16, 2026) is that security products entering ANSSI qualification from 2027 must include post-quantum cryptography, with the organizations it supervises to buy only quantum-safe solutions by 2030. Qualification is the condition of market access for security products used by French administrations and operators of vital importance.

The gate binds the operator's procurement whether or not its own sector regulator has set a date (enforcement tier 1). The tender template in this extension's Phase 7 adaptations is written to pass a gate of that kind. Federal mandates reach private operators as a signal and through directed contractor rules: Executive Order 14412 (June 22, 2026) sets dates for federal high-value assets and high-impact systems (December 31, 2030 for key establishment; December 31, 2031 for signatures) and directs FAR rulemaking for covered contractors, so an operator that sells into or operates for a federal customer inherits the mandate's shape through its contracts while holding no date of its own.

The jurisdiction roster and its dates are in the Universal's Regulatory Timeline Context and, kept current, on the Global PQC Migration Clock page (https://postquantum.com/pqc-migration-timelines/global-pqc-migration-clock/).

Framework Impact: Phase 0 must map all applicable CNI regulations and their quantum/cryptographic requirements and tag each with its enforcement tier. Phase 4 must align with the most demanding regulatory timeline. Phase 7 must issue the tender template. New equipment must pass the procurement gates the operator is subject to.

CHALLENGE 11: PROCESS HISTORIANS AND LONG-HORIZON OPERATIONAL DATA

OT migration teams typically treat data at rest as an IT problem, but the OT data estate has its own exposure profile. 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 growing: 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 follows 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) governs each 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 V3.0

Universal Framework v3.0 (September 2026) is a major version. Readiness against dated obligations is the mandate; crypto-agility is the method. The PQC migration is the first exercise of a standing capability. For OT-operating critical infrastructure the version changes the method, the records and the vendor governance, and corrects three published positions.

- **Method.** The charter states both outcomes (Phase 0). The program is organized into ten workstreams, with Discovery separated from the permanent Cryptographic Record and Crypto-Agility funded from Year 1 (Activity 0.3). Every migration gate and wave exit applies the agility criterion, and a system whose algorithm cannot be changed by configuration and rehearsed with rollback is recorded as migrated with agility debt (Activities 4.6 and 5.4).

Every wave includes an algorithm-change rehearsal (Activity 5.2). Closure requires a rehearsed second algorithm change per track inside the agility window (the 48-hour assessment plus the organization's change window, ten business days by default) and zero unaccepted agility debt (Migration Verification & Program Closure). Phase 3 produces an agility-debt register.

- **Records and evidence.** Every discovery finding is assigned an evidence grade E1 to E5; coverage is measured against a denominator enumerated before discovery ran. The accepted-gaps register is signed at gate G1 → G2 (Activity 1.2). The CBOM minimum record is the Universal's own (Activity 2.1), with the Applied Quantum CBOM Profile v1.0-RC or later cited as informative carriage and never required. The Cryptographic Concentration Framework is cross-referenced where the question is how many distinct implementations execute beneath the vendors (Activity 3.1), and no concentration figure is computed in this extension.
- **Vendor governance.** Every roadmap date is graded for firmness (committed, forecast, announced, unknown). The questionnaire opens with the two agility

questions and the firmness question; four certificate-authority questions and the non-standardized-algorithm rule with its one-afternoon test apply (Activities 7.2, 7.3 and 7.5). In OT the whole set enters the tender template in this extension's Phase 7 adaptations.

- **Corrections made in the open.** HNDL is stated as inference from demonstrated capability, never as observed harvesting. The June 2026 statement that no validated module offered approved PQC was wrong when published: CMVP certificate #5247, a software module validated on April 27, 2026, lists ML-KEM key generation and encapsulation-decapsulation at ML-KEM-768 and ML-KEM-1024 among its approved algorithms, and certificate #5497, validated on August 19, 2026, covers ML-KEM, ML-DSA, SLH-DSA and LMS in Level 3 hardware. Validation is decided per product, per operation and per certificate (Deployment Environment Classification).
- **Corrections made in the open: where the secured protocols run their cryptography.** The June 2026 edition made two statements about where the secured industrial protocols carry their public-key cryptography. Both were wrong when published.

On substation automation it said: "IEC 61850 relies on TLS and X.509 certificates for GOOSE message authentication and MMS communications."

GOOSE and Sampled Values are Layer 2 Ethernet multicast services that TLS does not reach. IEC 62351-6:2020 protects those frames with HMAC or AES-GMAC. The substation's asymmetric exposure is in the key management layer of IEC 62351-9 and in the station-bus MMS flows protected under IEC 62351-3 and -4.

On the secured protocols generally it said: "More modern protocols (OPC UA, IEC 62351, Secure DNP3) do incorporate TLS and X.509 certificates, all quantum-vulnerable."

OPC UA over the binary `opc.tcp` mapping uses its own SecureChannel and not TLS. TLS applies to the `opc.https` and `opc.wss` mappings (OPC UA Part 6). DNP3 Secure Authentication is application-layer authentication, distinct from the transport security beneath it, and SAv5 is predominantly symmetric. Its one asymmetric element is the optional remote Update Key change (IEEE 1815 and the DNP Users Group's 2026 update).

A reader who scoped from the published text should re-check two entries. First, an OPC UA deployment recorded as a TLS migration is a SecurityPolicy change on the server and its clients, scored from the policy and the MessageSecurityMode recorded per deployment. Second, a DNP3 link scored as an asymmetric dependency on the strength of Secure Authentication has that dependency in the transport key exchange, and in the remote Update Key change where the option is in use.

Challenges 3, 5 and 6 carry the corrected descriptions, and the scoring that follows from them puts the substation's TNFL exposure on the key management layer rather than on the GOOSE frame.

Standards currency runs to September 2026: RFC 9954 and RFC 10024 for hybrid TLS, RFC 9370 for hybrid IKEv2, RFC 10042 for hybrid SSH, and the section 8 conditions of SP 800-208 on the deploy-now firmware-signing action.

The subsections below read each element for OT estates. The last three read elements the June 2026 edition did not cover (the agility criterion and rehearsal; evidence grades and the coverage denominator; vendor dates and questions). The remaining Universal positions apply as written, with three notes. The data-at-rest decision framework (Activity 5.6) covers the OT data estate through Challenge 11 (historians and engineering data).

The counterparty coordination pattern (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. The Accelerated Execution Profile (Activity 4.7) meets a hard OT boundary: compression is bounded by maintenance windows and safety approvals.

The OT version of the profile pre-approves accelerated compensating-control deployment (segmentation, gateway insertion, key-lifetime reduction) instead of compressed device migration that the safety case will not permit. Its companion for slippage, the Re-Baseline Protocol (Activity 4.8), governs every committed date that depends on a vendor firmware release or a safety approval the operator does not control.

Integrity and Signatures Lead the OT Migration

The Universal Framework's two tracks map onto OT with the priorities inverted. Track B (Integrity / Signatures / PKI) leads. TNFL is the primary OT threat, and the assets Track B protects – firmware signing and secure boot, control-command authenticity, device identity certificates, and configuration signing – underpin the one property every OT safety case requires: 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. The Universal's guidance is to run the two tracks in parallel (Activity 3.3), weighting Track B above the default for critical infrastructure (Two-Track Migration Model). This extension places Track B's first move, SP 800-208 firmware signing, at the front of the program alongside the Track A VPN work. Phase 3 below swaps the Universal's default weights accordingly.

Validation Decided Per Product, Then the Safety Case

Under the Universal Framework's Deployment Environment Classification, validation is determined per product, per operation and per certificate. FIPS mode is a configuration. Validation is a certificate tied to a module version and a tested environment. The classification keys on the certificate.

The June 2026 statement that no validated module offered approved PQC was wrong when published. As of September 2026 the CMVP validated-modules list includes post-quantum operations as approved services in software and in hardware, and the two certificates this framework cites are not interchangeable evidence.

Property	Certificate #5247	Certificate #5497
Module	Go Cryptographic Module (versions v1.0.0 and v1.0.1, Geomys LLC)	QASM Cryptographic Module (Crypto4A Technologies, hardware version QASM 1.1, firmware 5.0.1.158)
Type and level	FIPS 140-3 Level 1 software module	FIPS 140-3 Level 3 multi-chip standalone hardware module
Dates	Validated April 27, 2026; updated July 7, 2026	Initially validated August 19, 2026; updated August 21, 2026; sunset date August 18, 2031
ML-KEM	KeyGen and EncapDecap, which covers encapsulation and decapsulation, at ML-KEM-768 and ML-KEM-1024 only, not ML-KEM-512	KeyGen and EncapDecap at ML-KEM-512, -768 and -1024
ML-DSA	None	KeyGen, SigGen and SigVer at ML-DSA-44, -65 and -87
Other approved algorithms	Not applicable	SLH-DSA across all twelve parameter sets, and LMS

Two qualifications from #5497's Security Policy apply to every citation of it. The first is that §2.7 states that the module does not establish SSPs using an approved KEM, and instead exposes ML-KEM functionality for an external application to use as part of an approved KEM. The second is that HSS key generation, signing and verification are vendor-affirmed, not CAVP-tested.

Every ML-DSA statement in this extension is evidenced by #5497 alone. A module that lists PQC only among its non-approved services does not count.

The planning rule is per product, not per calendar. For each deployment, record:

- the governing requirement
- the module and version
- the certificate number and status
- the approved services the certificate lists
- the required security level
- the tested operating environment

Then confirm that the intended cryptographic operation is covered, and set the production date per system from the certificate that covers its operation.

FIPS 140-2 certificates moved to the Historical list on September 21, 2026, the date stated in the maintained prose of NIST's FIPS 140-3 Transition Effort page (its transition-schedule table, stamped 2021, prints September 22, 2026). CMVP states a permission for those modules, not a prohibition:

- It supports their purchase and use for existing systems.
- It notes that the selection of FIPS 140-3 modules may be limited for several years.
- It recommends that purchasers consider every module on the validated-modules search page, regardless of whether it was validated against FIPS 140-2 or FIPS 140-3.

The exclusion of a Historical module from procurement for new systems follows from that scoping to existing systems and from agency and contractual policy, not from a CMVP prohibition. Whether an existing deployment on a Historical certificate may continue is decided under the applicable agency or contractual risk policy, and the two questions are assessed separately.

Most OT estates classify as FIPS-aware at best. Safety-certified systems form a class of their own on top of that. A validated module still waits for the safety authority before it can be deployed inside a certified boundary (IEC 61508 SIL levels, IEC 61511, sector safety cases). The safety authority's clock is independent of CMVP's.

Whether a cryptographic change reopens the safety case is a decision per change, not a blanket rule. Take it with the safety authority, against the change's effect on the safety function, and record it with the change:

- A gateway inserted in front of the zone, a key-lifetime reduction or a certificate renewal outside the certified boundary usually does not reopen the case.
- A firmware change to a controller inside the boundary usually does (Challenge 2).

Sequence accordingly. Pilot on non-safety systems and on gateways in front of safety systems now. Treat safety-system cryptographic changes as the long pole, whose

vendor and certification lead times Phase 4 records explicitly. The documented-risk-acceptance route exists in OT, and it never overrides a safety case.

Merkle Tree Certificates Affect Only the Browser-Facing OT Edge

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 vendors' fork on the browser vendors' schedule (the Chrome quantum-resistant root store is planned for Q3 2027; Universal Phase 6, PKI Architecture Evolution). 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 Framework's default (Activity 5.2) is composite or dual signatures, with solo deployment recorded as a risk decision. The hedge applies only where the verifier requires both signatures, and its acceptance policy is recorded with the format. In OT the default applies where size and compute allow: firmware images can usually accommodate dual signatures, and gateway TLS can run hybrid. It fails 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.

ECC-Based Modern Equipment Is the Early Quantum Target

The Universal position that quantum attack cost scales with key size, not with classical strength (Activity 3.1, where the 2026 resource estimates moved the 256-bit-curve figures first and left the RSA figures unchanged), 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 use 256-bit curves while legacy estates use RSA-2048 or 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.

Machine Identity Across the Industrial Network

The Universal's identity and authentication scope in Track B translates in OT to machine identity: device certificates in IEC 61850 substations and OPC UA deployments (the ApplicationInstance Certificates and the trust lists that verify them. The SecureChannel key establishment they authenticate is Track A, scored per SecurityPolicy in Phase 3), 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. Whether a device's trust store can take a new signature algorithm at all is recorded per device as the verifier-updatability factor (Phase 3). Inventory the machine-identity estate explicitly. It is where TNFL meets the network.

SP 800-208 Firmware Signing for Immediate OT Deployment

Challenge 1 of this extension is firmware signing. The Universal makes SP 800-208 stateful hash-based signatures (LMS/XMSS) the deploy-now component of Track B (Two-Track Migration Model), and the two meet. The standards are final, and hash-based signatures involve none of the lattice novelty that makes conservative OT engineering hesitate.

CNSA 2.0 recommends LMS and XMSS for signing software and firmware. This is the signature migration NSA prefers to begin now, because validated implementations of those schemes are commercially available. ML-DSA-87 is approved under CNSA 2.0 for all signature use cases, including firmware and software signing. NSA names it as possibly the more appropriate choice in two situations: where the signing volume exceeds what one LMS or XMSS key can reasonably produce, and in distributed signing environments (NSA CNSA 2.0 FAQ, Version 2.1, December 2024).

What the validated population supports:

- The validated LMS implementation this framework can evidence is CMVP certificate #5497, whose CAVP entry covers one parameter set, LMS_SHA256_M24_H5 with LMOTS_SHA256_N24_W2, while the module's own security-function table lists more.
- XMSS support is materially rarer than LMS, and the CMVP search form offers no filter for either scheme, so the validated population cannot be enumerated and no broader claim is made in either direction.
- The deploying organization verifies parameter-set coverage on the specific certificate, rather than inferring it from the algorithm's presence.

SP 800-208 imposes its own conditions in section 8:

- Key generation and signature generation happen inside a hardware module with at least Level 3 physical security.
- The private key is never exported, in any form.
- Signing state is managed inside the module, with backup, replication and failover designs that cannot reuse a state.

A signing service that does not meet section 8 is not a conforming deployment, and the verifiers in the field must accept the parameter set chosen.

State safety is an acceptance item evidenced inside the conforming implementation, not an inference from "HSM-backed" or "controlled ceremony":

- the supported parameter sets
- exhaustion monitoring
- atomic state handling
- tested backup, replication, crash-recovery and concurrent-signing behavior

The operator's lever is procurement, because firmware signing migrates at the vendor. The tender template in this extension's Phase 7 adaptations requires post-quantum firmware-signature verification in new equipment now, under an algorithm and parameter set the tender names, with LMS or XMSS as the default. The template also asks the vendor's signing service to state how it meets section 8, and which parameter sets its certificate covers.

The signing module's certificate reference, the parameter sets its certificate covers, and its entropy validation go in the Phase 6 register.

Securing the OT CBOM as Physical-Consequence Data

Universal Activity 2.5 treats the CBOM as a high-value intelligence target. In OT, 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 hold the SOC integration inside the same boundary.

Mark the document AMBER or RED at generation and never leave it at the default (Activity 2.5). When a safety authority, a regulator or an insurer asks for the CBOM, the Universal's rule applies. Send a signed commitment to the snapshot, a coverage statement with its denominator and method, and the predicate the requester needs, in place of the document.

Verification, Decommissioning, and the Decades-Long Tail

The Universal's Migration Verification & Program Closure section defines the evidence standard for declaring a system migrated, and the closure criteria. The criteria are a

verification disposition for every Tier-1 and Tier-2 service in one of four states, the closure proof, and the agility-debt register at zero unaccepted debt. The four states are: migrated; migrated with agility debt and a funded closure date; enclosed or compensated under an accepted exception; and retired.

Against OT's defining constraint, a tail of non-migratable devices measured in decades, those four states are the OT closure model.

- **Migrated systems.** The standard evidence applies. Decommissioning classical material includes vendor-escrowed keys and recovery material alongside operator-held copies.
- **The vendor-locked population**, which changes its algorithm only with a vendor release or a hardware replacement. "Migrated with agility debt" is the expected recorded state. Each entry records the reason (non-updatable verifier, vendor-locked configuration, hardcoded algorithm) and a funded treatment with a date.
- **The population that will never support post-quantum cryptography natively.** The compensating-control registry is where the accepted exceptions reside. Each entry states the control (the Encapsulate strategy, Phase 5), the residual-risk acceptance signed by the SteerCo, the agility-debt state and a re-evaluation date. "Closed" on such an entry means accounted for under a documented control regime.

The closure proof is run where the operator controls the change: for Track A on the gateway layer, and for Track B on the firmware-signing service or the OT issuing CA. Each runs inside the agility window and is minuted with the segment timings. Both evidence streams feed the safety case and the regulator.

The Agility Criterion and Rehearsal in OT

The Universal's agility criterion (Activity 4.6) asks four things of a migrated system: the negotiated outcome observed, classical-only refused and tested where policy requires it, the algorithm changeable by configuration, and a rehearsal in staging with the rollback exercised. In OT the third and fourth conditions are met at the layer the operator changes without reopening a certified boundary (the gateway or aggregation layer in front of the zone, the VPN concentrator, the firmware-signing service and the OT PKI) and are rarely met on the device population behind it.

This extension states the sector's agility objective in those terms: crypto-agility in OT means changing algorithms on a date the operator can plan, and the gateway layer is where that property is achievable. Every OT wave includes an algorithm-change rehearsal on that layer (a parameter-set change on a gateway or concentrator, a certificate-signature-algorithm change on the OT issuer, a parameter-set change on the firmware-signing service against a laboratory verifier), timed across assessment, decision, change and verification, with the rollback exercised in a staging replica of the zone or inside a maintenance window and never against a live safety function.

A rehearsal that cannot be scheduled because the change requires a vendor firmware release, a hardware replacement or a safety re-certification has found agility debt before production did. The entry goes to the Phase 3 register with its treatment.

Evidence Grades and the Coverage Denominator in OT

Every discovery finding is assigned an evidence grade in the Universal's five tiers (Activity 1.2): E1, runtime observed; E2, binary confirmed; E3, inventory declared; E4, vendor attested; E5, inferred. In OT the distribution is inverted relative to IT. Passive monitoring at zone boundaries produces E1 for the traffic it sees; active scanning is usually prohibited; binary analysis of firmware (E2) is feasible for a minority of device types. Most of what is known about embedded cryptography is E4 (a vendor's answer) or E5 (an inference from a certification record or a product manual).

The grade is recorded with the finding in the CBOM and in Phase 3, where an E5 entry scored Critical is a finding to verify before it is a finding to fund. Coverage is measured against a denominator enumerated before discovery runs, built from the asset register, the physical walkdown, the procurement records and the vendor firmware catalog, never from what the monitoring tools found. Device classes the monitoring method cannot observe (serial-attached equipment, devices behind protocol converters, the facilities estate) are named as unobserved, with coverage unknown rather than zero.

The accepted-gaps register, signed at gate G1 → G2 by the Discovery lead, the CISO and the SteerCo, records the scope the denominator contains and discovery did not reach, with the reason and a planned closure date. In OT that register is long by design. It is a governance artifact.

Vendor Dates and Questions in OT

Every vendor date in this extension's tables and vendor scorecards is graded under the Universal's four firmness grades (Activity 7.5): committed (contractual, with remedies), forecast (a planning date stated in writing), announced (a public roadmap statement) or unknown. Phase 3 Dimension 3 scores the firmness grade, independent of the calendar date. The questionnaire opens with the two agility questions and the firmness question (Activity 7.2); in OT the second agility question, whether the product's verifiers and trust stores can be updated in the field, decides the migration path for the installed base.

The four certificate-authority questions apply to every vendor that issues device identity certificates from its own CA, which most control-system vendors do, and to the operator's OT PKI provider. The non-standardized-algorithm rule and its one-afternoon test (Activity 7.3) apply to proprietary cryptographic stacks (Challenge 8). The tender template in this extension's Phase 7 adaptations is where the questions become contract terms.

PHASE-BY-PHASE FRAMEWORK ADAPTATIONS FOR CNI AND OT

Implement the adaptations below 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.
- **The dual-outcome charter:** State both outcomes in the charter in the operator's terms (Universal Activity 0.4): readiness against the operator's dated obligations (the regulator's plan-by and migrate-by dates, the procurement gates in Challenge 10, the insurer's questionnaire, the safety authority's expectations) as the mandate, and the standing capability to change cryptography at the gateway layer, in the OT PKI and in the firmware-signing service on a planned date as the end state. The compensating-control registry and its accepted exceptions are part of the readiness evidence.

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 alongside the CISO.

Two owners are named in the charter beside the SteerCo (Universal Activity 0.3): the Crypto-Agility workstream owner, which in OT belongs to the engineering function that owns the gateway layer and the OT PKI instead of IT security alone, and the Cryptographic Record owner, who keeps the OT CBOM after the discovery project ends. The three lines are stated by function: the program under the CISO and the Chief Engineer is first line and delivers; process safety and the risk function are second line and challenge the scoring model, the per-change recertification decisions and closure; internal audit is third line. Engage OT operations and site engineering before any discovery activity needs their cooperation. The first contact is the cryptographic ownership register conversation (Phase 1).

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. For every OPC UA deployment record the transport mapping (`opc.tcp`, `opc.https` or `opc.wss`), the SecurityPolicy and the MessageSecurityMode in use. The RSA and the ECC policies differ on forward secrecy, and Phase 3 scores the deployment from this field. For an RSA-policy deployment record the endpoint key pairings as well, with the certificate renewals and key rotations on each side and their dates. Those dates bound the recorded history a later key recovery would expose.
- **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, renewal mechanisms, and whether the relying device's trust store can be updated in the field.

Every finding on these tracks is tagged with its evidence grade (the alignment section's evidence subsection): E1 for a handshake observed at a zone boundary, E2 for a

firmware image analyzed, E3 for a register or configuration export, E4 for a vendor's firmware catalog entry or questionnaire answer, and E5 for a capability inferred from a product manual or a certification record. Each track states its denominator before discovery runs, from the asset register, the walkdown, the procurement records and the vendor firmware catalog. What the denominator contains and discovery did not reach goes to the accepted-gaps register signed at G1 → G2.

The Cryptographic Ownership Register

Before OT cryptography can be inventoried, prioritized or migrated it has to be claimed. The register maps every embedded credential, certificate store, signing dependency and key-holding component found on the tracks above to a named owner, across the engineering, operations, facilities and vendor boundaries, with a RACI for each entry: who can change the element, by what route (vendor firmware, operator configuration, integrator-held keys, escrowed recovery material), and who approves the change.

Without a named owner, a finding becomes a report nobody actions. The register is opened in Phase 0 as the first contact with OT operations and site engineering, before any discovery activity needs their cooperation. It is populated as discovery runs. An entry whose owner cannot be named after the walkdown is assigned an interim accountable owner, by default the Cryptographic Record owner or the site engineering lead for the zone.

The missing ownership is escalated as a remediation issue under the charter's access-governance path (Universal Activity 1.4). The entry receives its delivery state and its migration decision in Phase 3 like every other, and the open ownership item stays on it until a permanent owner is named. The register is a permanent artifact that transfers to the Cryptographic Record owner at closure. The CBOM's owner field (Activity 2.1) is populated from it.

The Facilities Estate as Its Own Discovery Scope

The facilities estate (access control, building management, elevators, fire and life-safety panels, CCTV and the controllers behind them) is a discovery scope of its own within Phase 1 (the sector characteristic above). Its owners are facilities management and the building owner, engaged through the ownership register before the walkthrough. Its data sources are the building management system's own device list, the facilities service contracts and the physical walkthrough (Universal Activity 1.4). The CMDB does not contain it.

Its denominator is enumerated from those sources. Its migration pattern is the Encapsulate strategy (Phase 5): almost none of the population will support post-quantum cryptography natively within its service life. Score it in Phase 3 like any other OT zone: the access-control and life-safety controllers have a physical-consequence factor, and their signing and identity certificates are Track B.

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. What discovery cannot reach is named in the accepted-gaps register. A device class the method cannot observe is recorded as unobserved.

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. The record is the Universal's own minimum record (Activity 2.1): an entry built from a vendor answer is graded E4.

A vendor-opaque entry is graded E5 with the disclosure request open. Organizations that structure the CBOM under the Applied Quantum CBOM Profile, v1.0-RC or later, record the same fields as Profile properties. The Profile is informative carriage and never required. Two fields are recorded on every signing and device-identity entry because Phase 3 reads them: the firmware-signing mechanism with its verification-key algorithm and whether the verifier can be updated in the field.

On every OPC UA entry the protocol context (Activity 2.1) carries the transport mapping and the SecurityPolicy recorded in Phase 1, and the key establishment and the ApplicationInstance Certificate on one interface are two rows, as the Universal's row unit requires.

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. Purdue levels are written as levels to avoid confusion with the Universal's discovery Layers 1 to 5 or CBOM Layers 1 to 4.

Phase 3 – Risk Scoring & Prioritization

Adapted Risk Scoring Model

The Universal's four dimensions (Activity 3.1) stand: Dimension 1, data sensitivity and exposure (HNDL); Dimension 2, trust infrastructure criticality (TNFL); Dimension 3, migration feasibility; Dimension 4, regulatory and compliance pressure. The OT adaptation adds no dimension. It adds two factors, reads one of the Universal's factors for the OT estate, re-weights one dimension and uses the Universal's arithmetic (Activity 3.2).

Under that arithmetic, Low = 1 to Critical = 4 and a dimension scores the highest of its factors. An inapplicable dimension is excluded with the weights renormalized. An unknown value is left unscored, listed and resolved before the entry is tiered. The tier is assigned by the Universal's ordered test (Activity 3.2), read from the top on Dimensions 1, 2 and 4: the first condition that matches assigns the tier, Dimension 3 and the delivery state place no tier, and the composite score orders the entries inside a tier and never assigns one.

In OT the second Tier 1 condition, Dimension 2 Critical on any factor, reaches a large population: the physical-consequence factor below scores every safety function Critical. The verifier-updatability factor scores every burned-in trust anchor Critical.

- **Physical consequence (a factor inside Dimension 2):** Could a forged signature or a forged command on this element cause physical harm? Loss of life or an environmental release = Critical; equipment damage or a service outage affecting the public = High; a process upset the operator can recover = Medium; none = Low. SIS controllers, protection relays and emergency shutdown systems score Critical.
- **Verifier updatability (the Universal's Dimension 2 factor, read for OT):** Verifiers that cannot be updated (burned-in trust anchors, unmanaged device fleets) = Critical; updatable by a firmware campaign inside a maintenance window = Medium; centrally managed trust stores = Low. Non-updatable verifiers are the primary source of agility debt in the OT estate.
- **Change path (a factor inside Dimension 3):** The device's cryptography changes by configuration in the field = Easy; by a firmware campaign inside a maintenance window = Medium; only by hardware replacement or with safety re-certification = Hard.
- **Weighting:** OT programs weight Dimension 2 above Dimension 1 (the Universal's Two-Track Migration Model), so the OT default swaps the Universal's weights to TNFL 0.35 and HNDL 0.25. The weights order entries inside a tier and the ordered test assigns the tier. The SteerCo ratifies the weights and the appeals rule before the first scoring run (Activity 0.3).

Algorithm-specific weighting: Apply the Universal's vulnerability weighting (Activity 3.1) in OT scoring: quantum attack cost scales with key size, not classical strength, so

modern ECC-based device identity and secure channels are at least as urgent as legacy RSA at equal criticality. See the alignment section's Algorithm Weighting subsection.

OPC UA and forward secrecy. The OPC UA population is scored per SecurityPolicy from the Phase 1 field. Each deployment is two rows:

- the key establishment on the SecureChannel (Track A, Dimension 1)
- the ApplicationInstance Certificate with the trust list that verifies it (Track B, Dimension 2)

The RSA SecurityPolicies (Basic128Rsa15 and Basic256, both deprecated; Basic256Sha256; Aes128_Sha256_RsaOaep; Aes256_Sha256_RsaPss) authenticate with RSA signatures over X.509 ApplicationInstance Certificates, and establish the session keys by RSA key transport. They have no forward secrecy. The session keys are derived from a client nonce and a server nonce that both travel under the endpoints' long-term RSA keys, and no per-session secret is discarded.

A recorded session becomes decryptable once an attacker recovers the key material that reconstructs both of its nonces. Each nonce is encrypted to its own receiver (OPC UA Part 6, sections 6.7.4 and 6.7.6), so one endpoint's private key does not by itself open every recorded session. What a recovery exposes is the history of the endpoint key pairings it covers, bounded by the renewals and rotations Phase 1 records. That is still the HNDL case without forward secrecy: the recorded traffic is opened by a key recovery rather than by an attack on each session.

The ECC SecurityPolicies added at version 1.05 (ECC_nistP256, ECC_nistP384, ECC_brainpoolP256r1, ECC_brainpoolP384r1) authenticate with ECDSA and establish keys by ephemeral ECDH, which has forward secrecy against a passive recorder. Each recorded session is exposed to a future quantum attack on its own ephemeral exchange, one session per attack.

MessageSecurityMode None remains a common shipped default and provides no message security. A deployment running it belongs to the first class of Challenge 3.

Phase 3 scores the RSA-policy population on Dimension 1 the way it scores any channel without forward secrecy. The confidentiality horizon is read from the data in those sessions (Activity 1.1). The accessibility is read from the network position a collector can reach, with a flow that crosses a carrier or a cloud boundary scoring partner-facing at least. The HNDL-exposure determination records the assessed exposure: which recorded sessions the endpoint key pairings, renewals and rotations place at risk if that key material is recovered.

The tier falls out of the ordered test, never from a placement by hand. Inside the tier, at equal composite score, the RSA-policy deployment is sequenced ahead of the ECC-policy deployment on that assessed exposure. Recovering the key material of an RSA-

policy channel yields the sessions its key pairings cover, while an attack on an ECC-policy session yields that session alone.

The migration path is a SecurityPolicy change on the server and its clients, not a TLS change (Pilot 3).

CNI/OT Priority Tiers

Priority	System Category	Rationale	Typical Delivery State
Tier 1	IT/OT boundary: VPN concentrators, jump servers, DMZ firewalls, remote access gateways; SCADA WAN and cloud SCADA connections that cross public infrastructure, or that carry data with a confidentiality horizon over 15 years across a carrier or cloud boundary; historian replication to data lakes and cloud analytics; firmware signing trust anchors and secure boot chains; SIS controllers, protection relays and emergency shutdown systems; device identity certificates, OT PKI roots and the substation key management layer where the verifier cannot be updated in the field or 15 years or more of verification remain	Placed by the ordered test of Activity 3.2: Dimension 1 Critical with accessibility High or Critical (an internet-facing flow, or a carrier- or cloud-crossing flow carrying data with a horizon over 15 years, the norm for telemetry that reveals a long-lived asset's topology, Challenge 11); or Dimension 2 Critical on any factor (a root or fleet-wide trust anchor, 15 years or more of verification, verifiers that cannot be updated, physical consequence Critical); or Dimension 4 Critical (a mandatory deadline within 2 years).	Available for the boundary equipment. Dependent or blocked where the algorithm changes with a vendor release, shown against the release date with its firmness grade and running under the bridging pattern named on the entry (below)

Priority	System Category	Rationale	Typical Delivery State
Tier 2	SCADA WAN links and OPC UA key establishment below the Tier 1 accessibility line or with a horizon of 15 years or under; historian and enterprise integration inside the operator's own network; OPC UA ApplicationInstance Certificates and DCS/PLC device identity certificates whose trust stores update by campaign and whose lifetime is 5 to under 15 years; controllers whose forged command causes equipment damage or a public service outage; legacy field devices and serial endpoints on unauthenticated links inside connected zones, scored on the data the link carries	Dimension 1 Critical or High, unless the entry is air-gapped; or Dimension 2 High (a shared key or intermediate, 5 to under 15 years of verification, verifiers updatable by campaign, physical consequence High); or Dimension 4 High (a mandatory deadline within 5 years, or a contract that requires PQC). The OPC UA RSA-policy population is scored per SecurityPolicy on Dimension 1 and sequenced first inside its tier (above).	Dependent on a vendor release with a firmness grade; blocked where the device cannot change and enclosed under the Encapsulate strategy, the entry keeping this tier
Tier 3	Entries whose highest applicable dimension is Medium: internal engineering-workstation and HMI sessions carrying data with a horizon of over 5 to 10 years, configuration and recipe signing	Any applicable risk dimension (1, 2 or 4) Medium or above, and none High or Critical. Plan now; execute in the roadmap's later waves.	Available, dependent or blocked as the record states; the delivery state moves the roadmap date and never the tier

Priority	System Category	Rationale	Typical Delivery State
	verified by centrally managed trust stores within one application, controllers whose forged command causes a recoverable process upset, entries under a general regulatory expectation only		
Tier 4	Entries whose every applicable risk dimension is Low: an air-gapped device carrying data with a horizon of 5 years or under, with no signature role and no regulatory expectation attached to it. Few CNI entries meet the condition	Every applicable risk dimension Low. Monitor; compensating controls; migrate when feasible. A blocked migration does not place an entry here: legacy field devices, serial endpoints and devices in hazardous environments are tiered on their risk above, take the delivery state blocked, and are treated by the Encapsulate strategy	Blocked entries are shown in the tier the ordered test gives them, not in this one

Delivery state and the agility-debt register. A blocked entry keeps the tier the ordered test gives it and is never demoted for being blocked (Universal Activity 3.2). The composite score orders entries inside the tier and never assigns one. The entry appears on the roadmap against its unblocking date, which in OT is a vendor firmware release with a firmness grade or a maintenance window, and a blocked Tier-1 entry names its bridging pattern on the record: the Encapsulate strategy's gateway or overlay for a Track A entry, the bounded out-of-band validation control for a firmware-signing entry, or Activity 7.4's documented residual-risk acceptance with a re-evaluation date.

The OT estate produces the agility-debt register's largest entries: every Tier-1 and Tier-2 entry scored Hard on the change path or Critical on verifier updatability is listed with the reason. The non-updatable-verifier population is the register's burn-down denominator in the KPI supplement. The entries are derived from the scores already recorded and add no dimension (Activity 3.1).

Phase 4 – Roadmap & Governance

Maintenance Window Alignment

OT migration roadmaps must be aligned with planned maintenance windows. A cryptographic change to a safety-critical device is deployed under a safety-impact assessment, the approvals the governing process requires, the process owner's acceptance and a validated change method. For most such devices that means a planned maintenance window, and for a redundant system it can mean an authorized rolling change under the same conditions. Map each activity to the window or the authorized change slot it will use and build the roadmap around them.

Gates, Recorded States and Re-Baselining

Every gate record from G5 → G6 onward, and every wave-exit record, shows two results as separate fields (Universal Activities 4.6 and 5.4): the protection result (which boundaries and functions are verified, which remain exposed) and the agility result (which change was rehearsed, through which mechanism, in what elapsed time). A device population that passes on protection behind a gateway and cannot change its own algorithm exits the wave as migrated with agility debt, with the entry and its closure date in the Phase 3 register, or as enclosed under an accepted exception; neither result stands in for the other.

Blocked Tier-1 and Tier-2 entries keep their tier and appear on the roadmap against their unblocking dates, which in OT are vendor firmware releases with a firmness grade and maintenance windows. The Re-Baseline Protocol (Activity 4.8) governs every committed date that depends on a party the operator does not control: a vendor release slipping past the bridging capacity recorded in Activity 7.4, a safety authority's recertification decision, or a maintenance window lost to an operational event opens a re-baseline review at the next SteerCo, minuted to the evidence dossier. A slipped OT date that is not re-baselined reads, to the regulator, as a program that lost its plan.

Recommended Year-1 Plan

- **Q1:** Secure joint CISO/Chief Engineer sponsorship. Name the Crypto-Agility workstream owner and the Cryptographic Record owner. Open the cryptographic ownership register with OT operations and site engineering. Begin Tier-1 inventory.

Issue PQC readiness RFIs to top-5 OT vendors, agility questions first. Begin regulatory pre-engagement.

- **Q2:** Complete IT/OT boundary inventory with evidence grades and the denominator stated. Begin hybrid PQC VPN pilot on non-production link. Rehearse an algorithm change on the pilot concentrator, timed and rolled back. Map maintenance windows for next 24 months. Issue the tender template with every new OT procurement from this quarter.
- **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:** Change the SecurityPolicy on an OPC UA server and its clients in a staging environment. Over `opc.tcp` the protection is OPC UA's own SecureChannel, not TLS. The migration path is a SecurityPolicy change: record the policy in use, move a deployment off an RSA policy (RSA key transport, no forward secrecy) and test the ECC policies (ephemeral ECDH) as the interim step, with a post-quantum SecurityPolicy treated as a delivery from the specification and the stack vendor, dated and graded for firmness (Phase 7).

Verify client compatibility and throughput. Sign alone authenticates messages and leaves application payloads readable. Record the MessageSecurityMode beside the SecurityPolicy and, where payload confidentiality is required, require SignAndEncrypt or a separately verified protective transport or overlay. Test that the server refuses MessageSecurityMode None and any mode below the one the selected policy requires.

- **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.

Rehearsal per wave and the wave-exit criterion. Every wave, from the boundary VPN outward, includes an algorithm-change rehearsal on at least one system in the wave, timed across assessment, decision, change and verification with the rollback exercised (Universal Activity 5.2). In OT the rehearsal target is the gateway, concentrator, issuer

or signing service the wave touches, and the rehearsal runs in a staging replica of the zone or inside a maintenance window, never against a live safety function.

Each wave exit applies the agility criterion (Activity 4.6): negotiated outcome observed at the gateway, classical-only refused and tested where policy requires it, algorithm changeable by configuration, change rehearsed with rollback. A device population behind a gateway that meets the first two conditions at the gateway and cannot meet the last two itself exits as migrated by enclosure with its agility-debt state recorded. The wave-exit record shows the protection result and the agility result separately.

Execution Failure Modes in OT

- **The reconnect storm:** A gateway or concentrator that is migrated and restarted forces every device behind it to re-establish its session at once. The devices behind a terminating gateway do not process the gateway's post-quantum handshake; what they see is a restart, and they reconnect on their own retry schedules while the gateway completes the larger post-quantum handshakes on its outward leg. Sessions time out, devices retry, and the SCADA master sees a site drop.

Migrate gateways in a maintenance window, stage the reconnection by conduit, and test the storm in the laboratory with the real device count before production. A change to the master's poll rate is a process-performance change, made only with a stated cause and the process owner's acceptance, never as a standing post-quantum accommodation.

- **Testing without an outage:** A pilot observed only on a live link, with no failure injected, has tested the happy path and nothing else. Rollback, failover to the standby gateway and behavior when the post-quantum peer is unreachable are exercised by injecting the failures in a test environment that mirrors the zone or, where the program has none, inside an outage the program scheduled with the process owner's acceptance; deliberately causing a live outage is not a test method. A program that can obtain neither has not tested the change and records it as untested.
- **Bricking and rollback:** A firmware update that changes the signature verification key or the trust anchor on a field device is one write away from a device that trusts nothing. Require dual-bank firmware with tested rollback from the vendor (the tender template, Phase 7) and update one device per type before the fleet. Run the signer and the verifier as a coordinated rollout, under four stated conditions:

    1. The new verification key is installed and confirmed on the device before the first image signed under it ships.
    2. The previous image stays valid under the previous key for a stated acceptance period, during which rollback is permitted.
    3. Anti-rollback protection closes that period. After it, an image older than the protected one cannot be reinstalled.

4. The verifier change and the signer change happen in separate maintenance windows. The exception is a redundant system, where the change may be authorized as a rolling change with the rollback exercised on the first unit.

- **The dual-stack decade:** Gateways, concentrators and OT PKIs will accept classical and post-quantum peers side by side for as long as the device tail lasts, which in OT is a decade or more. A dual stack is a permanent operating state that requires governance. Record the deprecation date for classical acceptance per conduit, test the refusal where policy requires it, and report the classical-only population as its own line in the KPI supplement. An unreviewed dual stack is an open downgrade path.

The Encapsulate Strategy

Populations that will never support post-quantum cryptography natively within their service life are protected by placing the cryptography in front of them: a gateway or aggregation layer at the zone boundary terminates or wraps their traffic under quantum-safe algorithms, and the CBOM records the population as migrated by enclosure, with the gateway as the migrated component and the enclosed devices linked to it. The Universal lists the pattern in the mechanisms catalogue of its Crypto-Agility foundation, and the OT and SCADA row of its first-layer selection table (Activity 5.2) names the OT/IT boundary gateway as the first layer to migrate. In OT the strategy is a legitimate terminal state as well as a bridge, and the record says which.

- **Permanent enclosure.** Enclosure is permanent on three conditions: no vendor path to native support for the enclosed population within its remaining service life, the gateway as the only conduit into and out of the zone, and the residual risk inside the zone accepted by the SteerCo with the safety authority informed. A permanent entry includes a re-evaluation date.
- **Bridge enclosure.** Enclosure is a bridge when the vendor has a dated release for native support (graded for firmness), the population will be replaced on a refresh date on the roadmap, or the gateway covers a path the zone will later lose. A bridge entry includes its end date.
- **What the pattern does not cover.** The CBOM entry and the wave-exit record state two exclusions. The first is the zone behind the gateway, where traffic between enclosed devices stays as it was. The second is firmware-signing integrity, which is Track B and is untouched by any change on the transport path. An enclosed population is protected on the conduit the gateway controls and nowhere else.
- **The agility objective in OT.** The objective is met at this layer. Crypto-agility in OT means changing algorithms on a date the operator can plan. The gateway is the layer the operator changes without reopening a certified boundary: its algorithm changes by configuration while the population behind it is untouched, and the rehearsal (Activity 5.2) is run on it.

- **Agility-debt state per entry.** Each compensating-control entry records its agility-debt state: enclosed under an accepted exception (the gateway is agile and the population is not, with the exception signed), or enclosed as a bridge with the debt funded to a date. At closure every entry has either a funded treatment with a date or a SteerCo-signed exception (Migration Verification & Program Closure). The registry is the OT closure artifact for this population.

The controls that implement the strategy:

- **Quantum-safe VPN gateways:** Deploy approved PQC-capable VPN appliances at zone boundaries to protect the defined inter-zone or WAN segment, whatever the endpoints behind them support. The tunnel protects the segment between the participating gateways: the entry records the terminating gateways, the local legs that remain as they were and any device-authentication path the tunnel does not cover. Observe the negotiated outcome on the protected segment (Activity 4.6) and keep the residual exposure on the entry. The tunnel leaves firmware verification and application authorization inside the zone untouched.
- **Network segmentation hardening:** Strengthen IEC 62443 zones and conduits to limit blast radius of any quantum-enabled compromise.
- **Out-of-band firmware validation:** Some critical devices have a firmware verifier that cannot be upgraded. For those, validate the post-quantum signature on each image out of band, on a separate appliance, before the image reaches the device. State the boundary of the control on the entry, and put five things on the record:
  - Every update path to the device is controlled: the engineering workstation, the vendor's tool, removable media and the remote-support session.
  - The hash of the checked image is bound to the image the device receives.
  - The roles that can bypass the check are named, and their use is logged.
  - A failed check blocks the update.
  - The residual risk that the device itself still accepts a classical signature is recorded. The check adds a control in front of the device and changes nothing about what the device will accept.
- **Physical isolation:** For the most critical legacy devices, maintain or restore true air gaps where operationally feasible.

The June 2026 device-class measurement cited as a data source in this extension's opening section corroborates the pattern independently: its mitigation recommendation for hard-to-upgrade unmanaged devices is a secure remote access gateway that centralizes quantum-safe controls at the gateway while migration of the devices behind it remains incomplete, which is the bridge form of this strategy.

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, per cryptographic function. A device that only verifies LMS or XMSS firmware signatures needs only a small verifier; stateful hash-based signatures are the constrained option for that function and do not replace a KEM where confidentiality is required, so a device that establishes keys implements ML-KEM or is enclosed behind a gateway that does. Size buffers against the protocol and profile the device will actually carry rather than against a fixed combination of the largest parameter sets.

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.

The OT HSM and KMS register records the Universal's four fields (Activity 6.2): the visible platform, the supplier's firmware family, the manufacturer of origin and the FIPS 140-3 certificate reference, plus the entropy references (the SP 800-90B validation as an ESV certificate reference or the ENT designation on the module certificate, with the operating envelope). Two OT rows are always present: the firmware-signing module, whose conformance to section 8 of SP 800-208 (the alignment section) is recorded against its certificate with the parameter sets the certificate covers and the state-safety evidence inside the implementation, and the key store of the OT issuing CA.

An engineering workstation or a vendor's hosted signing service used to sign firmware is a register row with the fields it can fill and a delivery state of blocked until the keys move into a module that fills them.

Phase 7 – Vendor & Supply Chain Governance

OT Vendor Classification

- **Tier A – Timeline-blocking:** The PLC, RTU and DCS vendors of the installed base (the control-system vendors named in the June 2026 edition are listed in the front-matter

Tool and Vendor References), SIS vendors, protection relay vendors. Engage at executive level. Every date they give is graded for firmness.

- **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.

Questionnaire Order, Certificate-Authority Questions and the One-Afternoon Test

The questionnaire opens with the two agility questions and the firmness question (Universal Activity 7.2), and for OT products the second agility question is asked for the installed base: can the verifiers and trust stores of deployed devices be updated in the field, by what mechanism, and inside what maintenance window. The four certificate-authority questions (ML-DSA and FN-DSA end-entity issuance dates; hybrid or composite issuance; the public Web PKI roadmap where a vendor portal or remote HMI chains to public roots; the date the vendor's own CA signing keys become PQC-capable and how the root transition reaches deployed devices) are asked of every vendor that issues device identity certificates from its own CA, and of the operator's OT PKI provider.

Any product that includes a public-key algorithm not standardized by NIST or an equivalent national authority is disclosed and run through the one-afternoon test (Activity 7.3): public specification with test vectors, public cryptanalysis by parties other than its designers, a standards-body track, a validated or CAVP-tested implementation. A proprietary stack that fails the first two tests is excluded from approved-mode use, with the sovereignty caveat for a national algorithm mandated under a documented regime. Every roadmap date in this section and in the vendor scorecard is graded for firmness. Phase 3 scores the grade.

The OT Tender Template for Immediate Procurement

Firmware signing, verifier updatability and algorithm agility migrate at the vendor, so the deploy-now action in Phase 7 is the tender template: the requirement set below goes into every RFI, RFP and contract renewal for OT equipment and software from the day the program is chartered, before any device in the estate has been migrated. The categories are ordered agility first. A product that meets the last requirement and fails the first turns every future algorithm change into a procurement.

1. **Configuration-driven algorithm selection.** Key-establishment and signature algorithms, parameter sets and hybrid combinations change by configuration, without recompilation, reinstallation or hardware replacement, and hybrid operation (classical plus post-quantum, with the classical component removable by policy) is supported through the transition. The acceptance test is a rehearsed algorithm

change on the product before go-live, executed by the operator's team with the elapsed times recorded and the rollback exercised (Universal Activity 7.3).

2. **Updatable firmware signature schemes, with the algorithm and profile named.** The device verifies post-quantum firmware signatures at delivery under the algorithm and parameter set the tender names for the use case: LMS or XMSS under SP 800-208 as the default and the conservative choice for firmware, with the parameter set stated, or ML-DSA where the signing volume or the distribution model calls for it (the alignment section). Its trust anchors and verification keys can be updated in the field, by a documented and authenticated mechanism, inside a maintenance window.

Where the vendor signs with a stateful scheme, its signing service states three things: how it meets section 8 of SP 800-208 (Level 3 hardware, no key export, in-module state), which parameter sets its module's certificate covers, and the state-safety evidence inside the implementation.

3. **Dual-bank firmware with tested rollback.** Two firmware banks, a documented rollback to the previous image within the maintenance window, and the previous image kept valid under the previous verification key for the rollback period. The vendor demonstrates the rollback in acceptance testing.

4. **Disclosure of embedded cryptographic libraries and a device CBOM at delivery.** Every cryptographic library, its version and its algorithms, disclosed at delivery in a CycloneDX CBOM conforming to the Universal's minimum record (Activity 2.1). A CBOM conforming to the Applied Quantum CBOM Profile v1.0-RC or later is accepted and is not required. CBOM handling terms state how the vendor stores, transmits and retains the CBOMs it receives and produces (Activity 2.5).

5. **Headroom in key and signature size limits.** State the maximum key, certificate and signature sizes for every interface. Require headroom in every buffer, message and storage limit the product exposes, for the parameter sets the interface's protocol profile will use. Name that profile in the tender.

Two cases cover most devices. Where the interface will negotiate or verify them, size for ML-KEM-1024 keys and ML-DSA-65 signatures. Where firmware verification is the only public-key operation the device performs, size for that parameter set alone. A product sized to today's ECDSA and X25519 lengths has a hardcoded algorithm choice in its data structures.

6. **A committed PQC roadmap with contractual dates and a firmness grade.** Dates for native ML-KEM, ML-DSA and hybrid support per product line, each graded committed, forecast or announced, with remedies attached to the committed ones (maintenance credits, right to replace, termination), and no public-key algorithm outside the NIST standards or those of an equivalent national authority in approved-mode use.

The government model clauses cited in Universal Activity 7.3 are the exemplars to adapt. A tender issued without the template buys a device the program will enclose for its service life.

CNI/OT REGULATORY ALIGNMENT MAP

The table is a dated snapshot of the sector bodies and the instruments that set a sector date, as of September 2026, with the status at this edition and the enforcement tier that Phase 3 Dimension 4 reads (Universal, Regulatory & Standards Alignment Map). Jurisdiction rows that repeat the Universal's roster are not reproduced here. The roster is in the Universal's Regulatory Timeline Context and, kept current, on the Global PQC Migration Clock page (https://postquantum.com/pqc-migration-timelines/global-pqc-migration-clock/).

Authority / Standard	Requirement	Dates	Status at this edition	Enforcement tier	CNI/OT Implication
EU NIS2 and the NIS Cooperation Group coordinated roadmap	Entities designated under national implementation apply NIS2's security measures; Member States plan and execute the PQC transition (roadmap)	National strategies end-2026; high-risk and critical use cases by end-2030; remainder by 2035 where practically feasible	Roadmap published June 2025; COM(2026) 13 (January 20, 2026) proposed and not adopted at this edition	Tier 4, hardening to tier 2 or 3 through national transposition and supervision	Whether an operator is an essential or an important entity follows from the entity and designation criteria of the national implementation, not from its sector; record the national instrument and the operator's designation before attaching a label or a date. Plan critical use cases to 2030 (Challenge 10).

Authority / Standard	Requirement	Dates	Status at this edition	Enforcement tier	CNI/OT Implication
ANSSI (France)	Post-quantum cryptography required for security products entering qualification; quantum-safe purchasing by supervised organizations	Qualification gate from 2027; quantum-safe purchasing by 2030	Stated in ANSSI's PQC FAQ (October 8, 2025) and restated June 16, 2026	Tier 1, market access	Binds the security-product procurement of French administrations and operators of vital importance; the tender template passes it.
NERC CIP	Critical infrastructure protection for the bulk electric system	CIP-013, CIP-005, CIP-007 as in force	No PQC-specific requirement at this edition	Tier 3 for the requirements in force	Supply chain risk (CIP-013) and electronic security perimeters (CIP-005) are where quantum risk enters the program's evidence.
IEC 62443	Industrial automation and control systems security	Series ongoing	No PQC parameter in the published series at this edition	Tier 4; tier 1 where a customer or a certification scheme requires conformance	Zone and conduit requirements are the structure the Encapsulate strategy is built on.
TSA Security Directives	Pipeline and rail cybersecurity mandates	SD-02 series and rail directives as in force	No PQC date at this edition	Tier 3	Cybersecurity implementation plans are where the PQC roadmap is filed for pipeline and rail operators.
IEC 62351	Security for power system	Parts published,	PQC revision of the	Tier 4	Defines the TLS profile for IEC

Authority / Standard	Requirement	Dates	Status at this edition	Enforcement tier	CNI/OT Implication
	protocols	evolving	profiles not published at this edition; re-checked at each release		61850 station-bus MMS traffic (parts 3 and 4), the HMAC or AES-GMAC protection of GOOSE and Sampled Values (part 6, 2020 edition) and the key management under part 9; the substation's asymmetric exposure is the key management layer and the TLS-protected flows (Challenge 5), and grid migration waits on the PQC revision of those profiles.
Nuclear regulators	Cyber security for nuclear facilities	10 CFR 73.54 (US), national variants	No PQC date at this edition	Tier 3	Most restrictive change management. PQC for nuclear OT will be slowest; enclosure is the expected state.
CISA / DHS	Post-Quantum Considerations for Operational Technology; quantum-	Published October 2024; ongoing	Guidance in force	Tier 4	First dedicated federal OT PQC guidance. Anchors segmentation,

Authority / Standard	Requirement	Dates	Status at this edition	Enforcement tier	CNI/OT Implication
	readiness migration guidance for ICS				crypto-agile procurement and gateway expectations for ICS; cite it in business cases and vendor requirements.

CNI/OT MATURITY MODEL SUPPLEMENT

The levels, names and descriptions are the Universal's single 0 to 5 scale (Maturity Levels), used by the enterprise model and every per-phase table alike. The sector indicators are read beside them.

Level	Universal Level	CNI/OT-Specific Indicator
0	Unaware: no organizational awareness of quantum cryptographic risk; no activities planned or underway	No sector indicator.
1	Aware: quantum risk acknowledged at leadership level; initial education conducted; no formal program	Joint CISO/Chief Engineer sponsorship. TNFL risk communicated to safety governance. Regulatory pre-engagement initiated.
2	Initiated: formal program chartered; budget allocated; discovery underway; initial CBOM in development	Charter states both outcomes; Crypto-Agility and Cryptographic Record owners named. Cryptographic ownership register opened with OT operations and site engineering. IT/OT boundary inventory complete with evidence grades and a stated denominator. Firmware signing cataloged. SCADA WAN mapped. Facilities estate scoped. Purdue-aligned CBOM initiated.

Level	Universal Level	CNI/OT-Specific Indicator
3	Progressing: CBOM operational; risk scoring complete; hybrid pilots in production; vendor engagement active; KPIs reported	Scoring model ratified with the OT factors; agility-debt register produced, with the non-updatable-verifier population listed. Multi-track roadmap approved with maintenance windows and the recertification decision recorded per change. Encapsulate strategy defined per zone, with permanent and bridge entries distinguished. First algorithm-change rehearsal run on the boundary gateway. Tender template in every new OT procurement.
4	Advanced: Tier-1 systems migrated to hybrid/PQC; PKI modernized; crypto-agility demonstrated; vendor commitments secured	Tier-1 boundary equipment migrated with the negotiated outcome observed; Tier-1 firmware-signing, safety-function and device-identity entries that wait on a vendor release running under their named bridging pattern, with the release date graded for firmness. SCADA WAN PQC rollout in progress, two results in every wave-exit record. Encapsulate deployed for the blocked population in whatever tier the ordered test gives it, with every entry recording its agility-debt state. An algorithm change rehearsed on the gateway layer inside the agility window. Tier A vendor dates graded for firmness, with committed dates for firmware signing.

Level	Universal Level	CNI/OT-Specific Indicator
5	Optimized: estate-wide PQC migration substantially complete; crypto-agility is organizational capability; continuous monitoring and posture management operational	All accessible OT cryptography PQC-protected or enclosed. Safety-certified devices migrated, or enclosed under SteerCo-signed exceptions with the safety authority informed. CBOM maintained across Purdue levels by the Cryptographic Record owner. Standing rehearsal cadence on the gateway layer and the firmware-signing service. Agility-debt register at zero unaccepted debt: every remaining entry funded with a date or under a SteerCo-signed exception.

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.
- **Encapsulate coverage:** Percentage of non-migratable OT devices enclosed under the Encapsulate strategy, with the share under a signed exception and the share on a funded bridge reported separately.
- **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 the enumerated denominator (Phase 1) with a graded cryptographic finding, reported with the known population count, the unknown population from the accepted-gaps register, and the field-updatable and non-updatable populations shown separately. A count of Purdue levels touched is not a coverage figure.
- **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.
- **Classical-only acceptance:** Conduits on which the gateway or concentrator still accepts classical-only peers, each with its recorded deprecation date (the dual-stack decade, Phase 5).

Agility KPIs (CISO cascade, monthly; summarized to leadership under the Agility KPI)

The four agility KPIs of the Universal (Metrics, KPIs & Reporting) are measured on the layer the operator changes. The enclosed device population is reported beside them, never inside them.

KPI	OT measurement	Threshold
Configuration-driven share	Percentage of the known Tier-1 and Tier-2 population (boundary gateways, concentrators, OT issuers, the firmware-signing service, SCADA WAN endpoints) whose key-establishment and signature algorithms change by configuration, verified by rehearsal; the enclosed population and the unknown population from the accepted-gaps register are each their own line and never enter the numerator	Target by year from the roadmap's agility milestones; a year missed by more than 10 points triggers Crypto-Agility workstream review
Rehearsed time-to-change	Elapsed time across assessment, decision, change and verification on the most recent rehearsal, per track: on the gateway layer for Track A, on the firmware-signing service and the OT issuer for Track B (Activity 5.2)	Inside the agility window on the gateway layer; a rehearsal whose change segment cannot run without a maintenance window has found agility debt on that system, recorded in the register rather than as a variance
Agility-debt burn-down	Entries closed on the Phase 3 register per quarter, with the non-updatable-verifier population as the denominator and the enclosed-under-exception population reported beside it	Any quarter with no reduction triggers workstream review; before closure every remaining entry carries a funded treatment with a date or a SteerCo-signed exception
New-system agility compliance	Percentage of new OT procurements issued with the tender template, and percentage of deliveries passing the acceptance-test rehearsal before go-live	Below 95% in any quarter triggers procurement governance review

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, with the evidence grade of each finding. These are Tier-1 targets with the delivery state available.
- **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.
- **8. Open the cryptographic ownership register.** Sit down with OT operations, site engineering and facilities management before any discovery activity needs their cooperation, and name an owner for every embedded credential, certificate store and signing dependency the walkdown finds. A finding with no owner becomes a report nobody actions.
- **9. Name a Crypto-Agility owner in engineering.** Give the workstream an owner in the function that controls the gateway layer and the OT PKI, a budget line from Year 1, and the agility-debt register as its scope.
- **10. Schedule the first rehearsal on the pilot concentrator.** Change the key-establishment parameter set on the hybrid VPN pilot by configuration, time the four segments, roll it back, and file the timings. The result is the first agility KPI reading and the first entry in the closure evidence.

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/policy-standards-regulations/dhs-cisa-pqc-ot/ – Analysis of the first dedicated federal OT PQC guidance (October 2024).

Why HNDL Cannot Be Detected (July 2026 analysis) – https://postquantum.com/post-quantum/cannot-detect-harvest-now-decrypt-later/ – The reasoning behind the framework's HNDL position: inference from demonstrated capability, and why the harvest itself cannot be observed.

90% of SSH Servers Still Not Quantum-Safe: Forescout Data – https://postquantum.com/security-pqc/forescout-pqc-adoption-data-2026/ – The June 2026 device-class measurement this extension uses as its calibration point for the OT gap.

ANSSI Sets 2027 Deadline for Quantum-Safe Certification – https://postquantum.com/security-pqc/anssi-pqc-certification-2027/ – The procurement-gate example in Challenge 10.

The EU Just Proposed Including Post-Quantum Cryptography (PQC) in NIS2 – https://postquantum.com/security-pqc/eu-pqc-nis2/ – COM(2026) 13 and the chain from the coordinated roadmap to entity-level obligations.

The Global PQC Migration Clock – https://postquantum.com/pqc-migration-timelines/global-pqc-migration-clock/ – The maintained jurisdiction roster that this extension's regulatory map points to.

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.

APPENDIX J: REQUIREMENTS REGISTER

This register is generated from the text of this edition at each build and lists every statement in this extension that uses *must*. The four program-level provisions of the Universal Framework's Normative Convention bind this extension through its parent and are listed in the Universal's Appendix J; they are not repeated here. Every statement below binds inside the section that states it, and a statement that appears here without its section's conditions is read with them. The appendix letter matches the Universal's, so "Appendix J" names the requirements register in every document of the set.

Statements in document order

1. *Why CNI and OT Require a Sector Extension, Safety-Critical Operations Where Failure Has Physical Consequences.* Phase 5 (Pilots) and Phase 6 (Infrastructure) must incorporate assessment processes that most IT migration programs never encounter.
2. *Why CNI and OT Require a Sector Extension, Trust Now, Forge Later (TNFL) as the Primary Threat.* This means the Universal Framework's risk scoring (Phase 3) must weight signature and authentication functions more heavily than encryption in OT environments.
3. *Why CNI and OT Require a Sector Extension, Extreme Equipment Lifecycles and Constrained Hardware.* Many OT devices simply cannot handle these sizes and must be protected through network-layer compensating controls rather than endpoint upgrades (the Encapsulate strategy, Phase 5).
4. *Why CNI and OT Require a Sector Extension, Limited Patching Windows and Rigid Change Control.* 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.
5. *Why CNI and OT Require a Sector Extension, Converging IT/OT Architectures Creating Expanded Attack Surface.* The IT/OT boundary protections (DMZ firewalls, jump servers, VPN concentrators) must be among the first systems migrated to PQC.

6. *Industry-Specific Challenges, Challenge 1: Firmware Signing and Secure Boot Vulnerability*. Updating the trust anchor requires a firmware update, which itself must be verified using the existing quantum-vulnerable mechanism.

7. *Industry-Specific Challenges, Challenge 1: Firmware Signing and Secure Boot Vulnerability*. Framework Impact: Phase 1 must inventory all firmware signing mechanisms and trust anchors across the OT estate.

8. *Industry-Specific Challenges, Challenge 1: Firmware Signing and Secure Boot Vulnerability*. Phase 5 must include firmware signing migration pilots with key OT vendors.

9. *Industry-Specific Challenges, Challenge 1: Firmware Signing and Secure Boot Vulnerability*. Phase 7 must require vendors to publish PQC firmware signing roadmaps, with a firmness grade on every date.

10. *Industry-Specific Challenges, Challenge 2: Safety Instrumented System Certification Constraints.* Framework Impact: Phase 3 must score SIS-certified systems Critical on physical consequence, which places them at Tier 1 under the ordered test, with the change path scored per device from the recertification decision (Hard where the change reopens the safety case or needs a hardware replacement; Medium where the safety authority accepts it as a firmware campaign inside a maintenance window) and the delivery state blocked until the vendor's certified release exists where one is required.

11. *Industry-Specific Challenges, Challenge 2: Safety Instrumented System Certification Constraints.* Phase 4 must model safety re-certification timelines and record the recertification decision per change.

12. *Industry-Specific Challenges, Challenge 2: Safety Instrumented System Certification Constraints.* Phase 5 must use the Encapsulate strategy for SIS zones while native PQC migration is pending.

13. *Industry-Specific Challenges, Challenge 3: Industrial Protocol Cryptographic Poverty*. The result is a bimodal challenge: some OT communications have no cryptography to migrate, while others have quantum-vulnerable cryptography that must be upgraded.

14. *Industry-Specific Challenges, Challenge 3: Industrial Protocol Cryptographic Poverty*. Framework Impact: Phase 1 must categorize OT protocols as "no cryptography," "quantum-vulnerable," or "symmetric-only," and for a quantum-vulnerable protocol record where the asymmetric operation runs and whether its key establishment has forward secrecy.

15. *Industry-Specific Challenges, Challenge 3: Industrial Protocol Cryptographic Poverty.* Phase 5 must prioritize adding PQC-protected overlay encryption to currently unprotected critical OT links and must record the placement decision per protocol class and per segment in the CBOM: native, tunneled or terminated, the component that bears the processing load, and the classical leg that remains.

16. *Industry-Specific Challenges, Challenge 4: Remote Access and VPN Dependency.* Framework Impact: Phase 3 must score OT remote access VPNs Critical on Dimension 1 as internet-facing entries, which places them at Tier 1 under the ordered test, with the delivery state available.

17. *Industry-Specific Challenges, Challenge 4: Remote Access and VPN Dependency.* Phase 7 must track VPN vendor PQC timelines.

18. *Industry-Specific Challenges, Challenge 5: Substation Automation and Grid Protection.* Framework Impact: Phase 1 must inventory IEC 61850/62351 deployments and protection relay firmware, recording per substation which flows run under TLS (station-bus MMS, IEC 62351-3 and -4), which run under the IEC 62351-6 MAC (GOOSE and Sampled Values), and the IEC 62351-9 key management that distributes the MAC keys, with the certificates and trust anchors that layer depends on.

19. *Industry-Specific Challenges, Challenge 5: Substation Automation and Grid Protection.* Phase 6 must benchmark PQC overhead against protection relay timing requirements on the flows that carry it, the key-management exchange and the MMS session.

20. *Industry-Specific Challenges, Challenge 5: Substation Automation and Grid Protection.* Phase 7 must engage grid equipment vendors on the PQC revision of the IEC 62351 profiles and on the firmware path that delivers it to deployed relays.

21. *Industry-Specific Challenges, Challenge 6: SCADA Wide-Area Network Exposure.* Framework Impact: Phase 1 must map SCADA WAN encryption endpoints and, for DNP3, record whether Secure Authentication is enabled and whether the asymmetric Update Key option is in use.

22. *Industry-Specific Challenges, Challenge 6: SCADA Wide-Area Network Exposure.* Phase 3 must score SCADA WAN links for both HNDL and TNFL exposure.

23. *Industry-Specific Challenges, Challenge 6: SCADA Wide-Area Network Exposure.* Phase 6 must test PQC overhead against SCADA polling and response time requirements.

24. *Industry-Specific Challenges, Challenge 7: Extended-Validity Certificates and PKI in OT.* Framework Impact: Phase 2 (CBOM) must capture certificate validity periods, renewal mechanisms and verifier updatability.

25. *Industry-Specific Challenges, Challenge 7: Extended-Validity Certificates and PKI in OT.* Phase 4 must plan certificate migration campaigns aligned with maintenance windows.

26. *Industry-Specific Challenges, Challenge 7: Extended-Validity Certificates and PKI in OT.* Phase 6 must address OT-specific PKI automation gaps.

27. *Industry-Specific Challenges, Challenge 8: Vendor Lock-In and Proprietary Cryptographic Stacks.* Framework Impact: Phase 2 must include vendor disclosure requests and CBOM generation through passive network observation.

28. *Industry-Specific Challenges, Challenge 8: Vendor Lock-In and Proprietary Cryptographic Stacks.* Phase 7 must issue this extension's tender template for all new OT procurement, agility requirements first.

29. *Industry-Specific Challenges, Challenge 9: Physical Security and Environmental Constraints.* Framework Impact: Phase 4 must model physical access and environmental constraints for each OT zone.

30. *Industry-Specific Challenges, Challenge 9: Physical Security and Environmental Constraints.* Phase 6 must assess which devices require hardware replacement vs. firmware update vs. compensating controls.

31. *Industry-Specific Challenges, Challenge 10: Regulatory Fragmentation Across CNI Sectors.* ANSSI's published position (FAQ on post-quantum cryptography, October 8, 2025; restated at France Quantum on June 16, 2026) is that security products entering ANSSI qualification from 2027 must include post-quantum cryptography, with the organizations it supervises to buy only quantum-safe solutions by 2030.

32. *Industry-Specific Challenges, Challenge 10: Regulatory Fragmentation Across CNI Sectors.* Framework Impact: Phase 0 must map all applicable CNI regulations and their quantum/cryptographic requirements and tag each with its enforcement tier.

33. *Industry-Specific Challenges, Challenge 10: Regulatory Fragmentation Across CNI Sectors.* Phase 4 must align with the most demanding regulatory timeline.

34. *Industry-Specific Challenges, Challenge 10: Regulatory Fragmentation Across CNI Sectors.* Phase 7 must issue the tender template.

35. *Industry-Specific Challenges, Challenge 10: Regulatory Fragmentation Across CNI Sectors.* New equipment must pass the procurement gates the operator is subject to.

36. *Industry-Specific Challenges, Challenge 11: Process Historians and Long-Horizon Operational Data.* Framework Impact: Phase 1 data classification must include historian estates, engineering repositories, and their replication paths, with confidentiality horizons set from asset life.

37. *Industry-Specific Challenges, Challenge 11: Process Historians and Long-Horizon Operational Data.* Phase 6 capacity planning must account for re-encryption at historian scale, which is a throughput problem before it is a cryptographic one.

38. *Alignment with Universal Framework v3.0, SP 800-208 Firmware Signing for Immediate OT Deployment.* A signing service that does not meet section 8 is not a conforming deployment, and the verifiers in the field must accept the parameter set chosen.

39. *Phase 0 adaptation, Governance Adaptation.* OT engineering and process safety must have co-equal status with IT security.

40. *Phase 1 adaptation, The Asset Discovery Problem in OT.* The framework must accept that OT cryptographic inventory will be incomplete and use risk-driven scoping.

41. *Phase 4 adaptation, Maintenance Window Alignment.* OT migration roadmaps must be aligned with planned maintenance windows.

42. *Phase 6 adaptation, OT-Specific Performance Constraints.* - Protection relay timing: Grid relays must operate within single-digit millisecond latency.

43. *Phase 6 adaptation, OT-Specific Performance Constraints.* PQC key exchange must not cause polling timeouts.

44. *Phase 6 adaptation, OT-Specific Performance Constraints.* PQC must not introduce destabilizing jitter.

ABOUT

ABOUT THE AUTHOR

Marin Ivezic is a former Fortune Global 500 CISO/CTO, the founder and CEO of Applied Quantum, and the founder of Quantum Academy (QuantumAcademy.com). PostQuantum.com is his personal blog. 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 standards, products and deadlines change, and the book supplies the depth that a methodology document omits by design.

QUANTUM ACADEMY

Quantum Academy (QuantumAcademy.com), founded by the author, offers trainings and certifications on the topics this framework covers, from executive education on quantum risk to practitioner courses on PQC migration, crypto-agility and cryptographic inventory, for the roles and training levels described in Skills & Team Structure.

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