Post-Quantum Cryptography for ICS Gateways

From quantum risk to practical OT trust-chain transition

Shaun Chen, CCSP, CISSP
AVP, APJ Lead Architect for AI & Quantum Security, THALES

Agenda: From Quantum Risk to OT Transition

1. **Quantum risk in plain language**

   What changes, what PQC is, and why standards now matter.

2. **Why it matters to OT**

   Lifecycle mismatch, HNDL / HNFL (harvest now — decrypt or forge later), remote access, and gateways.

3. **Where to start**

   Prioritize high-consequence trust boundaries:

   remote access, vendor access, ICS gateways, control-center links, and long-lived data.

4. **How to transition safely**

   Crypto-agility, hybrid PQC, operational resilience, governance, and demo.

PQC in Plain Language

PQC is the replacement path for public-key crypto before quantum risk becomes practical

Today’s trust foundation

Secure connections with key exchange

Certificates, device and user authentication

Digital signatures

What changes with quantum

Future quantum computers could break RSA/ECC.

PQC algorithms resist quantum attacks and run on today’s classical systems.

NIST standardized ML-KEM, ML-DSA, and SLH-DSA in 2024.

RSA/ECC: Key Exchange, Authentication, Signatures

PQC: ML-KEM, ML-DSA, SLH-DSA

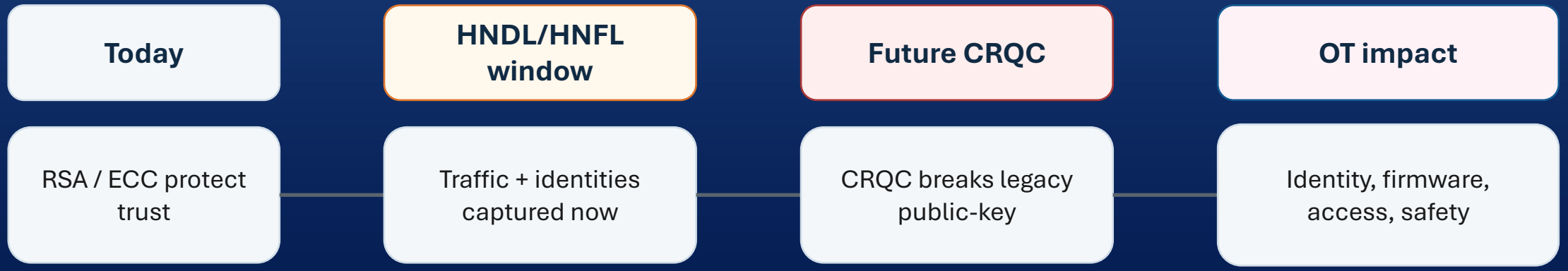
Quantum Risk Is Cryptographic Trust Risk

Trust function	Current dependency	Quantum concern
Key exchange	RSA / ECC-based mechanisms	May be broken by a future CRQC (Cryptographically Relevant Quantum Computer)
Authentication	Certificates / public-key trust	Certificate-based identity assurance may weaken
Digital signatures	RSA / ECDSA	Firmware / update integrity may be affected
Long-lived confidentiality	Encrypted traffic/data	Harvest-now-decrypt-later (HNDL)

CSA's Quantum-Safe Handbook and Quantum Readiness Index (2025) help organizations assess readiness and prioritize migration.

Quantum Risk in OT Terms

Lifecycle overlap: 2026 assets run past 2035



Lifecycle overlap

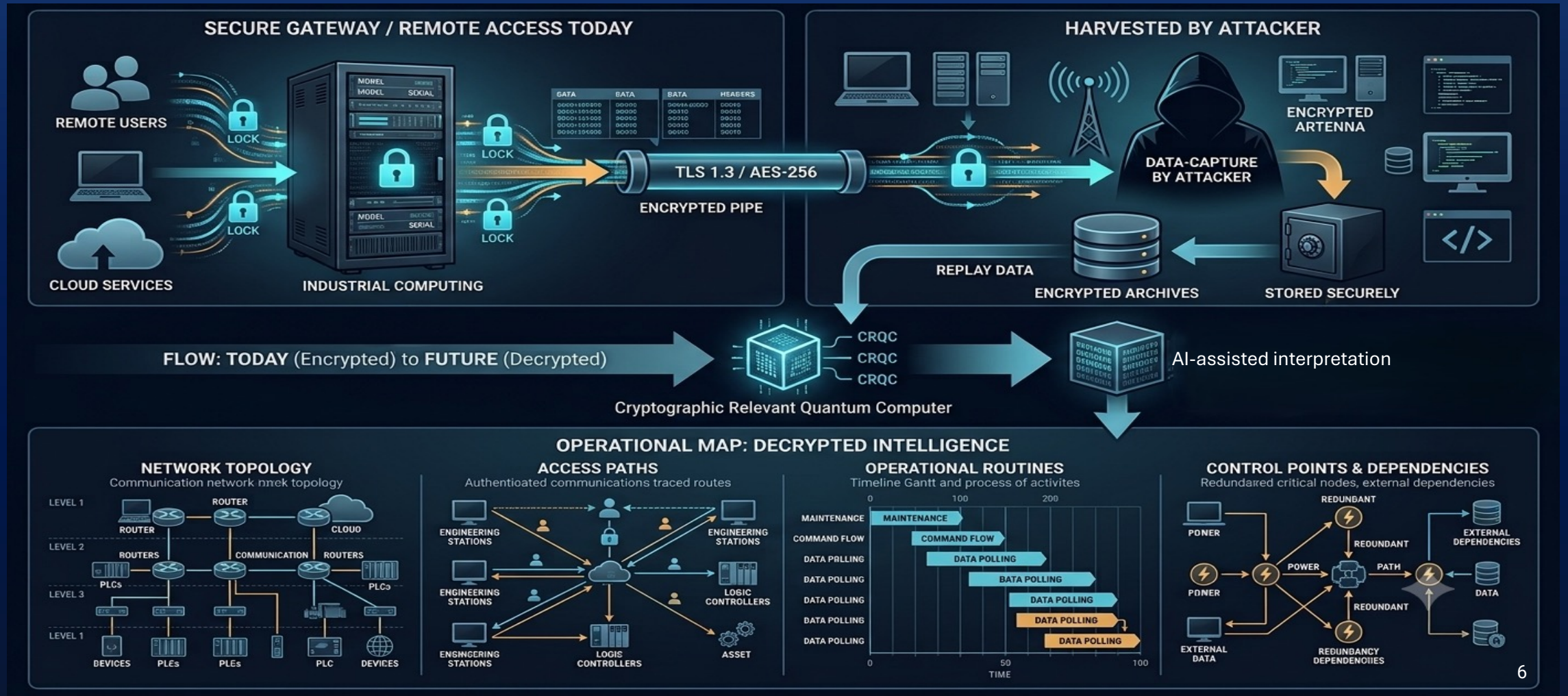
RSA / ECC: deprecated 2030, disallowed 2035 (NIST IR 8547)
OT asset life: 15–30 years — well past the crypto horizon
The overlap is the exposure window — plan inside it

Air-gapped does not mean crypto-free

Isolation reduces exposure
but trust still crosses via:
updates, backups, vendor tools,
engineering access, signed firmware

HNDL in OT: The Risk Is the Map

Captured encrypted traffic today may become tomorrow's operational map:



Case Reference: FrostyGoop (2024)

What happened:

Public reporting described OT-impacting malware using Modbus TCP, contributing to heating disruption across 600+ buildings in Lviv.

Why it mattered:

Once the OT pathway was exposed, controllers accepted Modbus TCP commands with limited downstream validation. This was not a quantum attack — it shows how weakly governed OT pathways can be exploited.

PQC relevance:

Start planning at the same high-consequence boundaries where remote access, gateways, and OT control paths meet.

*Case takeaway: **boundary trust** is operational resilience.*

Where to Start: Prioritize Trust Boundaries

Start where four factors intersect:

Exposure
+ Operational consequence
+ Asset / data lifetime
+ Migration feasibility
= PQC priority

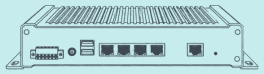
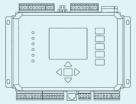
Priority-first approach

1. Identify high-consequence OT capability.
2. Map its cryptographic trust boundary.
3. Inventory keys, certificates, tunnels, and protocols around that boundary.
4. Build it passively: network observation, offline config review, vendor attestation — no active scanning at lower OT levels.
5. Classify control ownership and vendor dependency.
6. Decide pilot and migration sequence; output a CBOM (CycloneDX 1.6) keyed to remaining service life.

Priority Use Case: Remote Access and ICS Gateways

Use case	Why it matters	PQC relevance
Remote/Vendor access	External or semi-exposed path; third-party operational dependency	Protects sessions and long-lived access trust relationships
ICS gateway	Concentrates segmentation, protocol translation, telemetry, command paths	High-value trust chokepoint
Site/control-center link	High-consequence communications path	Availability and integrity-sensitive
Engineering data transfer	Long-lived sensitive data	HNDL concern

Three Asset Classes. Three Migration Playbooks.

Asset type	Action	Typical characteristics	PQC placement / playbook
 **Class A**	**Agile now** ⭐Recommended First Step	Remote access Modern gateway Software-updatable crypto	**Start with gateways and remote access** **Deploy hybrid PQC at OT gateways**
 **Class B**	**OEM-dependent**	Capable hardware Vendor firmware + certification dependency	Track vendor firmware, support, and safety certification
 **Class C**	**Contain and protect**	Embedded cryptography Legacy hardware Serial-only / microcode	Use gateways; segment; assign residual risk
 **New**	**Specify PQC now**	Assets bought today may operate for 10–15+ years	Add crypto-agility and PQC roadmap to every OT RFP

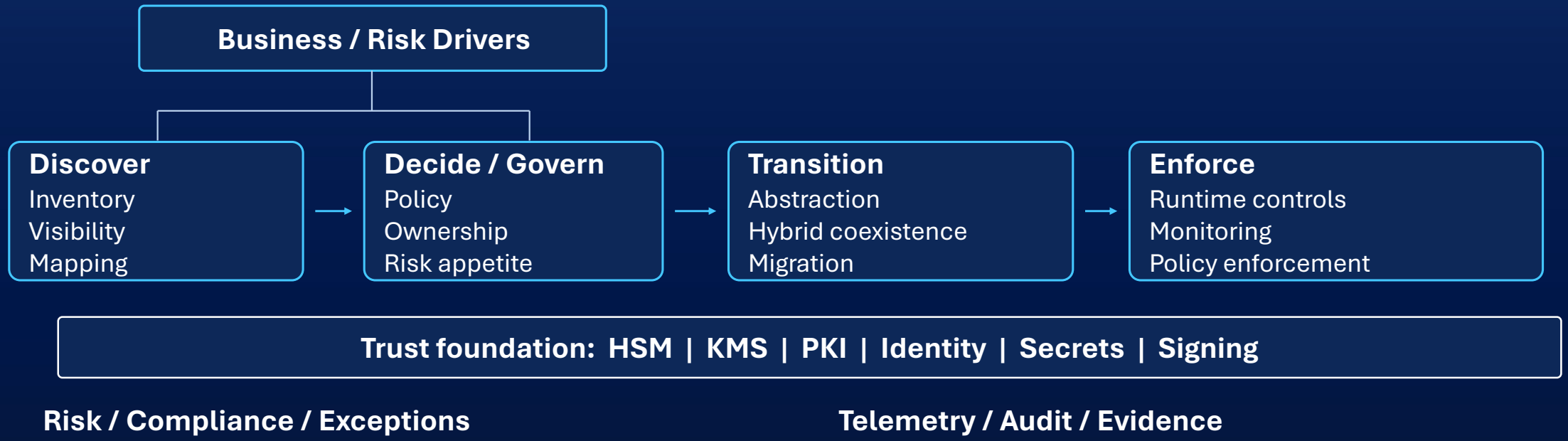
Start with gateways and remote access — wrap legacy assets, manage vendors, and specify PQC-ready purchases.

Migration Principle: Crypto-Agility as an Operating Model

Crypto-agility:

Identify, replace, test, and govern cryptography without redesigning the OT environment.

Agility ends at vendor microcode: Class C never becomes agile — plan compensating architecture instead.



Migration Approach: Hybrid PQC Transition

Hybrid transition:

Classical cryptography

+

Post-quantum cryptography

↓

Transitional trust model

Benefits:

- Preserves current assurance while adding PQC protection
- Supports phased migration
- Reduces dependency on ecosystem-wide cutover

Costs / constraints:

- Larger keys, ciphertexts, and signatures
- Performance and latency testing
- Interoperability and vendor support dependency

Hybrid shifts risk from algorithm choice to interoperability and operations — unalarmed fallback to classical is an adversary-selectable downgrade.

Why Placement Matters: The Handshake Budget

Impact area	OT concern
Larger key exchange payloads	Fragmentation and middlebox behavior
Larger signatures / certificates	Embedded parser and buffer limits
Reconnect / rekey events	Latency spikes and failsafe-timer interaction
Narrowband links	Handshake may exceed timing assumptions

Deterministic protection traffic (GOOSE / SV) is not the migration target — PQC protects key distribution and boundary trust only.

Operational Governance for PQC Deployment

Governance area	Practical requirement
Lab validation	Gateway-class silicon: performance, failover
Pilot scope	Start with gateway or remote-access path
Parallel running	Compare classical and hybrid/PQC path
Rollback	Fail-open/closed per boundary; alarm on fallback
Fallback operation	Ensure manual / alternative operating process
Vendor validation	Roadmap in writing; warranty + SIL/TÜV impact resolved
Telemetry	Certs, keys, tunnels; P95 latency vs failsafe timers
Evidence	Keep decision log, test results, exceptions

CSA's OT Masterplan 2024 is structured around People, Process, and Technology, and promotes Secure-by-Deployment principles.

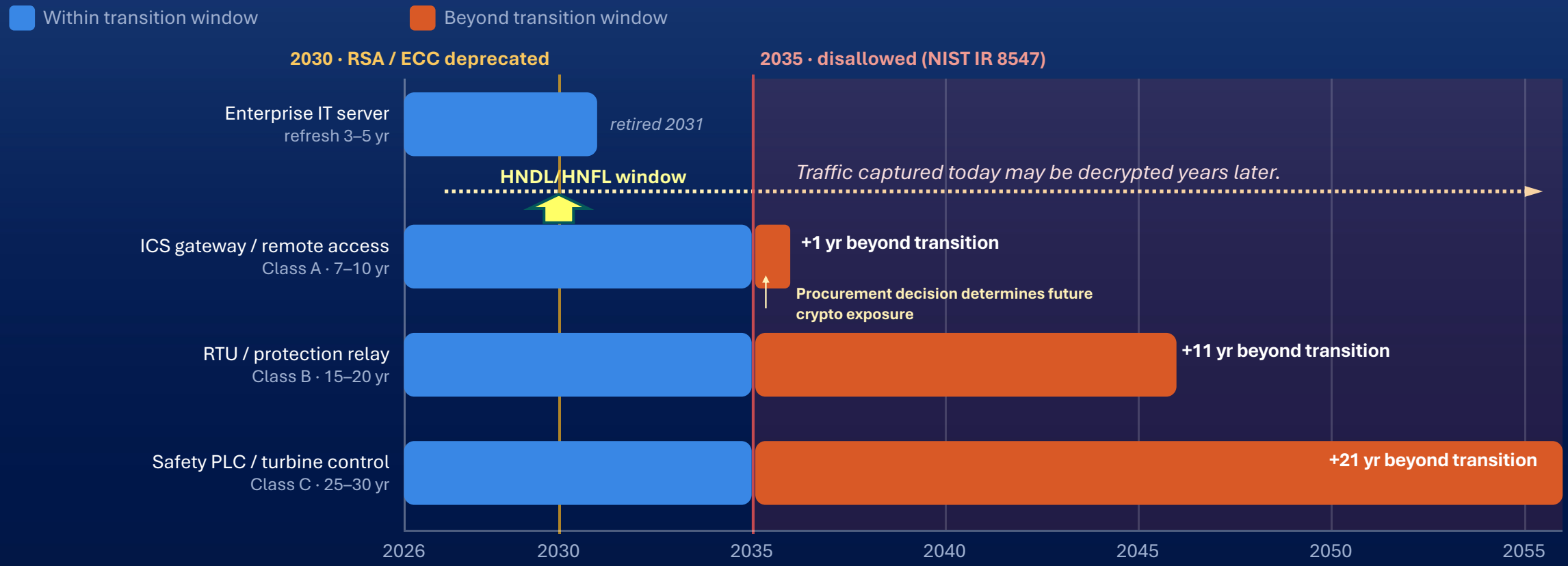
The Vendor Dependency Chain — and the Real Timeline

Dependency stage	Where it stands (mid-2026)
1. NIST algorithm standards — done. FIPS 203 / 204 / 205 published Aug 2024	IR 8547: RSA / ECC deprecated after 2030, disallowed after 2035
2. Protocol standards: IEC 62351, OPC UA profiles, DNP3-SA — PQC editions not yet published	OEMs cannot ship compliant firmware before the standards move
3. OEM firmware + safety recertification — Installed-base controller PQC roadmaps remain immature or uneven across vendors.	TÜV / SIL recertification adds years per family; Require vendor disclosure of firmware-signing algorithms and a quantum-resistant signing roadmap.

For most of this decade, the only control we can deploy unilaterally is external wrapping at boundaries.

Everything inside the vendor stack is contract management — get the roadmap in writing.

The Overlap Creates the Risk: Asset Life vs Cryptographic Trust



Most OT assets will outlive today's public-key cryptography.

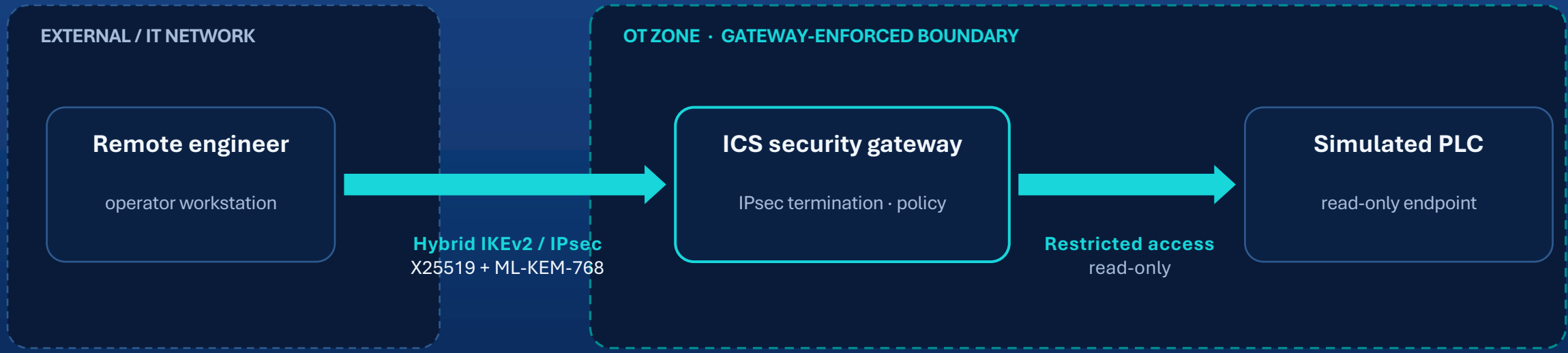
The lifecycle risk is determined at procurement—include PQC readiness and crypto-agility requirements in every OT RFP today.

Reference: NIST IR 8547 transition milestones.

TECHNICAL DEMONSTRATION · LAB VALIDATION

Demo: Hybrid PQC IPsec for ICS Gateway Protection

Objective — demonstrate quantum-resistant key establishment protecting remote access at the OT boundary, with access strictly tied to tunnel state and classical-only negotiation refused.



THE DEMO IS DESIGNED TO SHOW

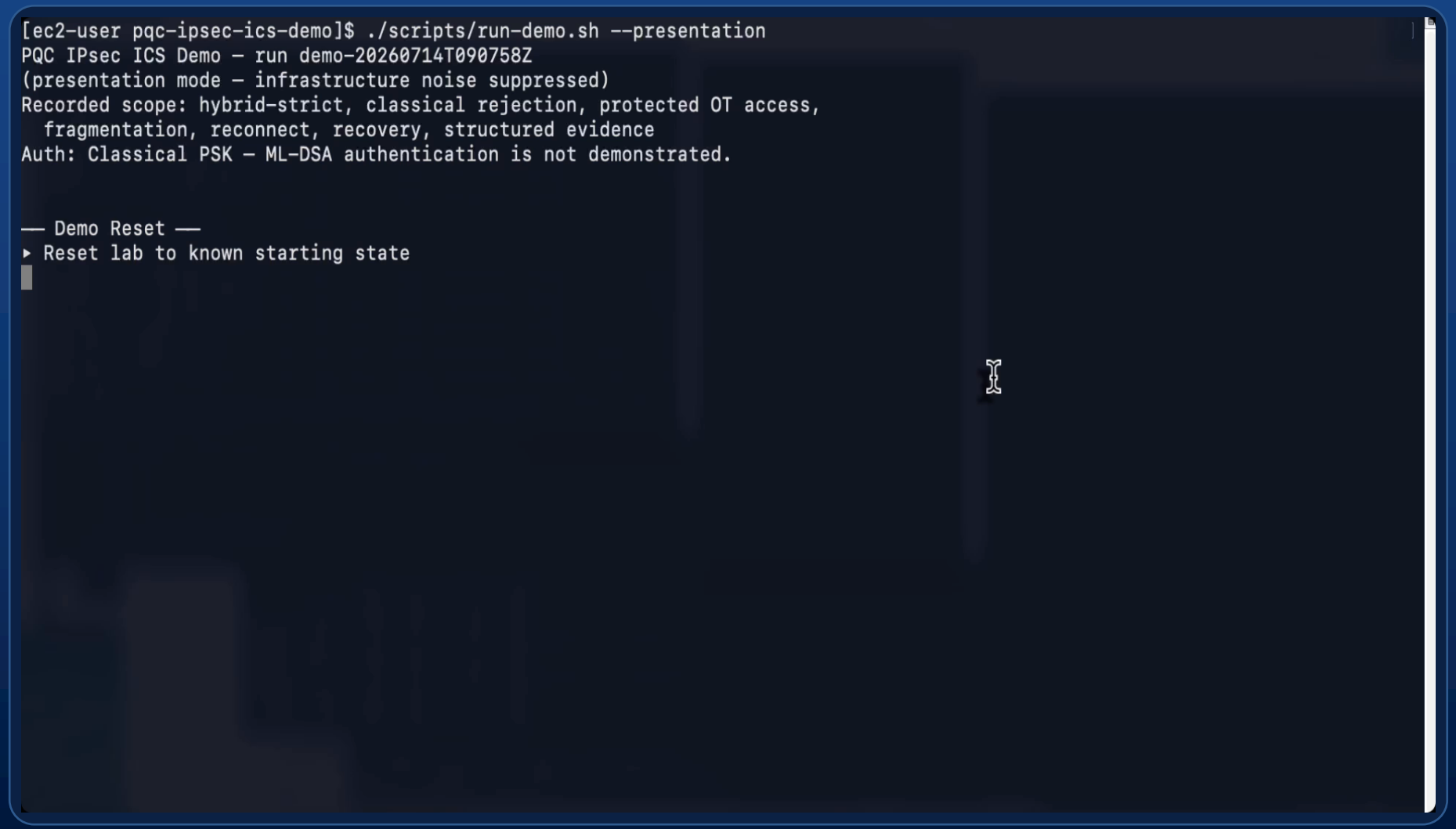
- Runtime hybrid negotiation
- Access tied to tunnel state
- Classical-only refused
- Evidence integrity

Vendor-neutral, standards-based mechanisms: IKEv2 (RFC 7296), hybrid key exchange, ML-KEM-768 (FIPS 203).

RECORDED DEMONSTRATION

Hybrid PQC IPsec — runtime evidence

2 min 08 s · 1080p



Terminal capture, presentation mode — hybrid-strict negotiation, classical rejection, protected OT access, fragmentation, reconnect and recovery, structured evidence.

OUTCOMES · SCOPE · TAKEAWAY

What the Demo Established — and What It Did Not

VALIDATED OUTCOMES

- ✓ Runtime hybrid negotiation evidenced
- ✓ Protected OT access succeeded
- ✓ OT access blocked after tunnel teardown
- ✓ Classical-only negotiation rejected
- ✓ RFC 7383 IKEv2 fragmentation observed at MTU 1280
- ✓ Reconnect and recovery tests passed
- ✓ Evidence package hash verification passed

SCOPE LIMITATIONS

- — Classical PSK authentication
- — ML-DSA authentication not demonstrated
- — Single implementation stack
- — Simulated OT endpoint
- — Lab validation — not production performance or HA certification

Takeaway — hybrid PQC key establishment can protect OT boundary access today using standards-based IKEv2. These results are lab evidence of feasibility and enforcement behavior — not a production or certification claim.

Key Takeaways

1

Quantum risk is real — prepare, don’t panic.

NIST standards published; CSA handbook and QRI released.

2

Start at high-consequence trust boundaries.

Passive-first CBOM; PQC stops at the gateway.

3

PQC transition must be operationally governed.

Crypto-agility, hybrid PQC, timing budgets, downgrade alarms, procurement, evidence.

Quantum-safe OT is achieved by disciplined trust-chain transition, not panic-driven replacement.

Q&A

Post-Quantum Cryptography for ICS Gateways

References and source anchors

- NIST Post-Quantum Cryptography standards: FIPS 203 ML-KEM, FIPS 204 ML-DSA, FIPS 205 SLH-DSA.
- Cyber Security Agency of Singapore: Quantum-Safe Handbook, Quantum Readiness Index, and OT Masterplan 2024.
- MAS Advisory on Addressing the Cybersecurity Risks Associated with Quantum, 20 Feb 2024.
- Banque de France and MAS Quantum-Safe Experiment Report, Nov 2024.
- NIST SP 800-82 Revision 3 — Guide to Operational Technology (OT) Security.
- NIST IR 8547 — Transition to PQC Standards: classical public-key deprecated 2030, disallowed 2035.
- NIST SP 800-208 — Stateful Hash-Based Signatures (LMS / XMSS) for firmware signing; NSA CNSA 2.0 timelines.
- RFC 7383 — IKEv2 Fragmentation; CycloneDX 1.6 — Cryptographic Bill of Materials (CBOM).

Feedback form

BACKUP · Q&A

What About QKD? Complementary in Selective Use Cases

QKD distributes symmetric keys over dedicated quantum channels. It solves a different, narrower problem than PQC — and it is not where an OT migration starts.

WHERE QKD FITS

- ✓ **Fixed, high-value point-to-point links** where dedicated fiber or engineered free-space infrastructure already exists
- ✓ **Additional key-distribution assurance** for selected high-consequence communications
- ✓ **Must be paired with quantum-resistant authentication** — it does not replace PQC
- ✓ **Singapore context:** NQSN+ networks are being deployed nationwide to support integration of PQC and QKD

WHY IT IS NOT THE OT STARTING POINT

- — **Specialized infrastructure** — dedicated links, endpoint hardware, distance engineering and potentially trusted relays
- — **Authentication remains separate** — QKD distributes keying material but does not authenticate the communicating parties
- — **Limited fleet scalability** — not easily deployed across diverse, long-lived OT estates during normal change windows
- — **Guidance differs by jurisdiction** — Singapore recognizes niche complementary use; NSA and UK NCSC prioritize PQC for national-security and government systems

Doctrine unchanged — begin with PQC at replaceable gateway and network-encryption boundaries. QKD may add another key source on selected high-assurance links, without changing PLCs or field protocols.

Wrapping the Long Links: PQC-Capable Network Encryptors

A boundary-first option for persistent, geographically exposed, high-consequence OT links.

WHERE THEY FIT

- ✓ **Site ↔ control centre, disaster recovery and metro trunks** — persistent, high-consequence links
- ✓ **External-wrapper deployment** — protects the communication boundary without changing controller firmware or the certified safety function
- ✓ **Addresses long-lived exposure** — historian replication, engineering transfers, configuration data and backups
- ✓ **Line-rate Layer 2/3 protection** — MACsec for suitable Ethernet services; hardware IPsec for routed WANs

SELECTION AND GOVERNANCE CRITERIA

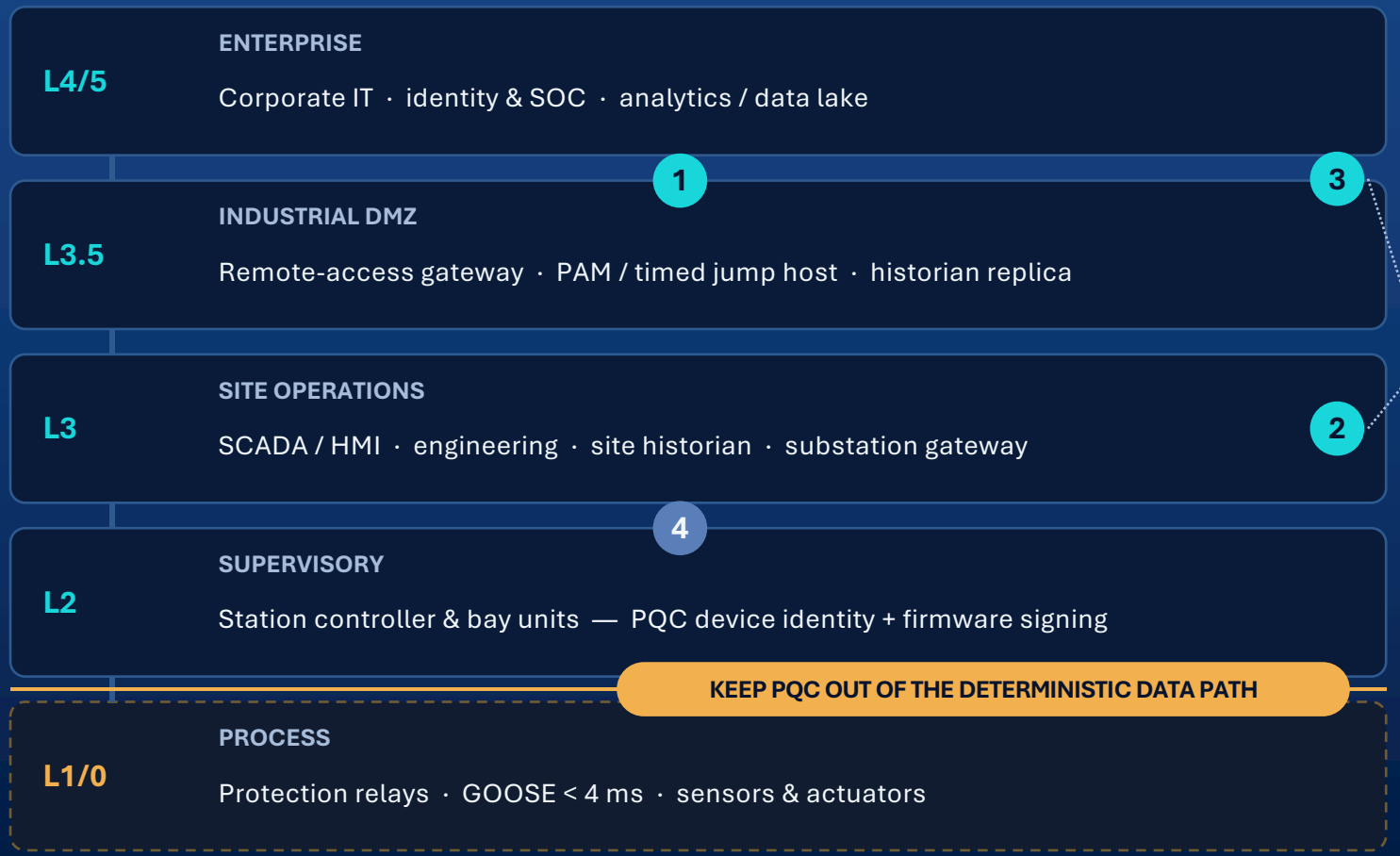
- — Hybrid classical + ML-KEM key establishment with explicit evidence of the negotiated cryptographic profile
- — **Fail closed or alarm on classical-only fallback** according to the approved transition policy
- — Validate latency, jitter, MTU, rekey and failover behaviour against operational and failsafe requirements
- — **Verify CMVP / FIPS 140-3 scope and approved mode**, including explicit coverage of required PQC algorithms
- — Crypto agility & supply chain — algorithm update path, library provenance, signed firmware, SBOM/CBOM, lifecycle support
- — **Interoperability & recovery** — test endpoints, rekeying, loss of peer, rollback, key recovery and mixed-version operation before cutover

Category, not product — evaluate any vendor against these criteria. The control is the wrapped boundary, not the box.

BACKUP · WORKSHOP CANVAS

Where PQC Fits in OT: The Bigger Picture

Four practical insertion points — modernise replaceable trust boundaries first, without disrupting the deterministic process loop.



1 Remote & vendor access — IDMZ

Hybrid IKEv2/IPsec using X25519 + ML-KEM-768. Deployable now — demonstrated, slides 17–19.

2 Site ↔ site trunks — WAN

High-speed encryptors: MACsec for Layer 2 services or hardware IPsec for routed WANs; hybrid + ML-KEM. Deployable now.

3 Historian replication & backups

Assess next: long-lived data flows may require hybrid TLS and re-encryption planning.

4 Identity & firmware signing

PQC PKI / KMS trust plane at L2 — longer-term, OEM-dependent migration; not deployable unilaterally.

Below the line — GOOSE, Sampled Values and process traffic retain deterministic symmetric protection. PQC strengthens key establishment, identity and software trust outside the real-time message path.