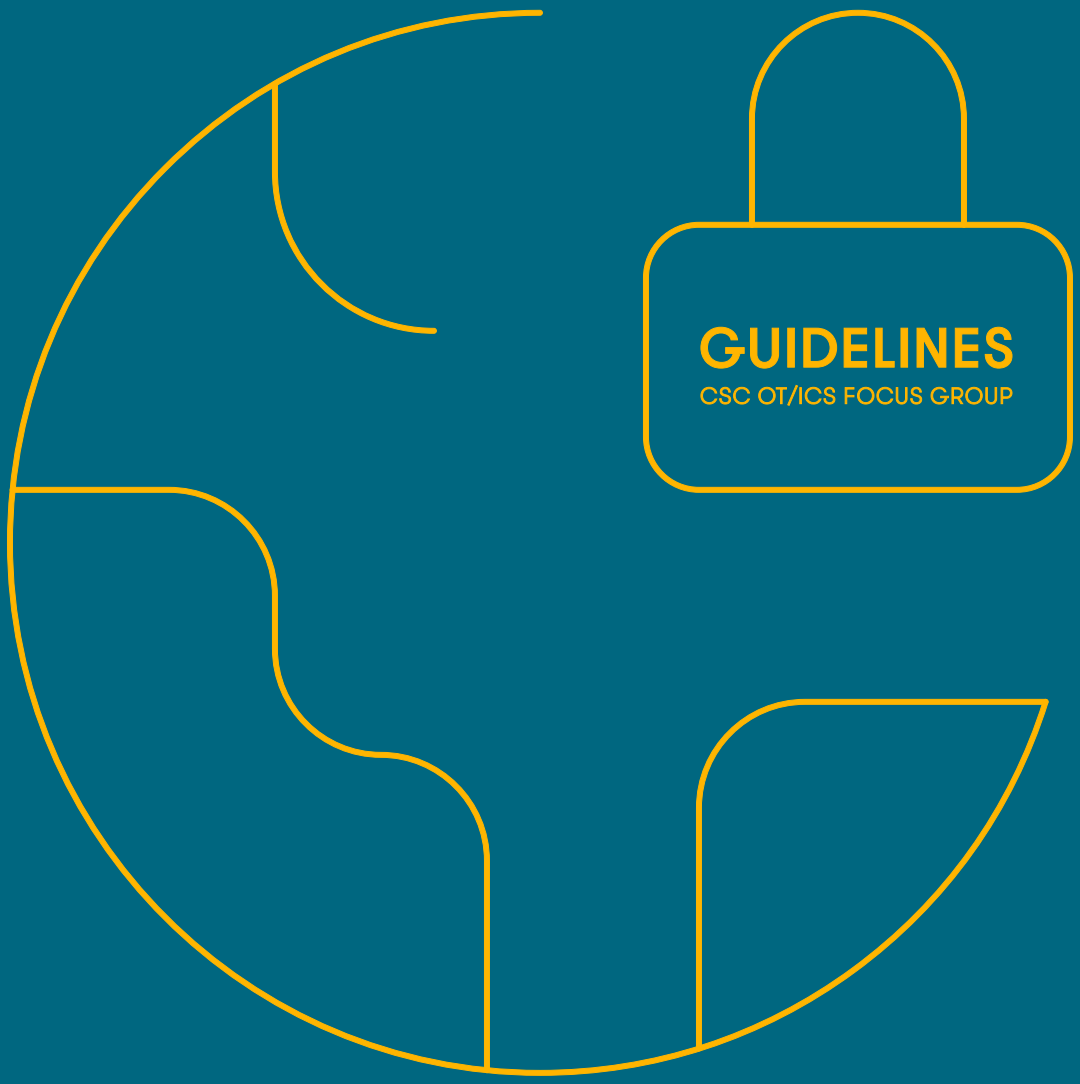


PQC IN OT

Plan for the decades to come



The TL;DR 3
About Post-Quantum Cryptography 4
The Challenge is Different for OTs 5
The Priority is the Boundary 6
Firmware Signing Deserves Attention 7
Availability and Safety Determine the Priorities 8
The Deepest Layers Will Go Last... or Not At All 9
The Real Programme is Cryptographic Lifecycle Management 10
What To Do About It 11
The Central Lesson 12



Post-quantum cryptography (PQC) is becoming an issue for every organisation that depends on long-lasting digital trust. For active operational technology (OT), the objective is not simply to deploy new algorithms to comply with new regulations. It is to preserve trustworthy access, operations and software while keeping industrial processes available and safe. The main focus of this article is how to start making OT plants and sites PQC ready, efficiently and result-driven.



The TL;DR

Post-quantum cryptography is not a reason to replace or alter every device: OT systems last for decades and cannot risk disruption to safety or availability.

Start by strengthening the external facing components, migrating relatively easily upgradeable trust boundaries — remote access, certificate validation chains, external links, and firmware or software signing — using hybrid approaches where appropriate.

Assess the cryptographic risk against the potential impact of the change procedure.

Test performance, interoperability, failure recovery, and rollback at gateways before expanding and iterating, and build crypto-agility requirements and capabilities into procurement and refresh cycles.

Protect legacy control networks with segmentation and other already established controls; PQC does not secure protocols that lack cryptographic protections or do not support them.

01

About Post-Quantum Cryptography

Post-quantum cryptography refers to cryptographic algorithms designed to resist attacks from both conventional and sufficiently capable quantum computers. It runs on conventional hardware and networks and is intended to replace soon-to-be-vulnerable public-key mechanisms.

A cryptographically relevant quantum computer could undermine RSA, Diffie–Hellman, ECDH and ECDSA, the so-called asymmetric cryptography. These mechanisms currently support many of the security functionalities we know, such as key establishment, certificates, device and user authentication, digital signatures, secure remote access and software authenticity. PQC introduces new key-establishment and signature algorithms designed to provide those functions without relying on the mathematical challenges that quantum algorithms can efficiently break.

Not all cryptography is subject to the same impact. Symmetric cryptography is less directly affected and can generally remain suitable with adequate key sizes. Therefore, for this text, we will only consider the migration of asymmetric cryptography mechanisms.

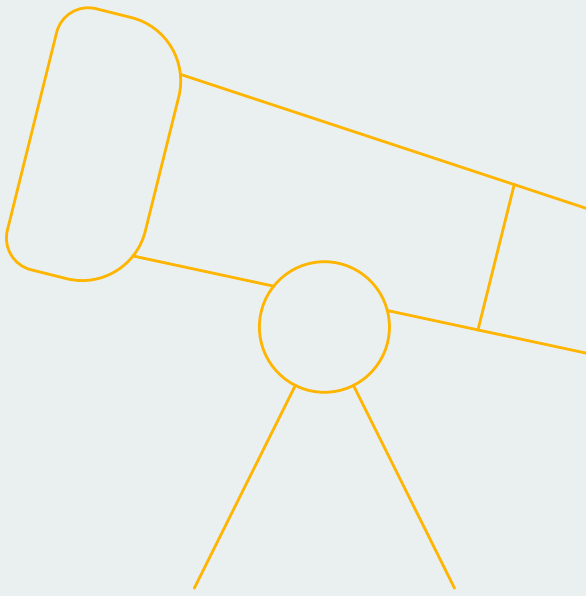
During migration, organisations will commonly use hybrid approaches that combine classical and post-quantum mechanisms. The classical component maintains compatibility and protects against potential weaknesses in a PQC algorithm, whilst the post-quantum component addresses future quantum attacks.

The best-known PQC threat is “harvest now, decrypt later” attacks: an attacker records encrypted data today and decrypts it once a capable quantum computer exists. This matters when information must remain confidential for many years. What typically remains unsaid is that PQC also protects a broader and often more operationally important property: the future authenticity of identities, software, firmware and digital commands.

Because of these threats, authorities have defined advisories and timelines to tackle PQC. There are several milestones we face, which are coordinated on several levels: US-Based NIST IR 8547 (deprecate quantum-vulnerable algorithms by 2030, disallow by 2035) and the EU coordinated PQC roadmap (similar 2030/2035 milestones).

These timelines seem short, but take into consideration that if we calculate the urgency by: how long data or signatures must stay trustworthy plus the needed migration time, in most cases it is greater than the time until a quantum computer can break them. So in fact, you’re most probably already late.

PQC doesn’t require quantum hardware. It is a new generation of cryptography designed to run on conventional systems while resisting future quantum attacks.



02

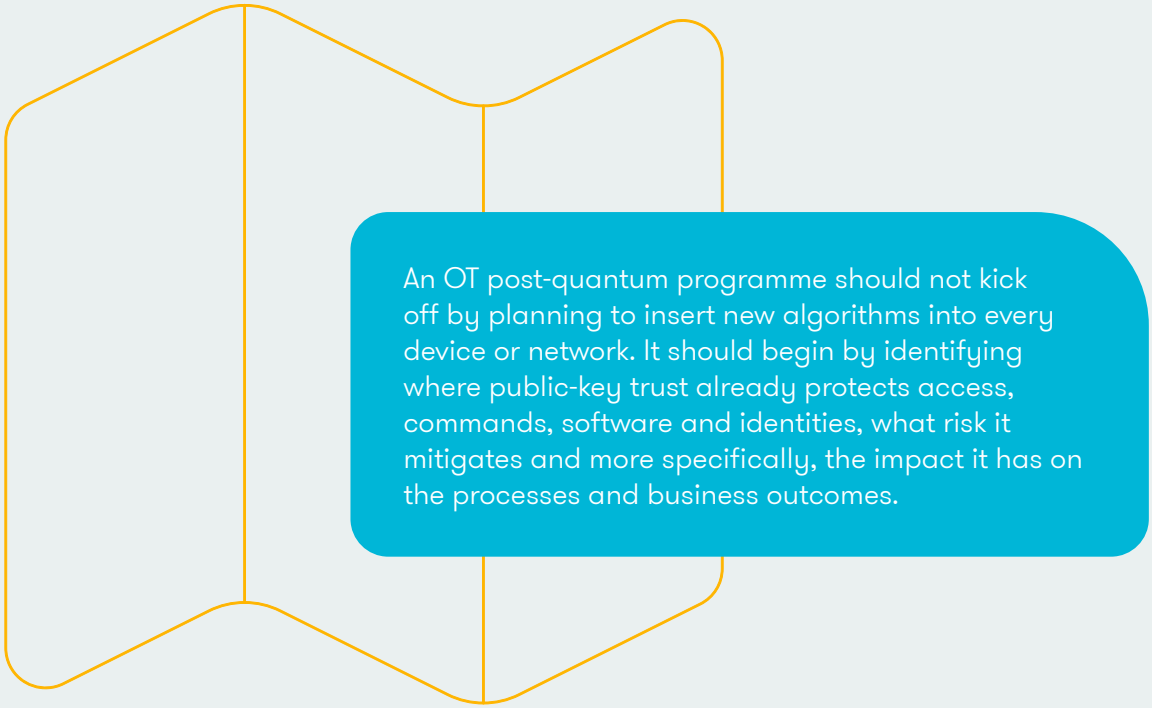
The Challenge is Different for OTs

Industrial systems often remain in service for decades. Their protocols, controllers, gateways and safety-certified applications change slowly or sometimes not at all. Maintenance windows are scarce, vendor dependencies are strong, and even a technically successful cryptographic upgrade can invalidate certification, cause unacceptable latency, packet fragmentation, processor load or failure behaviour.

Many field-level industrial protocols use little or no asymmetric cryptography, for good reason. Hence, there may be no cryptography inside a legacy bus-level protocol to replace to begin with. PQC does not correct that underlying lack of authentication or encryption.

In OT, the hardest post-quantum cryptography problem is time: assets last for decades, but trust mechanisms must change before they become vulnerable.

The main question is therefore not just whether OT should adopt post-quantum algorithms. It is where organisations should complete that transition and how they should do it without compromising availability, operation or safety. As there are plenty of different cases where OT is being deployed, from a centralised nuclear energy production site to a mobile machine, the factors to take into consideration for the PQC migration plan will be very different for each case as well.



An OT post-quantum programme should not kick off by planning to insert new algorithms into every device or network. It should begin by identifying where public-key trust already protects access, commands, software and identities, what risk it mitigates and more specifically, the impact it has on the processes and business outcomes.

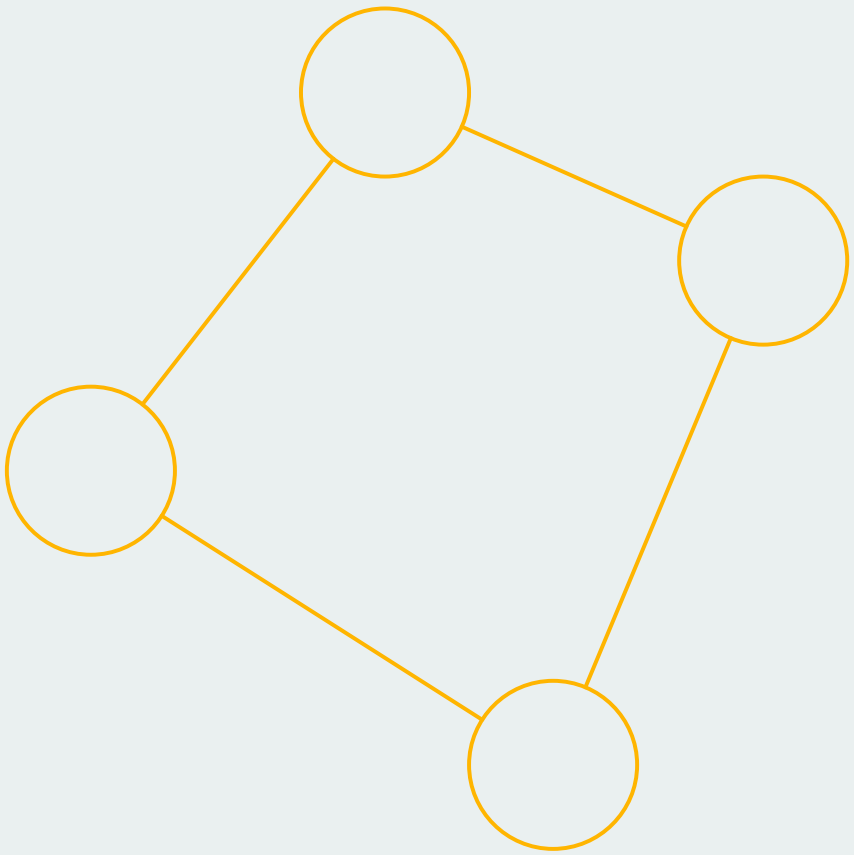
03

The Priority is the Boundary

The most exposed, and most repeatable, post-quantum use cases sit where trust crosses a trust boundary: remote operator and vendor access, plant-to-grid, utility or control-centre communications, device, server and user certificates, firmware, software and controller-logic signing.

These boundaries concentrate cryptographic dependencies and are usually more upgradeable than embedded controllers. A VPN concentrator, access broker or protocol-security gateway can often adopt a hybrid classical and post-quantum mode more flexibly. But even there, you should progress in steps: start with key establishment, expect signatures and PKI to lag as they are more complex and will take more effort to change.

That trust boundary is also the area where a failure has the greatest reach. If an attacker can forge a remote-access identity, impersonate a trusted gateway or defeat a shared certificate authority, the attacker may enter through an approved channel and then use legitimate engineering tools because most security tools are focussed on defending the perimeter and most often, a legitimate-looking entry goes unnoticed. If a signing mechanism fails, malicious firmware or controller logic may appear authentic. If a central OEM platform or trust root is shared across sites, one cryptographic weakness can create a fleet-wide problem. This is greatly increasing the existing risk of supply chain attacks, because it adds a new exploitation path.



04

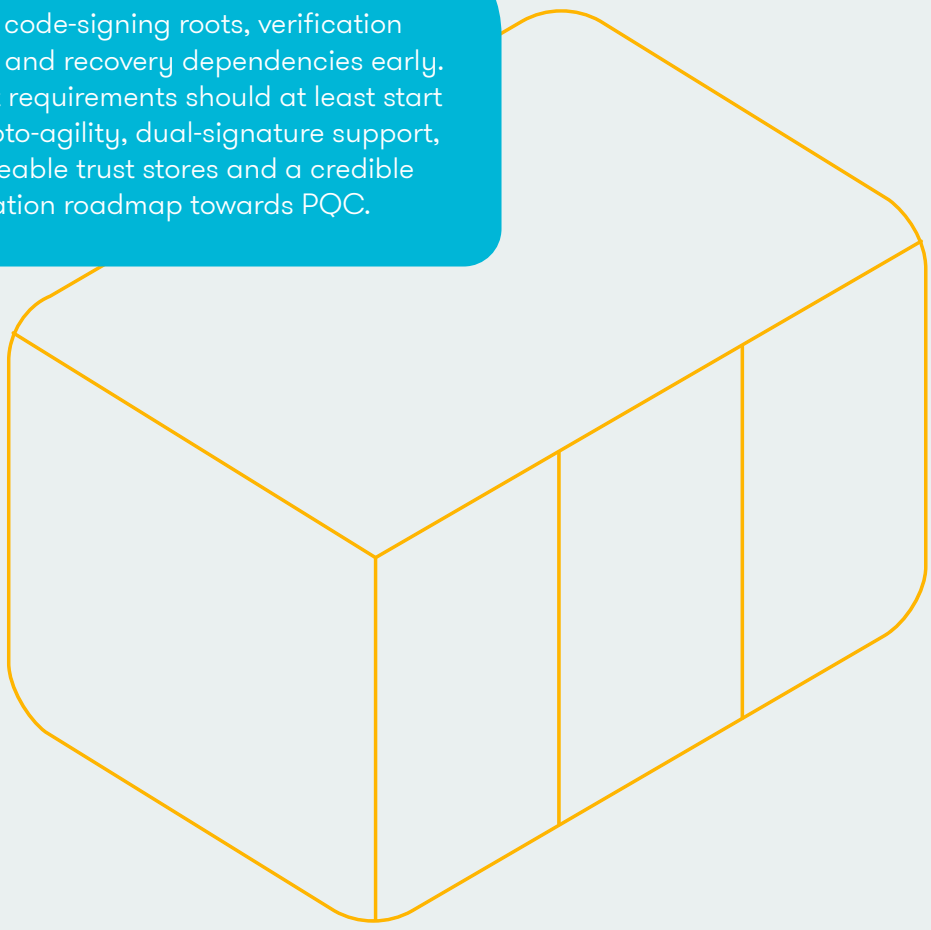
Firmware Signing Deserves Attention

Confidentiality discussions often dominate quantum-security messaging, but authenticity can be more consequential in OT. Asset owners must ensure that firmware, controller logic, configuration packages, recovery images and trust-store updates are genuine from the supplying party and are unmodified.

A firmware signature may need to remain trustworthy for much longer than a remote session needs to remain confidential. Some controllers rarely receive trust-store updates and may continue accepting the same signing root for years to decades.

Replacing that root can require vendor support, regression testing, a planned outage and, in some cases, physical access to a remote or unmanned site. As the Cyber Resilience Act (CRA) requires security updates to be provided by the manufacturer over the full support period, the signing-root migration must fit inside that window, so this process will gain importance in the future as well.

OT owners should therefore start inventorying code-signing roots, verification mechanisms and recovery dependencies early. Procurement requirements should at least start to cover crypto-agility, dual-signature support, field-upgradeable trust stores and a credible vendor migration roadmap towards PQC.



05

Availability and Safety Determine the Priorities

Post-quantum algorithms are not always drop-in replacements. Keys, ciphertexts, certificates and signatures can be substantially larger than their classical equivalents, which might cause the devices to struggle against hardware limitations. Temporary hybrid modes add further overhead because they combine classical and post-quantum mechanisms during the transition.

In a typical office environment, this may just result in a slower handshake or a software compatibility issue. In OT, it can cause packet fragmentation, higher memory load, timeout or watchdog activation…

The correct migration question is therefore not "Did the session handshake still succeed?" It is "Does the complete system remain safe and available during normal operation, degraded communications, failover, certificate expiry, revocation, loss of WAN connectivity and rollback?"

Safety functions, local operating limits and independent process protections must not depend on a single remote identity or certificate hierarchy. A site should retain safe local operation when its WAN connection, vendor platform or PKI becomes unavailable or untrustworthy. In that case, critical safety procedures such as graceful shutdowns or other must still be able to execute without any problems.

A successful cryptographic handshake is not a successful OT migration. The complete system must remain safe and available through failure, recovery and rollback.

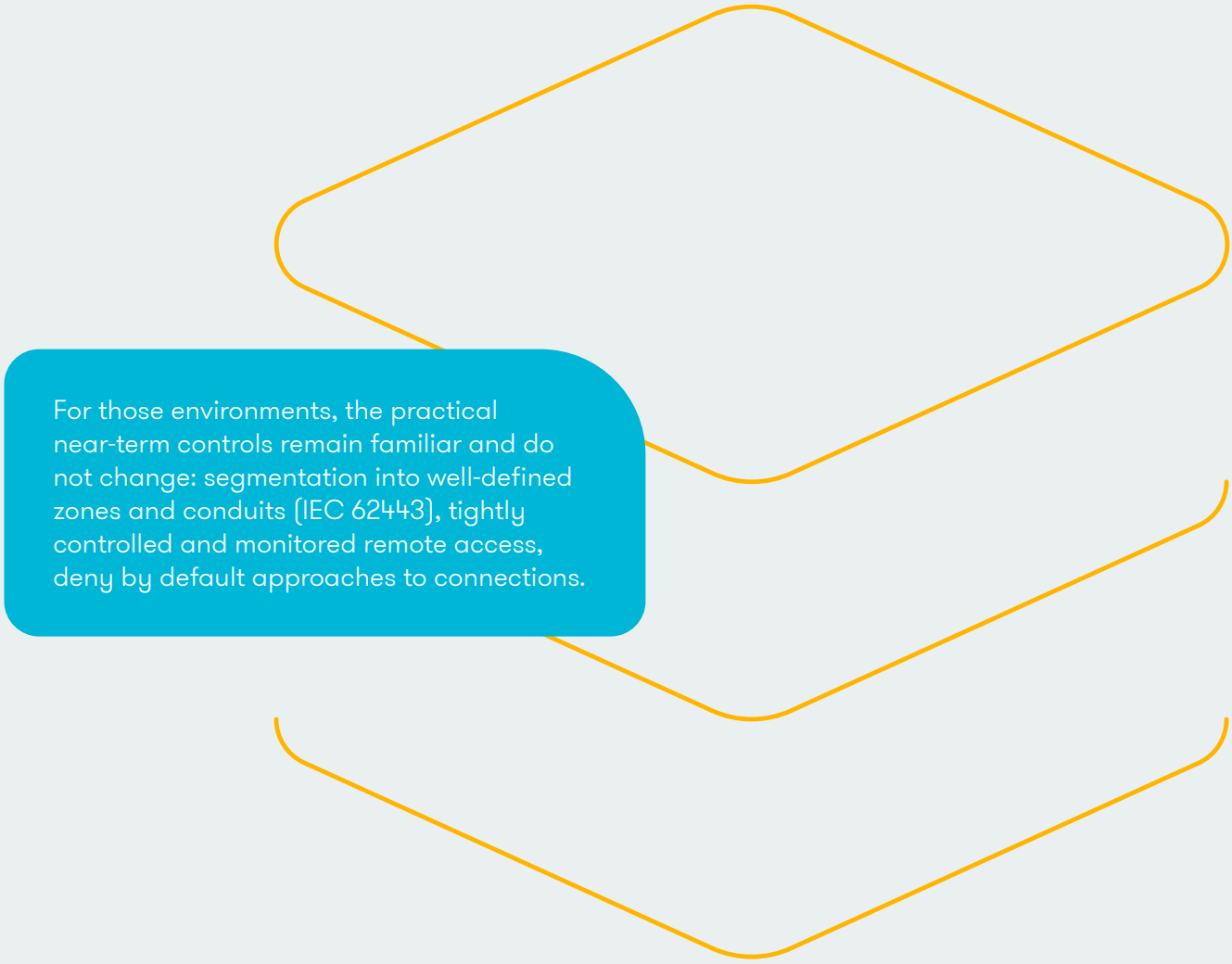
06

The Deepest Layers Will Go Last... or Not At All

Many internal industrial protocols — such as legacy Modbus, Modbus TCP, PROFIBUS, PROFINET, CAN or proprietary real-time buses — have no native encryption or strong peer authentication. Post-quantum cryptography does not fix that baseline. Attempting to add large signatures or complex handshakes directly to control paths may create more risk than it gains security benefit.

For reference: A PQC(ML-DSA-65) signature is about 3.3 KB , compared with 64 bytes for an ECDSA P-256 signature. A PQC certificate chain easily exceeds a 1500-byte MTU.

Gateways can buy time. They allow organisations to introduce post-quantum or hybrid protection around a legacy zone while its embedded assets follow a safe replacement cycle. They do not make insecure internal protocols secure, but they reduce exposure and constrain how compromise can propagate.



For those environments, the practical near-term controls remain familiar and do not change: segmentation into well-defined zones and conduits (IEC 62443), tightly controlled and monitored remote access, deny by default approaches to connections.

07

The Real Programme is Cryptographic Lifecycle Management

A “normal” asset inventory, already very difficult to create and maintain, is not enough. Organisations need to know, at a minimum, which algorithms, certificates, trust anchors and signing mechanisms support each operational function.

A basic cryptographic inventory contains:

* protocol and cryptographic mechanism;
* algorithm, key size and certificate chain;
* data or signature validity lifetime;
* supplier and operational owner.

Post-quantum readiness starts where trust enters the environment — not with a rushed retrofit of every device.

Additional fields can be added in an iterative manner as the inventory matures:

* the business, safety or operational purpose;
* key and trust-anchor location;
* software or firmware library;
* update and recovery route;
* support and replacement dates;
* dependencies on external operators or service providers.



Organise a cryptographic inventory around conduits and use cases, not only devices. Remote maintenance, monitoring, grid control, software updates and disaster recovery each have different consequences and migration constraints.

What To Do About It

A risk-based OT transition can follow five steps:

01

Secure the exposed perimeter first

This can be the site perimeter, the crossover between IT and OT, links to other OT sites,… Everywhere a trust boundary is crossed: remove obsolete cryptography, strengthen remote access, require independent multifactor authentication and demand post-quantum or hybrid roadmaps, or even better: a working integration, from VPN, firewall and access-broker suppliers.

02

Build requirements into refresh cycles

Make crypto-agility, field-upgradeability, algorithm diversity and signed-update support mandatory procurement criteria. Assets purchased now may still operate when classical public-key algorithms are deprecated.

03

Map signing and trust roots

Identify firmware, secure-boot, controller-logic and recovery-signing dependencies. Assess how trust stores can be updated and how long signatures must remain valid.

04

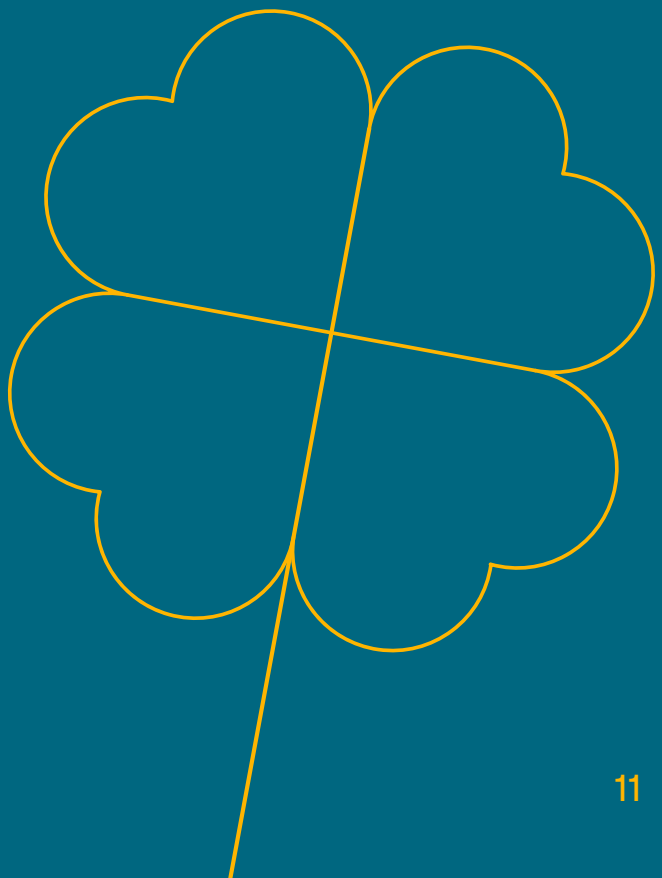
Coordinate external conduits

Align migration plans with OEMs, utilities, grid operators, telecom providers and managed service providers. One party cannot unilaterally change a shared protocol or certificate profile. Both parties will have to coordinate a protocol or algorithm switch.

05

Pilot at upgradeable gateways

Test hybrid key establishment and new certificate chains at boundaries before touching control networks. Include failure, recovery and rollback scenarios.



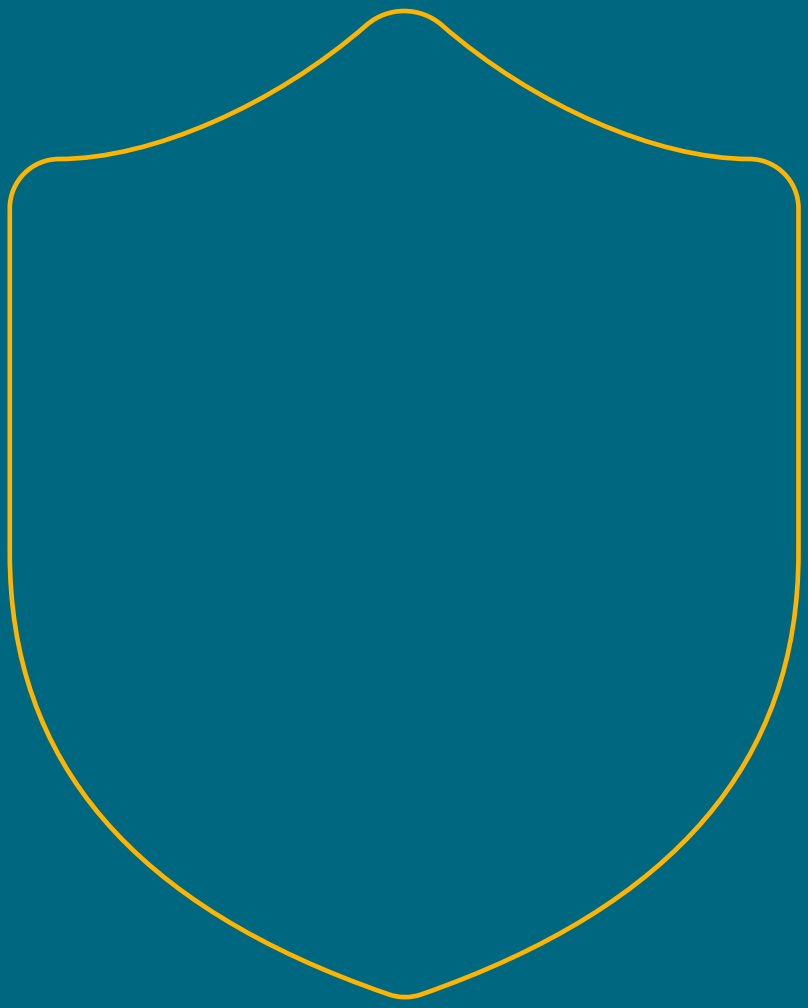


The Central Lesson

For most OT environments, post-quantum risk is not primarily a race to protect every process from future decryption. Some engineering data, credentials and long-lived records do require confidentiality, and organisations should assess their secrecy lifetime. But the larger operational challenge is migrating authentication, signing and key-establishment mechanisms across infrastructure that changes slowly and cannot tolerate disruption.

The transition should therefore start at the exposed ends of the environment: remote connections, connections between sites, monitoring platforms, external control links, certificates, software updates and firmware signatures. Embedded control systems should follow through carefully tested, vendor-supported lifecycle replacement — not through rushed cryptographic retrofits.

In OT, post-quantum readiness ultimately means preserving trustworthy commands, identities and software while keeping the process available and safe.



Publication Date

November 2026

Authors

Vincent Haerinck
Sarah Ampe
Dieter Sarrazyn
Johan Kestens

Contact

Cyber Security Coalition

Koning Albert II Laan 4
4 Boulevard Roi Albert II
1000 Brussels

info@cybersecuritycoalition.be
www.cybersecuritycoalition.be

CYBER SECURITY
COALITION