Embedding PQC in Supply Chain Security

Gareth T. Davies

EU PQC Conference
Den Haag
December 2025

Embedded Devices: the Security Anchor for Thousands of Industries

Factory Automation

Real-time control

HMI

Robotics

Healthcare

Monitoring/Diagnostics

Personal health

Medical imaging

Power and Energy

Energy management

Green energy

Electrification

Home & Building Automation

Building & home control

Smart access

Smart appliances

Automotive

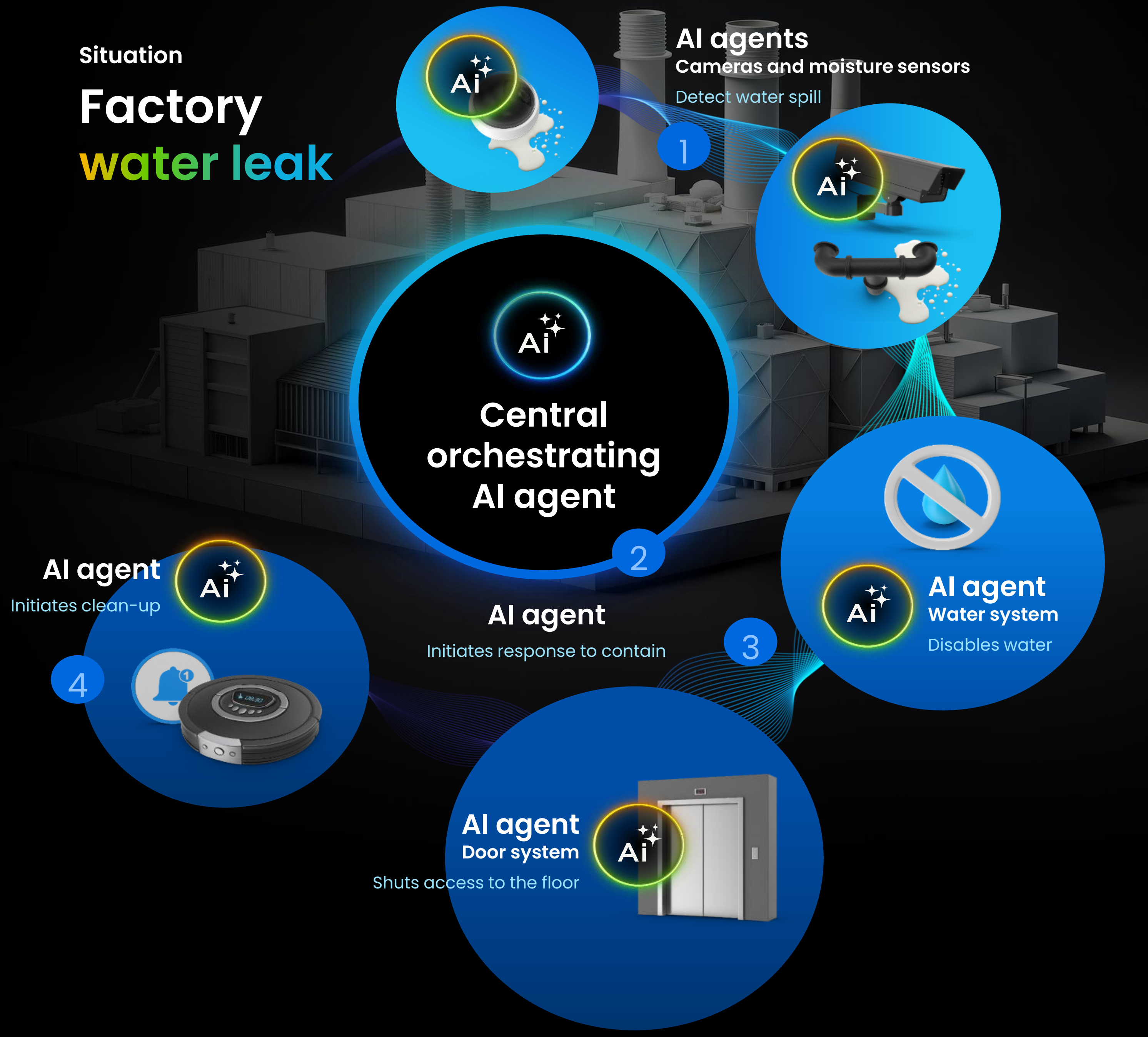
SDVs & Zonal Architecture

ADAS / Autonomy

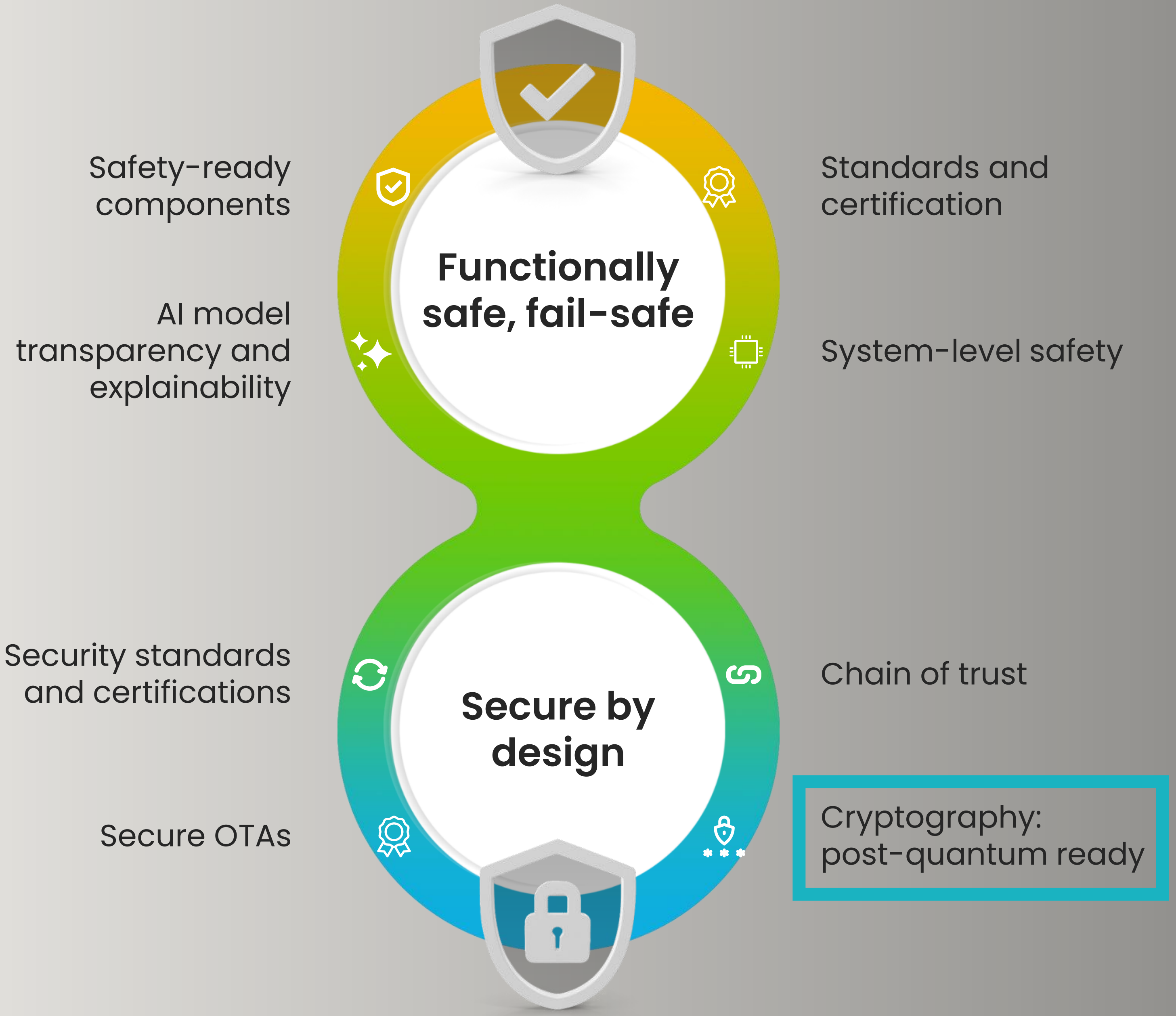
Electrification

An autonomous future is becoming a new reality

Edge agentic AI system in action



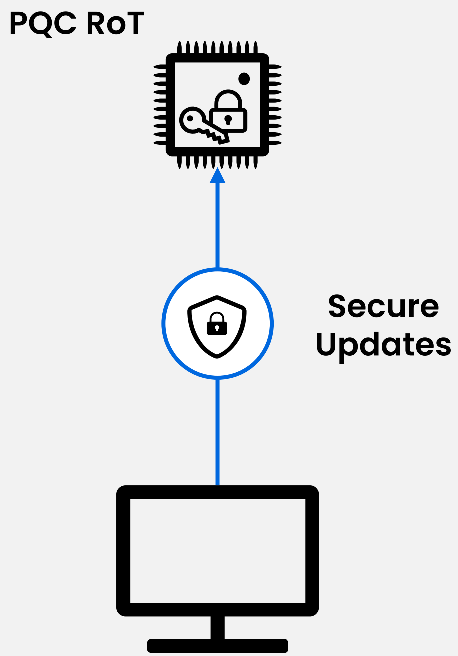
Safety and security



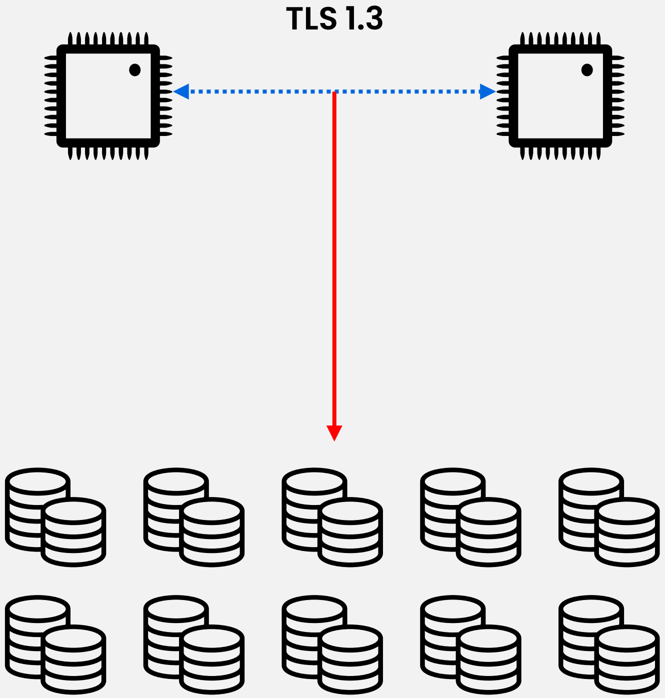
What drives migration to Post-Quantum Cryptography?

Standards & Compliance

Trust Anchor / Hardware



Store Now Decrypt Later



PQC Algorithms in Typical Embedded Use Cases

Many more ongoing and upcoming!

		FIPS 203 ML-KEM	FIPS 204 ML-DSA	FIPS 205 (Verify) SLH-DSA	SP 800-208 (Verify) XMSS / LMS
Security Goals	Secure Boot	✗	✓	✓	✓
	Secure Update	✓	✓	✓	✓
	Secure Attestation	✗	✓	✗	✗
	Secure Debug / Test	✓	✓	✗	✗
	Certificates (PKI)	✗	✓	✓	✓**
	Runtime Crypto API	✓	✓	✓	✓
Protocols	TLS 1.3 (Hybrid)	✓	✓*	✗	✗
	IKEv2 (Hybrid)	✓	✓*	✗	✗
	GSMA eSIM	✓	✓	✗	✗
	GlobalPlatform: TEE/MCU	✓	✓	✓	✓

** Signatures for client authentication excluded from initial proposals, discussions ongoing*
*** Possible but the number of issued certificates should be carefully managed (e.g., Root CA)*

Challenges in Migrating Devices to PQC

Devices can get FW/SW updates, but not more HW acceleration

➔ Restrictiveness of CNSA 2.0 is useful

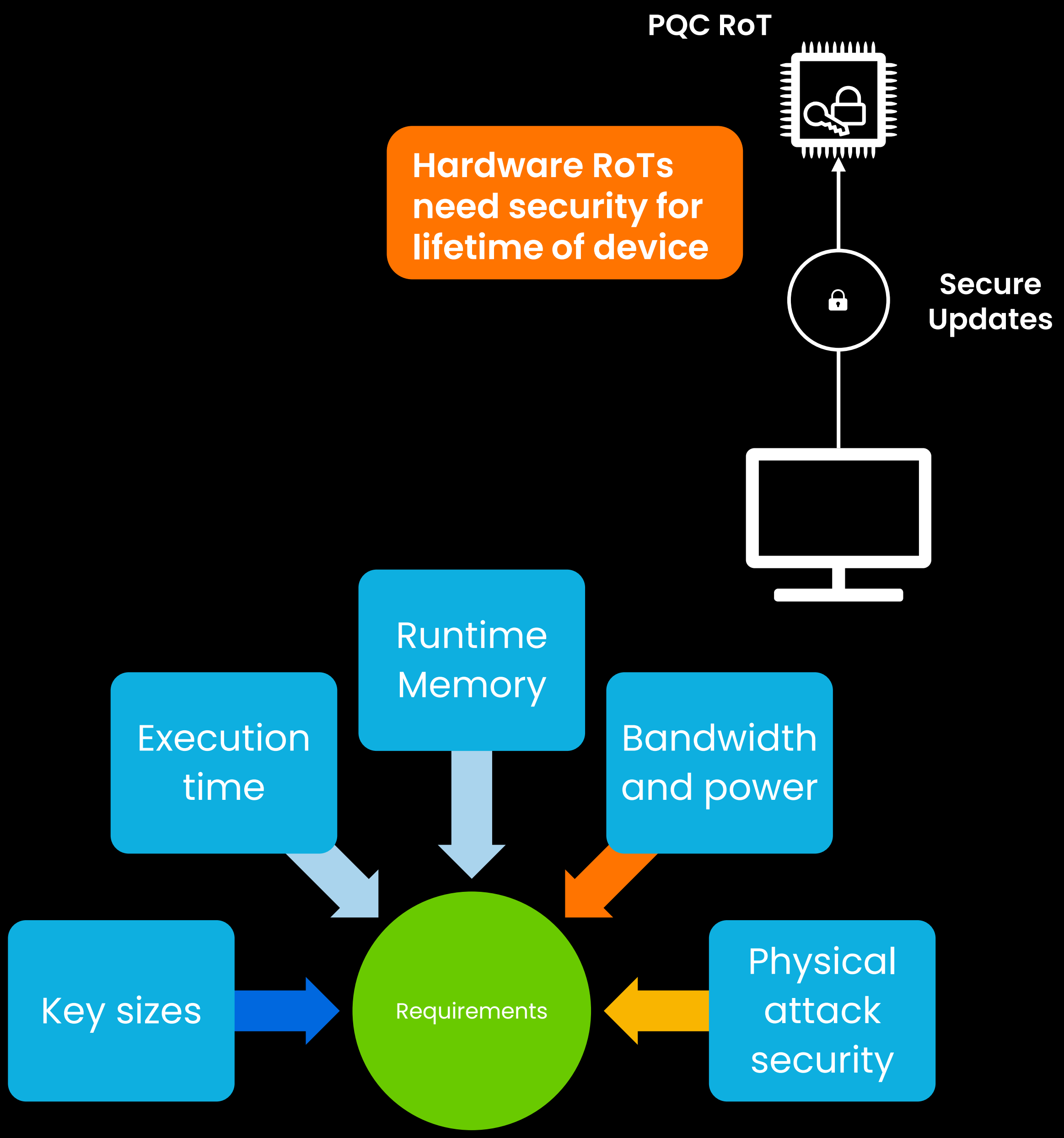
Many consequences for secure devices:

➔ Chip area for crypto acceleration limited

- unfortunate divergence in mathematical structure
- can't support everything

➔ Each mini-generation of chips could target different schemes for acceleration

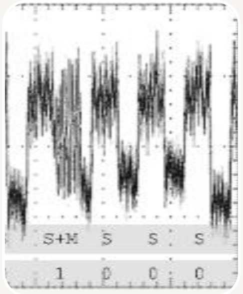
➔ Global certification landscape not static; progresses in sync with attack literature



Resistance against Physical & Logical Attacks

Hardening can be expensive but necessary

SCA-protected hashing ≈ 40% of runtime for ML-DSA
→ HW acceleration

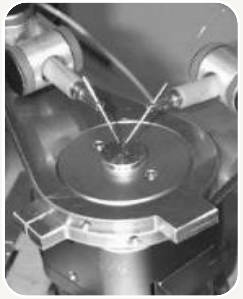


Side-channel attacks

- Power analysis (SPA, DPA)
- Electromagnetic analysis (SEMA, DEMA)
- Timing Analysis
- Photo-emission microscopy (high-end)
- Profiled, unprofiled and ML-assisted variants

Fault injection attacks

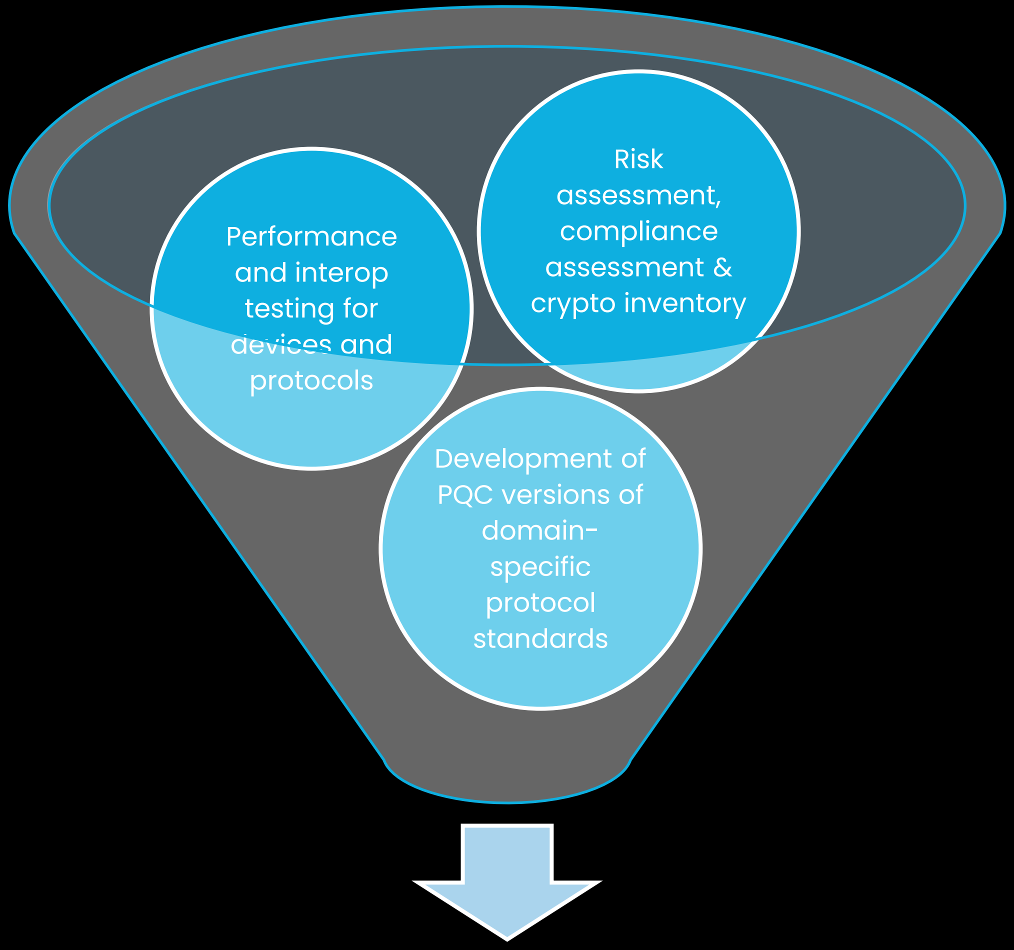
- Voltage or clock glitching
- Electromagnetic fault injection (EMFI)
- Body bias injection
- Laser fault injection
- Single and multi-shot scenarios



Invasive attack

- Focused Ion Beam (FIB) modifications
- Micro/Nano-probing of internal signals
- Signal forcing
- Delayering
- Reverse-engineering

Challenges in migrating Infrastructure & Supply Chains to PQC



Migration Readiness?
More likely: a new set of action points

Increased urgency for PKI migration plan

Device lifecycle plan adjustment

Adjustment of protocol flows or data packet sizes

More advanced mitigation plan for future threats (including: what to do when the QC announced)

Outlook

- Not just HNDL → Signature use cases just as urgent
- Many implementation challenges, hardware acceleration will develop over time
- Size (/memory) is often a bigger issue than speed
- Physical attack resilience is essential; for PQC side-channels are a fast-moving target
- Hybrid crypto increases user/customer confidence

Get in touch

Gareth T. Davies
garethhomas.davies@nxp.com

nxp.com

nxp.com