Securing EV Charging Infrastructure: A QNX- Based Approach for High-Assurance Systems

Abstract

As electric vehicle (EV) adoption accelerates globally, charging infrastructure has emerged as a mission-critical cyber-physical asset. Modern Electric Vehicle Supply Equipment (EVSE) is highly connected, integrating with vehicles, cloud backends, payment systems, and the electrical grid for bidirectional power transfer and demand response.

This connectivity significantly expands the attack surface, with potential consequences ranging from billing fraud to power grid disruption. While most EVSE systems rely on general- purpose Linux platforms, this whitepaper evaluates QNX Neutrino RTOS, a real-time, microkernel-based operating system, as a high-assurance alternative.

This paper attempts to analyse its security architecture, post-quantum readiness, and compliance capabilities, presenting an in-depth system model tailored for OCPP 2.1, ISO 15118-20, and safety-critical EVSE deployments compliant with IEC 62443 and EU AFIR standards.

1. Introduction

EVSE has evolved beyond a simple electrical switch into an intelligent, connected computing node at the edge of the energy network. It manages critical functions, including:

- OCPP 2.1 sessions with Charge Station Management Systems (CSMS) for Vehicle-to- Everything (V2X) and Distributed Energy Resource (DER) control.
- ISO 15118-20 / Plug-and-Charge (PnC) communication with vehicles.
- Grid-side integration for load balancing, demand response, and bidirectional charging (V2G/V2H).
- Payment processing, over-the-air (OTA) updates, and fleet management APIs.

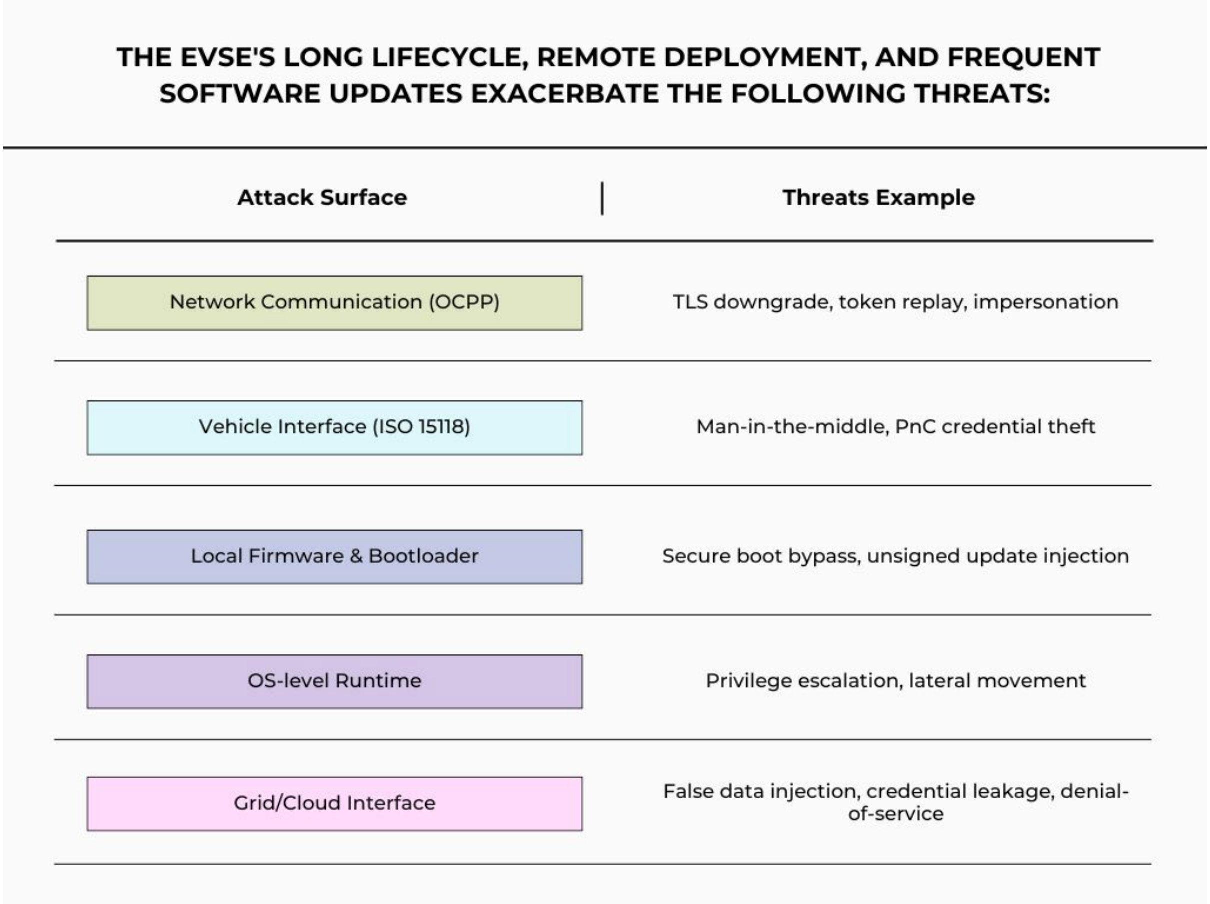
This multi-role operation exposes EVSE to diverse and sophisticated cyber threats. Linux- based systems, while cost-effective, introduce a large attack surface requiring extensive hardening. In contrast, QNX offers:

- Microkernel isolation.
- Deterministic real-time performance.

- Safety and security certifications (e.g., IEC 62443-4-2).
- Built-in support for fine-grained privilege control.

2. Threat landscape

The EVSE's long lifecycle, remote deployment, and frequent software updates exacerbate the following threats:

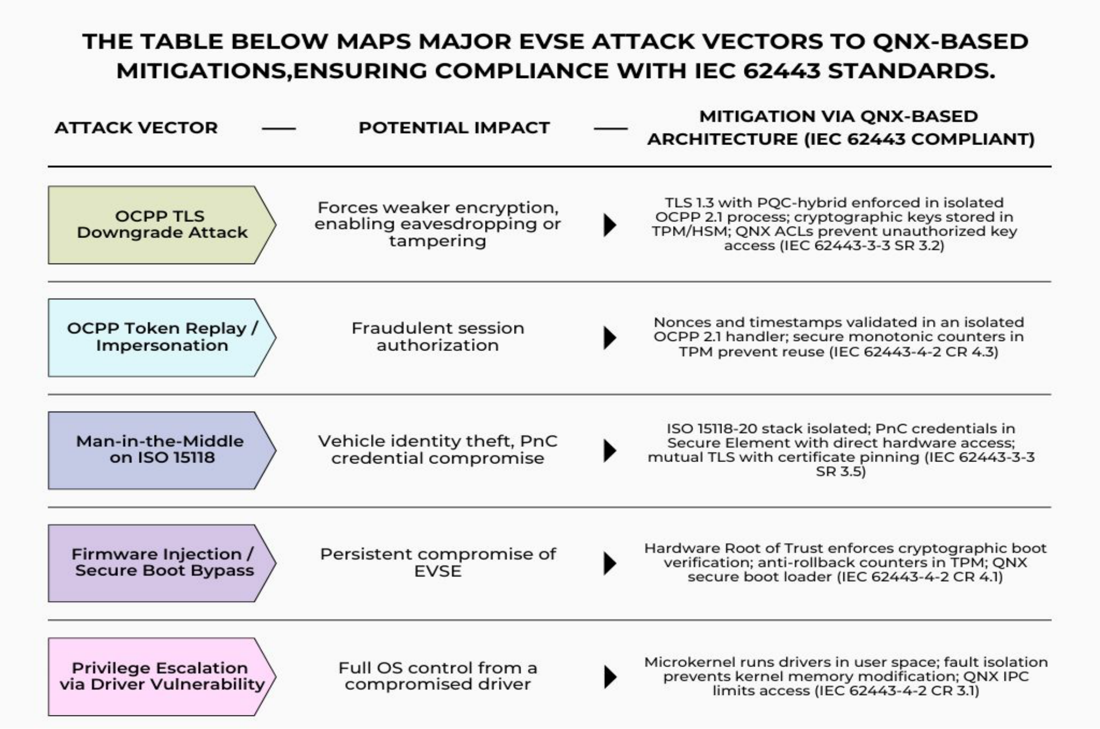


THE EVSE'S LONG LIFECYCLE, REMOTE DEPLOYMENT, AND FREQUENT SOFTWARE UPDATES EXACERBATE THE FOLLOWING THREATS:

Attack Surface	Threats Example
Network Communication (OCPP)	TLS downgrade, token replay, impersonation
Vehicle Interface (ISO 15118)	Man-in-the-middle, PnC credential theft
Local Firmware & Bootloader	Secure boot bypass, unsigned update injection
OS-level Runtime	Privilege escalation, lateral movement
Grid/Cloud Interface	False data injection, credential leakage, denial-of-service

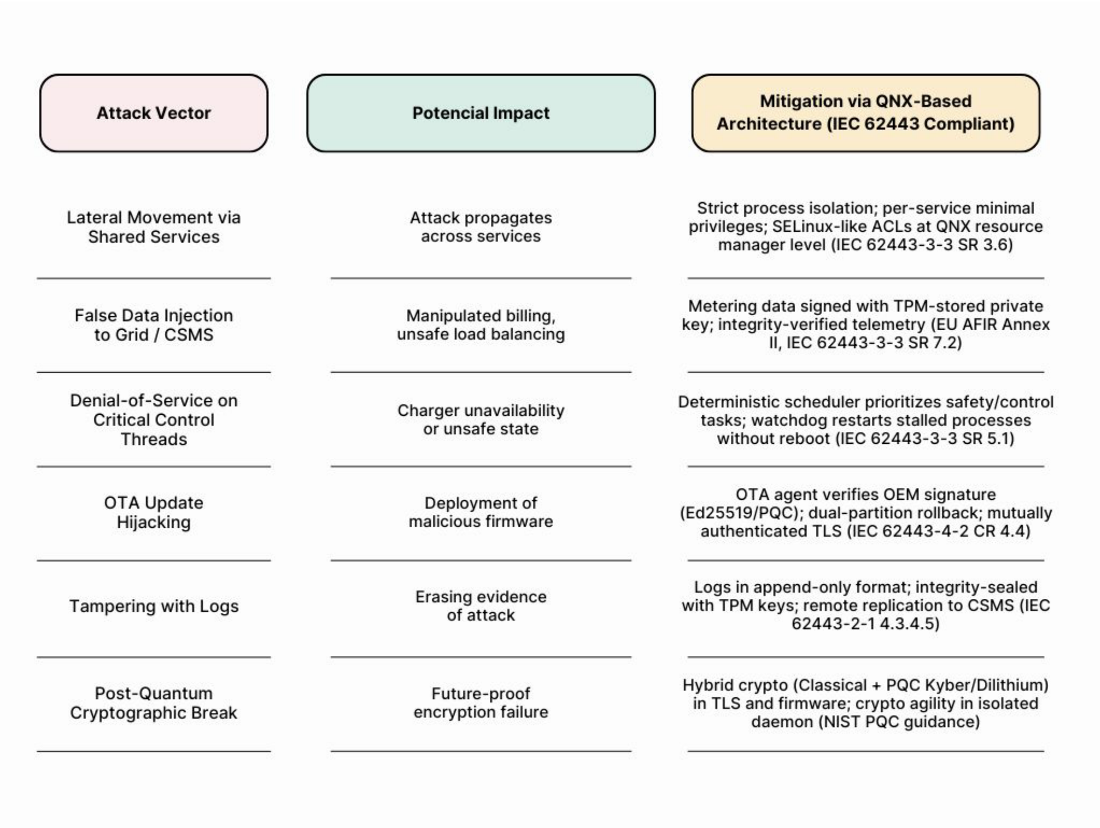
3. Security Assurance

The table below maps major EVSE attack vectors to QNX-based mitigations, ensuring compliance with IEC 62443 standards.



THE TABLE BELOW MAPS MAJOR EVSE ATTACK VECTORS TO QNX-BASED MITIGATIONS,ENSURING COMPLIANCE WITH IEC 62443 STANDARDS.

ATTACK VECTOR	POTENTIAL IMPACT	MITIGATION VIA QNX-BASED ARCHITECTURE (IEC 62443 COMPLIANT)
OCPP TLS Downgrade Attack	Forces weaker encryption, enabling eavesdropping or tampering	TLS 1.3 with PQC-hybrid enforced in isolated OCPP 2.1 process; cryptographic keys stored in TPM/HSM; QNX ACLs prevent unauthorized key access (IEC 62443-3-3 SR 3.2)
OCPP Token Replay / Impersonation	Fraudulent session authorization	Nonces and timestamps validated in an isolated OCPP 2.1 handler; secure monotonic counters in TPM prevent reuse (IEC 62443-4-2 CR 4.3)
Man-in-the-Middle on ISO 15118	Vehicle identity theft, PnC credential compromise	ISO 15118-20 stack isolated; PnC credentials in Secure Element with direct hardware access; mutual TLS with certificate pinning (IEC 62443-3-3 SR 3.5)
Firmware Injection / Secure Boot Bypass	Persistent compromise of EVSE	Hardware Root of Trust enforces cryptographic boot verification; anti-rollback counters in TPM; QNX secure boot loader (IEC 62443-4-2 CR 4.1)
Privilege Escalation via Driver Vulnerability	Full OS control from a compromised driver	Microkernel runs drivers in user space; fault isolation prevents kernel memory modification; QNX IPC limits access (IEC 62443-4-2 CR 3.1)



Attack Vector	Potencial Impact	Mitigation via QNX-Based Architecture (IEC 62443 Compliant)
Lateral Movement via Shared Services	Attack propagates across services	Strict process isolation; per-service minimal privileges; SELinux-like ACLs at QNX resource manager level (IEC 62443-3-3 SR 3.6)
False Data Injection to Grid / CSMS	Manipulated billing, unsafe load balancing	Metering data signed with TPM-stored private key; integrity-verified telemetry (EU AFIR Annex II, IEC 62443-3-3 SR 7.2)
Denial-of-Service on Critical Control Threads	Charger unavailability or unsafe state	Deterministic scheduler prioritizes safety/control tasks; watchdog restarts stalled processes without reboot (IEC 62443-3-3 SR 5.1)
OTA Update Hijacking	Deployment of malicious firmware	OTA agent verifies OEM signature (Ed25519/PQC); dual-partition rollback; mutually authenticated TLS (IEC 62443-4-2 CR 4.4)
Tampering with Logs	Erasing evidence of attack	Logs in append-only format; integrity-sealed with TPM keys; remote replication to CSMS (IEC 62443-2-1 4.3.4.5)
Post-Quantum Cryptographic Break	Future-proof encryption failure	Hybrid crypto (Classical + PQC Kyber/Dilithium) in TLS and firmware; crypto agility in isolated daemon (NIST PQC guidance)

4. QNX Microkernel: Security-Centric Design.

4.1 Microkernel Architecture

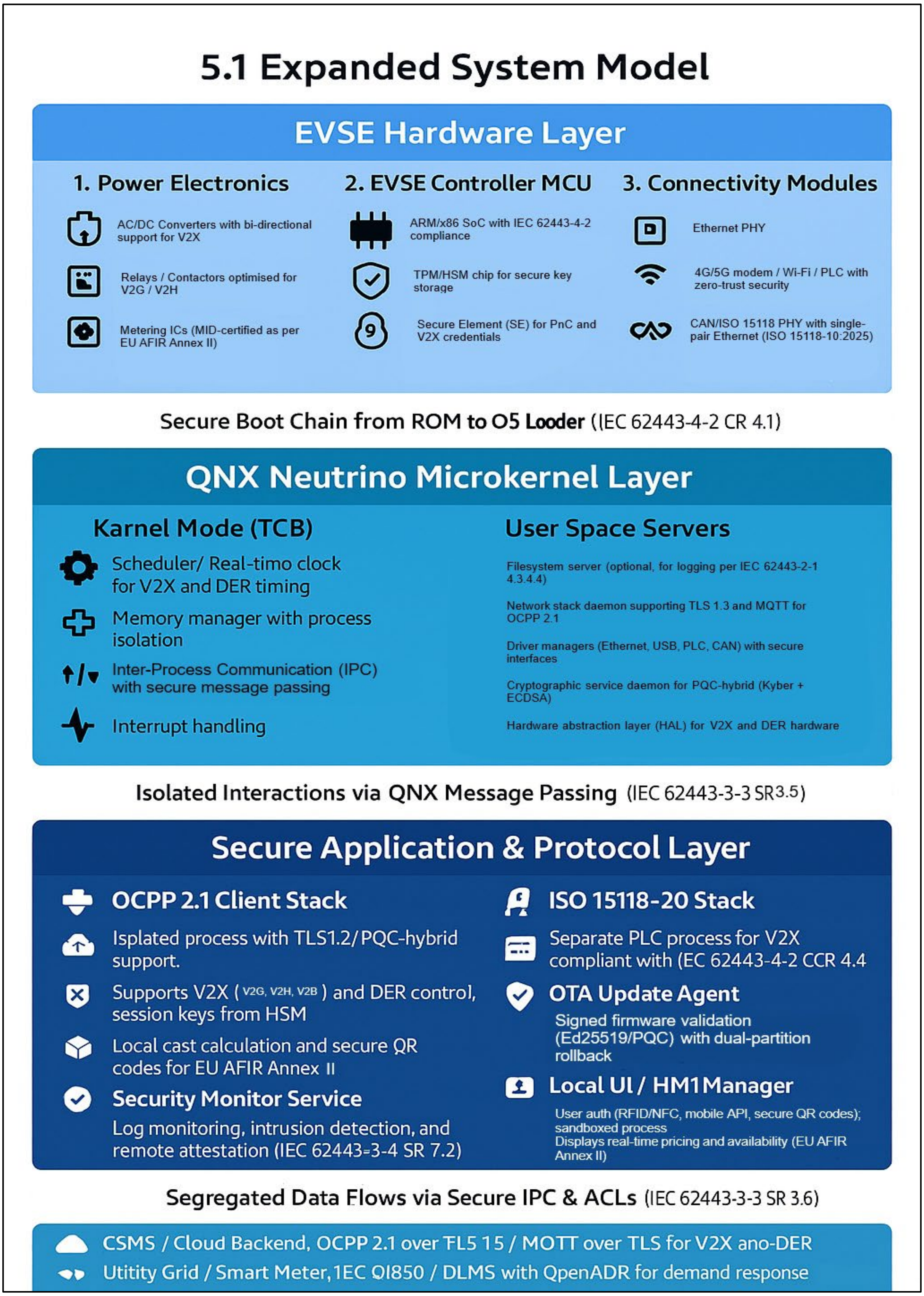
QNX employs a true microkernel architecture where only essential services (scheduler, IPC, memory manager) operate in kernel mode. All other services-drivers, network stack, filesystems, and applications-run in user space, offering:

- **Minimized TCB:** Reduced lines of critical code.
- **Fault Isolation:** A network driver crash does not affect the system.
- **Recovery Without Reboot:** Independent process restarts.

4.2 Process Isolation and IPC

- Each service (e.g., ISO 15118-20 stack, OCPP 2.1 stack, update manager) operates with least privilege.
- No shared memory; communication via QNX's secure message passing.
- Hardware access is controlled via fine-grained resource managers (IEC 62443-4-2 CR 3.1).

5. Deep-Dive: QNX-Based EVSE Security Architecture



5.1 Expanded System Model

EVSE Hardware Layer

1. Power Electronics

- AC/DC Converters with bi-directional support for V2X
- Relays / Contactors optimised for V2G / V2H
- Metering ICs (MID-certified as per EU AFIR Annex II)

2. EVSE Controller MCU

- ARM/x86 SoC with IEC 62443-4-2 compliance
- TPM/HSM chip for secure key storage
- Secure Element (SE) for PnC and V2X credentials

3. Connectivity Modules

- Ethernet PHY
- 4G/5G modem / Wi-Fi / PLC with zero-trust security
- CAN/ISO 15118 PHY with single-pair Ethernet (ISO 15118-10:2025)

Secure Boot Chain from ROM to O5 Looder ((IEC 62443-4-2 CR 4.1)

QNX Neutrino Microkernel Layer

Karnel Mode (TCB)

- Scheduler/ Real-timo clock for V2X and DER timing
- Memory manager with process isolation
- Inter-Process Communication (IPC) with secure message passing
- Interrupt handling

User Space Servers

- Filesystem server (optional, for logging per IEC 62443-2-1 4.3.4.4)
- Network stack daemon supporting TLS 1.3 and MQTT for OCPP 2.1
- Driver managers (Ethernet, USB, PLC, CAN) with secure interfaces
- Cryptographic service daemon for PQC-hybrid (Kyber + ECDSA)
- Hardware abstraction layer (HAL) for V2X and DER hardware

Isolated Interactions via QNX Message Passing (IEC 62443-3-3 SR3.5)

Secure Application & Protocol Layer

OCPP 2.1 Client Stack

- Isplated process with TLS1.2/PQC-hybrid support.
- Supports V2X (V2G, V2H, V2B) and DER control, session keys from HSM
- Local cast calculation and secure QR codes for EU AFIR Annex II

Security Monitor Service

Log monitoring, intrusion detection, and remote attestation (IEC 62443=3-4 SR 7.2)

ISO 15118-20 Stack

Separate PLC process for V2X compliant with (EC 62443-4-2 CCR 4.4

OTA Update Agent

Signed firmware validation (Ed25519/PQC) with dual-partition rollback

Local UI / HM1Manager

User auth (RFID/NFC, mobile API, secure QR codes); sandboxed process
Displays real-time pricing and availability (EU AFIR Annex II)

Segregated Data Flows via Secure IPC & ACLs (IEC 62443-3-3 SR 3.6)

- CSMS / Cloud Backend, OCPP 2.1 over TL5 15 / MOTT over TLS for V2X ano-DER
- Utitity Grid / Smart Meter, 1EC Ql850 / DLMS with QpenADR for demand response

5.2 Trust Anchors & Security Zones

5.2.1 **Root of Trust (RoT):** TPM 2.0 or SE storing boot keys, TLS certs, PnC contracts, PQC keys (IEC 62443-4-2 CR 4.1).

5.2.2 **Zone 0:** Hardware trust (TPM, secure JTAG, anti-rollback).
5.2.3 **Zone 1:** QNX TCB.
5.2.4 **Zone 2:** Protocol handlers (OCPP 2.1, ISO 15118-20, payment).
5.2.5 **Zone 3:** Non-critical apps (HMI, telemetry).

5.3 Data Flow Example - OCPP 2.1 Session

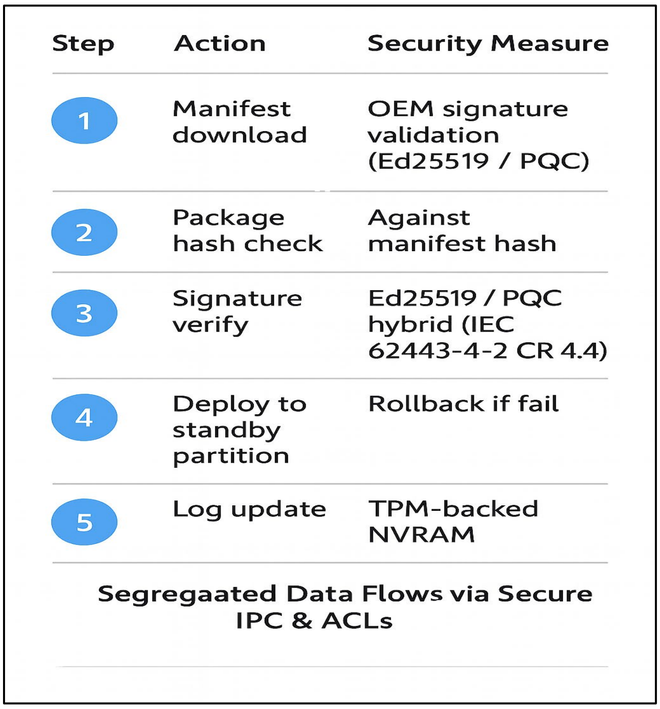
1. EV plugs in➔ ISO 15118-20 handshake.
2. PnC contract fetched from SE.
3. OCPP 2.1 TLS 1.3 session with CSMS using HSM keys+ attestation, supporting V2X/DER.
4. Meter/session data signed and sent to CSMS.
5. Payment confirmation stored in tamper-evident log (EU AFIR Annex 11).

5.4 Intrusion Detection & Runtime Integrity

5.4.1 **Watchdog:** Monitors process hashes, restarts compromised services without full reboot (IEC 62443-3-3 SR 5.1).

5.4.2 **Integrity Verification:** Merkle Tree for executables.
5.4.3 **Anomaly Detection:** Resource usage profiling with thresholds.

5.5 OTA Security Workflow



Step	Action	Security Measure
1	Manifest download	OEM signature validation (Ed25519 / PQC)
2	Package hash check	Against manifest hash
3	Signature verify	Ed25519 / PQC hybrid (IEC 62443-4-2 CR 4.4)
4	Deploy to standby partition	Rollback if fail
5	Log update	TPM-backed NVRAM

Segregaated Data Flows via Secure IPC & ACLs

6 Post-Quantum Security Readiness

As NIST finalises its Post-Quantum Cryptography (PQC) standards (e.g., Kyber for key encapsulation and Dilithium for digital signatures), EVSE operators face a long-term risk from quantum computers compromising stored credentials, firmware signing keys, and historical transaction records.

QNX's architecture supports PQC adoption with process isolation, crypto agility, and rollback-safe OTA updates, ensuring compliance with IEC 62443 and EU AFIR security requirements.

6.2 Hybrid Cryptography for TLS Sessions

Hybrid TLS combines ECDHE + AES-GCM with Kyber-1024, providing:

6.2.1 Immediate quantum resistance for session key establishment.
6.2.2 Backward compatibility with CSMS, grid, and payment infrastructure.
6.2.3 QNX runs PQC in a dedicated crypto daemon with TPM/SE key access, secure IPC, and no direct network exposure.

Example (OCPP 2.1 Handshake):

1. Classical ECDHE runs parallel with Kyber KEM.
2. Session key= KDF(ECDHE 11 Kyber), resistant to classical and quantum attacks.
3. Keys stored in secure element RAM until session teardown.

6.3 PQC-Signed Firmware Packages

6.3.1 **Dual Signature Model:** Ed25519 + Dilithium.
6.3.2 **Verification Pipeline:** Bootloader verifies both signatures; PQC verification in an isolated service; rollback on mismatch.

6.3.3 **Future-Proof:** Crypto daemon upgradable OTA for new PQC standards.

6.4 Crypto-Agile Daemon

6.4.1 Hot-swappable algorithms in user-space daemons.
6.4.2 Versioned crypto profiles for PQC test mode.
6.4.3 OTA updates support new PQC algorithms (e.g., BIKE, Falcon) and A/B validation.

6.5 Isolated PQC Testing & Rollback

6.5.1 Sandboxed PQC testing with no shared memory.
6.5.2 Test results logged to secure audit storage.
6.5.3 Rollback-safe OTA with fallback to classical crypto.

6.6 PQC Integration into EVSE Protocol Stacks

6.6.1 OCPP 2.1: Hybrid TLS for CSMS communications.
6.6.2 ISO 15118-20: PQC in PnC contract certificate verification.
6.6.3 Backend APIs: PQC in REST/MQTT authentication.
6.6.4 Payment Security: PQC-signed tokenization requests.

6.7 Operational Benefits

6.7.1 Future-proof security per N1ST 2030+ guidance.
6.7.2 No forklift upgrades; PQC modules integrate into existing QNX systems.
6.7.3 Resilient deployment with algorithm swaps without affecting safety-critical layers.

7 Limitations & Considerations

- **Cost:** Licensing per unit vs. free Linux.
- **Developer Onboarding:** Smaller ecosystem.
- **Tooling:** Limited open-source support.
- **Vendor Lock-In:** Depends on QNX distribution policies.

8 Conclusion

The QNX Neutrino RTOS delivers a robust and future-ready foundation for securing EVSE infrastructure, underpinned by its advanced microkernel architecture, rigorous process isolation, and deterministic real-time scheduling.

This architecture not only ensures comprehensive runtime verification and fault tolerance but also aligns seamlessly with stringent international standards, including IEC 62443 for industrial cybersecurity, EU AFIR for smart charging and interoperability, and OCPP 2.1 for enabling Vehicle-to-Everything (V2X) and Distributed Energy Resource (DER) functionalities.

By integrating post-quantum cryptography and rollback-safe OTA updates, QNX provides a resilient defence against evolving cyber threats, positioning it as a superior alternative to traditional Linux-based systems. For mission-critical deployments such as bidirectional

DC fast chargers, fleet depots, and intelligent grid nodes, QNX offers a scalable, compliant, and sustainable solution that supports the global transition to a secure and efficient EV ecosystem.

Acknowledgements

We acknowledge contributions from cybersecurity, embedded systems, and electric mobility communities, aligning with ISO 15118-20, OCPP 2.1, ISO 21434, IEC 62443, and EU AFIR standards. This paper is independent and not influenced by QNX or BlackBerry. The author of this paper was an employee with the BlackBerry APAC team.

Special thanks to teams advancing secure RTOS and EVSE compliance.

Next Steps

- Benchmark QNX vs. embedded Linux in EVSE deployments.
- Implement PQC hybrid handshake on QNX.
- Develop a formal threat model for IEC 62443 and EU AFIR certification.
- Welcome feedback for field testing.

1. Glossary of Acronyms & Terms

Acronym	Definition
EVSE	Electric Vehicle Supply Equipment
PnC	Plug and Charge (ISO 15118-20)
OCPP	Open Charge Point Protocol
RTOS	Real-Time Operating System
TCB	Trusted Computing Base
HSM	Hardware Security Module
RoT	Root of Trust
V2X	Vehicle-to-Everything
DER	Distributed Energy Resource

2. References

- NIST PQC Round 3 Report - https://csrc.nist.gov/publications/detail/nistir/8309/final
- ISO 21434:2021 - Road vehicles - Cybersecurity engineering
- ISO 15118-20:2022 - Vehicle to Grid Communication Interface
- OCPP 2.1 Specification - Open Charge Alliance
- IEC 62443 Series - Industrial Automation and Control Systems Security
- EU AFIR Regulation - Alternative Fuels Infrastructure Regulation
- BlackBerry QNX Certification Data Sheets

3. Limitations & Future Work

This whitepaper reflects a technical architecture and security model for quantum-secure Electric Vehicle Supply Equipment (EVSE) using QNX Neutrino RTOS. The concepts, mitigations, and protocol enhancements discussed are based on current standards (e.g., IEC 62443, ISO 15118-20, OCPP 2.1, EU AFIR) and incorporate best-effort security design using post-quantum cryptography (PQC).

Real-world implementation may require adaptation, validation, performance profiling, and certification audits.

The design has not yet undergone full-scale field validation, and results may vary in practical deployments. Readers are encouraged to adapt the ideas to their specific environments and conduct appropriate testing.

Feedback and collaboration are welcome to help improve and operationalise this work.

All product names, logos, and trademarks referenced remain the property of their respective owners. No commercial endorsement is implied.

4. Author's Contact Information

For technical correspondence or collaboration inquiries, please contact:

Sumit Chouhan (TMIET) Sumit Chouhan

- Email: insanemechanic@proton.me
- Website: www.sumitchouhan.com