

Quantum Safe SCADA Encryptor

Serial Communications



Rising Threats to OT Infrastructure

Critical infrastructure operators continue to rely on legacy SCADA serial communication networks to manage power grids, water treatment plants, oil & gas pipelines, transportation systems and industrial facilities. These operational environments were engineered for reliability and availability, not cybersecurity.

As IT and OT environments become increasingly interconnected, previously isolated serial communications are now exposed to sophisticated cyber attacks, insider threats and emerging quantum computing risks. Replacing existing SCADA infrastructure is expensive, operationally disruptive and often impractical.

Organisations require a solution that secures existing operational technology while preserving system availability, deterministic communications and long operational lifecycles.

Securing Operational Networks

The Quantum Safe SCADA Encryptor transparently encrypts serial communications between control centres and remote terminal units (RTUs), protecting mission critical operational traffic without modifying existing SCADA applications or field equipment.

Built for operational technology environments, the solution combines Post-Quantum Cryptography (PQC) with Quantum Key Distribution (QKD) interoperability, enabling organisations to protect today's infrastructure while preparing for the quantum era.

Designed for seamless deployment, the encryptor preserves existing operational workflows while providing trusted, end to end protection across legacy serial communication links.

Built for Critical Infrastructure

Quantum Safe SCADA Encryptor secures legacy SCADA communications while ensuring operational continuity, quantum readiness and long term resilience.



Quantum Ready Security

Supports PQC with QKD integration, enabling organisations to transition towards quantum resilient communications.



Operational Continuity

Designed for mission critical environments where reliability, deterministic communications and system availability cannot be compromised.



Purpose Built for Legacy OT

Protects existing serial SCADA communications without requiring upgrades or replacement of operational systems.



Proven OT Experience

Built on over a decade of protecting the SCADA communication links of Singapore's power distribution network.



High Assurance Security Hardware

Powered by ST Engineering's indigenous *d'Cryptor* SC security chip, certified to NIST FIPS 140-2 Level 4.

Benefits

Quantum Safe SCADA Encryptor strengthens operational resilience with quantum safe cybersecurity designed for today's SCADA environments and tomorrow's threats.



Operational Continuity

Protect critical operational communications.



Risk Reduction

Reduce cyber and operational risk.



Infrastructure Longevity

Extend the life of existing SCADA infrastructure.



Regulatory Compliance

Support regulatory compliance for critical infrastructure.



Quantum Readiness

Accelerate quantum readiness through phased migration.

Deployment Scenarios

Quantum Safe SCADA Encryptor secures mission critical communications across diverse operational environments, from enterprise networks to defence and critical infrastructure.



Power Transmission & Distribution

- Control centre communications
- Substation connectivity
- Remote terminal units



Oil & Gas Operations

- Pipeline monitoring
- Remote terminal communications
- Production facilities



Water & Wastewater Utilities

- Water treatment facilities
- Pumping stations
- Distribution networks



Rail & Transport Networks

- Signalling systems
- Operational control
- Transport infrastructure

