UTSI INTERNATIONAL | SEQURE quantum technology

Quantum-Ready OT Security

A Practical Path for critical infrastructure

A Joint Whitepaper

Table of Contents

EXECUTIVE SUMMARY

A Joint Perspective from SeQure and UTSI

The Imperative for Quantum Readiness

Critical infrastructure operators are entering a decisive moment. Operational technology (OT) environments—power grids, water systems, pipelines and transportation networks—are increasingly digitized, interconnected and exposed. They all rely on secure, resilient systems.

As quantum computing progresses, these same systems face a threat unlike any before: quantum-enabled attacks that can render classical cryptography obsolete almost overnight. Traditional cryptographic methods, from Rivest–Shamir–Adleman (RSA) to Elliptic Curve Cryptography (ECC), depend on assumptions about computational difficulty that quantum algorithms, such as Shor's, can break efficiently. This creates an urgent need for a strategy known as quantum readiness (QR), which ensures that organizations are prepared not just for today's technologies, but for the capabilities of tomorrow.

At the core of QR lies randomness.

Every cryptographic key, digital signature and secure communication depends on high-quality random numbers. Conventional pseudo-random number generators (PRNGs) draw from deterministic algorithms or environmental noise, making them predictable under certain conditions. Quantum random number generators (QRNGs), on the other hand, leverage the inherent unpredictability of quantum mechanics, delivering true randomness with high entropy. SeQure's self-certifying QRNG, SeQRNG, takes this further by continuously validating its quantum output, ensuring that every bit generated is both unpredictable and verifiably quantum in origin.

UTSI complements this innovation by providing the operational context in which these technologies will be deployed. Through their SCADA laboratory, UTSI simulates OT environments to assess how randomness is generated, validated and used in real-world systems. By analyzing the weaknesses of algorithmic randomness under realistic OT conditions, UTSI illustrates why self-certifying QRNGs are a critical defensive tool in the quantum era.

For the leaders responsible for keeping physical systems safe, the challenge is twofold:

- **Defend and modernize aging OT systems** that were never designed for today's digital realities, and
- **Prepare for an adversary** with computational capabilities far beyond today's threat actors.

This paper outlines a practical, low-friction roadmap developed jointly by SeQure, a leader in quantum-grade cryptographic infrastructure, and UTSI, an Industrial Control Systems (ICS) and SCADA modernization firm with 40+ years of operational expertise.

Together, the two organizations demonstrate how critical infrastructure operators can strengthen security now while building toward a quantum-ready architecture that supports compliance, resiliency and long-term defensibility.

Understanding the Quantum Threat Landscape

Quantum computing represents a fundamental shift in how computations are performed. It is not merely a faster classical computer; it is a disruptive technology capable of solving certain problems in parallel at scales previously unimaginable. For cybersecurity, the most immediate implication is the potential to break asymmetric cryptography. Shor's algorithm, for instance, can factor large integers exponentially faster than classical methods, jeopardizing digital signatures, secure key exchanges and encryption schemes that underpin OT security.

While the threat from algorithms is well understood, another, often-overlooked vulnerability resides in the quality of randomness. Cryptographic keys are only as strong as the entropy they are built from. Classical random number generators, whether software-based PRNGs or hardware components exploiting thermal noise, exhibit subtle patterns that can be exploited by sophisticated adversaries.

UTSI's experiments in the SCADA laboratory demonstrated that even seemingly minor deterministic biases, such as recurring processor behaviors, can compromise key security. In contrast, SeQRNG generates quantum-based entropy that passes rigorous FIPS 140-3 randomness tests consistently, eliminating deterministic predictability and mitigating this critical attack vector.

The combination of weak randomness and advancing quantum computing creates a dual threat: adversaries could both break cryptographic algorithms and exploit the very seeds that generate keys. Addressing this requires both innovative technology and operational validation.

Case Study: The Weaknesses of Algorithmic Randomness

UTSI operates one of the industry's most mature SCADA and Industrial Control Systems training environments. In the lab, they simulate real pipelines, energy facilities and water systems—complete with controllers, networks, historians and field devices.

Across modernization projects, UTSI consistently observes five trends:

OT systems have cryptographic gaps that operators cannot see.
Because OT runs on long lifecycle equipment, cryptography in field devices often goes untouched for 10–20 years.

Remote access is the largest and fastest-growing attack vector.
Third-party integrators and field teams depend on it, but without strong key management, it introduces significant risk.

The shift toward AI and digital twins increases dependency on secure data.
If the data feeding machine learning models is tampered with or decrypted, operators lose trust and situational awareness.

PQC awareness is growing, but readiness is low.
Most operators acknowledge the risk, but few have begun the inventory, assessment and planning process.

Modernization cannot disrupt operations.
Any security enhancement must be lightweight, interoperable and deployable with minimal downtime.

In a controlled SCADA laboratory experiment, UTSI examined how traditional Linux cryptographic modules generate random numbers. These modules rely on hardware-generated entropy derived from classical processes, which, while appearing random, are influenced by predictable physical factors. Random numbers extracted from these sources were subjected to statistical tests aligned with FIPS 140-3 standards. The results revealed detectable patterns and irregularities that could, in principle, be exploited in an attack.

SeQRNG, deployed in parallel, demonstrated the advantages of a self-certifying quantum approach. By interleaving randomness-generation rounds with continuous certification rounds, SeQRNG verifies the quantum integrity of each output in real time. Statistical analysis confirmed higher entropy and the absence of detectable patterns, providing a level of security unattainable with classical or first-generation QRNGs. These findings underscore that true quantum randomness, coupled with continuous self-certification, is essential for defending OT systems against quantum threats.

SeQure brings deep expertise in quantum-grade randomness, cryptographic infrastructure and secure key generation. UTSI brings decades of ICS engineering, SCADA modernization and operational experience. Together, they offer a pragmatic roadmap built on:


Low-friction integration


Standards-aligned cryptographic upgrades


Operationally safe rollout


Compliance support


A future-proof foundation for PQC

Planning for Quantum Readiness in OT Environments

Preparing OT systems for quantum threats requires a phased, risk-based approach. Migration to post-quantum cryptography (PQC) in industrial environments demands precision and operational awareness. The joint UTSI + SeQure migration plan is structured to maximize safety, compliance and minimal disruption.

Organizations must first understand the landscape of cryptographic dependencies within their infrastructure, identifying legacy algorithms and devices vulnerable to quantum attacks. Integrating a self-certifying QRNG establishes a robust foundation, ensuring that all cryptographic keys derive from verified, high-quality entropy.

Migration to quantum-safe cryptography should be executed in a controlled and flexible manner, enabling hybrid operation where classical and post-quantum algorithms coexist during transition periods. Operators should prioritize high-risk communications, remote access points and critical control loops while adopting post-quantum encryption for data in transit and at rest. Continuous monitoring, threat simulation and operational testing in environments like UTSI's SCADA laboratory provide confidence that these measures are effective under realistic conditions.

By emphasizing true randomness, controlled migration and continuous validation, organizations can address immediate vulnerabilities and position themselves for long-term resilience against quantum-enabled attacks.

Key Principles of Quantum-Ready OT Security

Several principles guide the effective deployment of quantum-ready strategies:

Foundation First:
High-entropy, self-certified randomness is the cornerstone of secure cryptography. Without it, even post-quantum algorithms are compromised.

Operational Alignment:
Security measures must reflect the realities of OT environments, including legacy systems, high-availability requirements and regulatory constraints.

Phased Migration:
PQC adoption should be gradual and controlled, combining classical and quantum-safe mechanisms to minimize operational risk.

Continuous Validation:
Ongoing testing and monitoring ensure cryptographic integrity is maintained even as hardware ages or environmental conditions fluctuate.

These principles provide a roadmap for organizations seeking to navigate the challenges of quantum readiness while maintaining operational reliability.

SeQure + UTSI: A Complementary Partnership

SeQure's SeQRNG and UTSI's operational expertise form a unique synergy. SeQure delivers provably secure, self-certifying quantum randomness suitable for deployment in SCADA, HMI and field devices. UTSI ensures these technologies are applied effectively in OT environments, simulating realistic conditions, validating security improvements and identifying risks that might otherwise go unnoticed.

This collaboration ensures quantum readiness is not just a theoretical goal but a practical, achievable outcome. By combining technology and operational expertise, organizations can take proactive steps today to safeguard critical systems against the quantum threats of tomorrow.

The Limitations of Traditional and First-Generation QRNGs

While quantum mechanics provides an ideal foundation for true randomness, early implementations of QRNGs fell short in operational environments. First-generation devices often relied on passive quantum noise and one-time calibrations, producing outputs that were theoretically random but vulnerable in practice. Device aging, environmental interference and unmonitored hardware parameters could reduce entropy, creating subtle biases that compromised cryptographic strength. Additionally, these systems typically offered only statistical tests of output, leaving the quantum integrity of the source unverified.

Classical random number generators suffer similar, if not greater, weaknesses. The deterministic nature of hardware components governed by classical physics, coupled with flawed entropy estimation, leaves keys and cryptographic protocols vulnerable. Attempts to monitor parameters in real time were often incomplete, and one-time calibrations created trust gaps between laboratory testing and real-world operation. These shortcomings underscore why high-assurance OT systems require a new approach.

Self-Certifying QRNG: SeQure's SeQRNG

SeQRNG represents the next generation of quantum random number generators. Unlike passive first-generation devices, it operates as an active, self-testing system. Randomness-generation rounds are interleaved with certification rounds that continuously validate the quantum source, ensuring that every bit is unpredictable, private and auditable.

This approach closes the gap between theoretical randomness and operational deployment.

The device architecture integrates quantum photonics, electronics and secure computing to deliver high-rate entropy generation suitable for OT environments. Each random string comes with self-certification metadata, providing independent verification of quantum origin, traceability and regulatory compliance. By deploying SeQRNG, operators gain confidence that cryptographic keys, initialization vectors and other critical security components are derived from provably secure entropy, even in the presence of potential adversarial interference.

Integration with existing cybersecurity infrastructure is straightforward. SeQRNG can feed entropy into hardware security modules, key management systems and encryption libraries through a REST API. This enables seamless adoption across cloud, enterprise and IoT environments without extensive retrofitting while maintaining continuous monitoring and audit readiness for regulated industries.

Operational Validation in OT Environments

SeQure's technological innovation is complemented by UTSI's operational expertise. In UTSI's SCADA laboratory, quantum and classical randomness sources are evaluated under conditions replicating the unique dynamics of OT systems, including network latency, device heterogeneity and real-time control constraints. These simulations highlight both vulnerabilities and mitigation strategies, providing empirical evidence of the benefits of self-certifying QRNGs.

For example, when classical RNGs were subjected to stress tests in a SCADA environment, minor environmental fluctuations produced detectable patterns in key-generation sequences. In contrast, SeQRNG maintained consistently high entropy and verified its output in real time. These tests illustrate the dual importance of quantum-based entropy and continuous operational validation: it is not enough for a device to be theoretically quantum; it must demonstrate reliable randomness in the conditions in which it will be used.

Post-Quantum Cryptography and Hybrid Strategies

Randomness alone is not sufficient. Quantum readiness requires adoption of post-quantum cryptographic algorithms that resist attacks from quantum computers. SeQure's QRNG ensures the integrity of cryptographic keys, while hybrid strategies allow OT systems to operate securely during the transition from classical to post-quantum algorithms. Key encapsulation mechanisms, lattice-based encryption and digital signature schemes like CRYSTALS-Kyber can be combined with high-entropy quantum randomness to safeguard both data in transit and at rest.

Hybrid deployment strategies are critical because OT systems cannot tolerate abrupt disruptions. SeQure and UTSI advocate a phased approach, where quantum-safe algorithms are introduced in tandem with existing protocols, monitored in operational settings and scaled according to risk and criticality. Continuous assessment and adjustment, guided by IEC 62443 standards, ensure both security and system availability are maintained throughout the transition.

Strategic Implications for Critical Infrastructure

For operators of critical infrastructure, quantum readiness is not a distant concern—it is a strategic imperative. Weak randomness and vulnerable cryptography can expose systems to catastrophic failures, including service disruptions, safety incidents and regulatory non-compliance. By integrating self-certifying QRNGs with post-quantum algorithms and validating them under operational conditions, organizations can establish a resilient defense posture that extends from the control room to remote field devices.

Moreover, quantum readiness strengthens trust with stakeholders. Regulators, customers and partners can be confident that critical operations are protected against emerging threats. By prioritizing QR, organizations not only defend against attacks that may arrive years in the future but also address immediate vulnerabilities inherent in classical cryptography and algorithmic randomness.

Critical infrastructure organizations should begin taking action now:

Near-Term (0–6 months)

- Conduct a quantum-risk assessment
- Begin cryptographic inventory
- Deploy QRNG for secure key generation
- Align with TSA/NIST/NERC requirements
- Integrate QRNG into VPNs, remote access and SCADA authentication

Mid-Term (6–24 months)

- Begin phased deployment of elastic cryptography
- Introduce PQC-capable systems during refresh cycles
- Update firmware signing and code integrity processes

Long-Term (18–60 months)

- Transition core systems to PQC
- Establish continuous crypto auditing and lifecycle practices
- Validate builds in UTSI's SCADA Lab
- Retire classical algorithms as standards evolve

This phased approach supports immediate security gains while building a resilient, quantum-ready future.

A Practical Roadmap for Quantum Readiness

The quantum era is coming—and for critical infrastructure, the impact will be profound. But with the right approach, operators can strengthen security today while preparing for tomorrow's threats. SeQure provides the cryptographic innovation. UTSI provides the operational expertise.

Together, they provide a practical framework for achieving quantum readiness in OT environments.

The combination of self-certifying QRNGs and operational validation ensures that organizations can:

Secure cryptographic keys with provably high-entropy randomness

Transition safely to post-quantum cryptographic algorithms without operational disruption

Continuously monitor and validate system integrity under real-world conditions

Reduce the risk of catastrophic failures and maintain regulatory compliance

Quantum computing is no longer a distant theoretical concern. By taking proactive steps now—leveraging proven technology and operational expertise—critical infrastructure operators can fortify their systems against a threat that is already approaching reality.

SeQure's SeQRNG and UTSI's SCADA-based validation form the cornerstone of a quantum-ready strategy, combining innovation, reliability and operational insight to protect the world's most critical systems.

About the Authors

About SeQure

SeQure Quantum is a deep-tech company developing quantum technologies for cybersecurity, founded in Chile and Poland. Built on more than two decades of scientific research in quantum information, the company designs and commercializes quantum random number generators (QRNGs) that self-test and certify their entropy in real time. SeQure Quantum's technology enables high-assurance cryptography and supports the transition toward quantum-safe security architectures for critical infrastructure, finance, telecommunications, and digital services

About UTSI

UTSI International Corporation has been a trusted leader in OT Cybersecurity, Pipeline Applications and Industrial Control Systems (ICS), SCADA modernization and Leak Detection for the past 40 years. The company's elite engineering team collaborates closely with clients to craft customized strategies that maximize efficiency and minimize risk in industrial automation. UTSI's comprehensive expertise spans all applications and technologies that comprise modern real-time industrial control systems, including AI expertise, ensuring cutting-edge and reliable solutions.

SEQURE quantum technology

Paulina Assman,
CEO & Co-Founder

paulina@sequrequantum.com

sequrequantum.com

UTSI INTERNATIONAL

Shaun Six
President

scs@utsi.com

utsi.com