Securing energy assets in the quantum era



Regulatory and system-operator perspective on post-quantum cybersecurity for Australia's energy infrastructure.

Prepared for Government, Regulators, and System Operators.

Public Release

29.09.2026

Nisient

Contents

01 **Executive summary**
03 **Energy system context and regulatory risk**
04 **Regulatory imperative for post-quantum readiness**
05 **IoTransit as a quantum-resilient communications layer**
06 **Architecture aligned to energy system resilience**
07 **Application across the energy value chain**
08 **Bridging Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC)**
12 **Governance, assurance, and oversight**
13 **Conclusion**

Nisient Pty Ltd

Level 1, 55 Collins St
Melbourne VIC 3000
Australia
ABN 40616962899

enquiries@nisient.com
+61 7 5227 9613
nisient.com

Executive summary

Australia's energy system depends on digital infrastructure to maintain system security, market integrity, and a reliable supply of electricity and gas. According to the Australian Energy Market Operator (AEMO)'s FY25 Annual Report, national energy markets increasingly rely on strong operational control of geographically dispersed assets and resilient control environments that can operate under extreme weather or system stress events, including cyber-attacks.

"Malicious foreign cyber actors gained access to the network of a U.S. industrial automation solutions company that offered services – such as system integration [and] engineering consulting – for clients including power utilities and transportation systems. The company specialized in a kind of OT known as supervisory control and data acquisition systems. SCADA systems enable the remote operation and monitoring of industrial machinery."

Publish Date: September 23, 2026
cisa.gov

The emergence of advanced agentic automation and quantum computing offers long-term operational advantage for energy distribution. At the same time, it also risks infrastructure being accessed through virtual power plants and consumer energy resources.

Operational technology relies on classical public-key cryptography, such as RSA, but legacy Supervisory Control and Data Acquisition (SCADA) environments and remote access pathways, including low-bandwidth networks, still rely on decades-old protocols. When emerging agentic AI cyber threats combine with cryptographically relevant quantum computers, these protections will no longer provide adequate security.

For national energy infrastructure with asset lifecycles measured in decades, post-quantum cryptography (PQC) shouldn't be considered a future enhancement, but a current risk-mitigation requirement.

Recognising that the quantum security landscape and anticipated cyber threat development will continue to evolve, Nisient maintains a strategic vision to bridge post-quantum cryptography with the future gold standard in cybersecurity, Quantum Key Distribution (QKD).

Executive summary (continued)

Quantum Key Distribution leverages fundamental quantum properties to detect interception and provides additional security assurances by triggering rekeying of the advanced security layer. By combining deployable PQC cryptographic agility today with advanced quantum key uniqueness for tomorrow, Nisient seeks to ensure remote energy operations remain secure, resilient, and trusted across the full quantum transition horizon.

This white paper outlines how Nisient's IoTransit network will continue to deliver a production-ready, quantum-resilient communications layer and how we support secure remote operations in a quantum-enabled future. Undertaken to protect SCADA equipment, align with future system security mandates and SOCI Act obligations, while supporting the broader objective of sustaining confidence in Australia's energy markets throughout our transition from fossil-fuel-based to renewable energy and a future embedded in renewable exports.

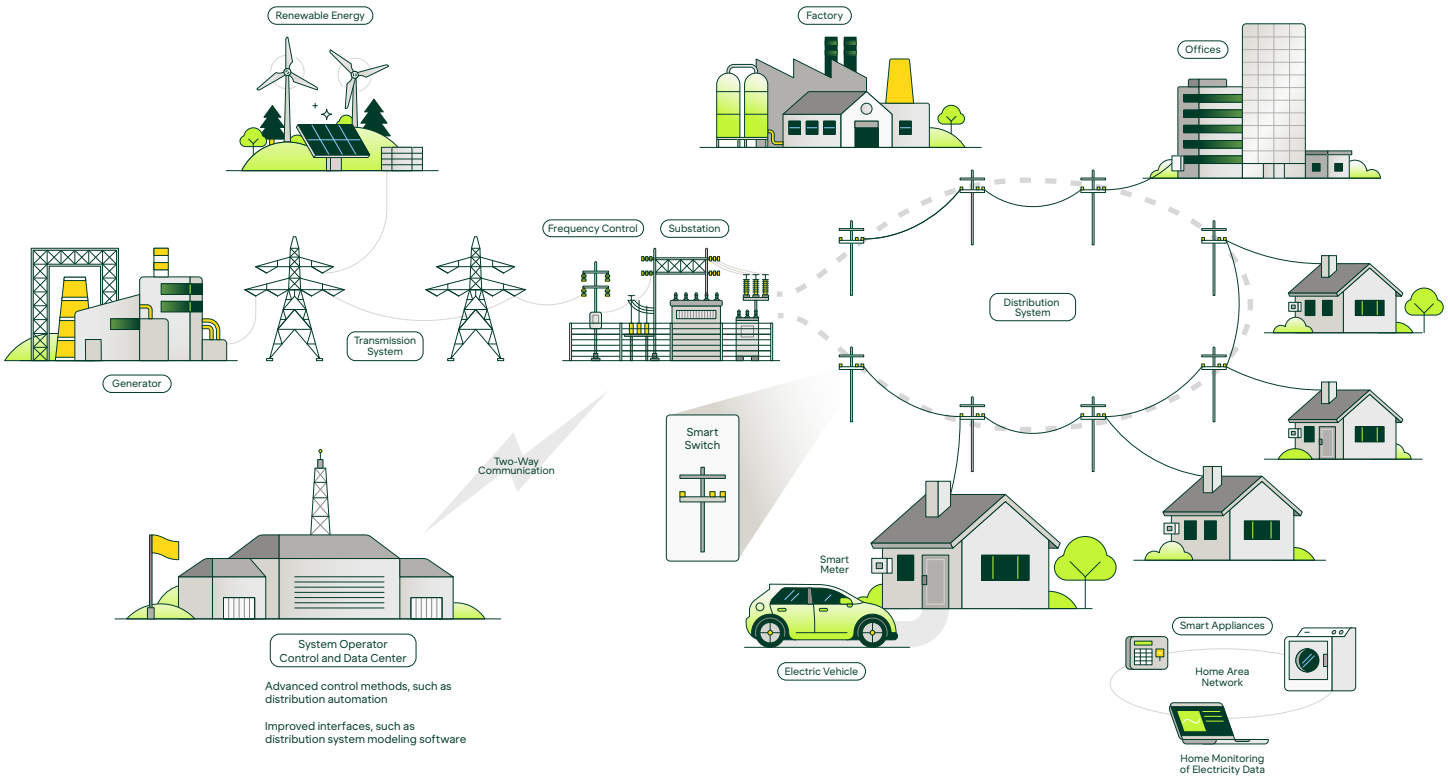


Figure 1

Australia's energy network

Energy system context and regulatory risk

Increasing digital criticality

Australia's energy landscape is undergoing rapid and unprecedented change. This change is driven by an evolving energy supply mix as we transition from fossil fuels to renewables. Challenges include ageing infrastructure, changing weather patterns, evolving technologies and unprotected long-lived assets. Opportunities include shifting consumer preferences, renewable hydrogen exports, and growing interdependencies between consumer energy resources, our gas, and traditional electricity markets.

As the world embraces Agentic AI and increased data centre capacity drives additional resource demand, a secure energy supply will depend on resilient digital operations spanning real-time monitoring and control of production, transmission, storage, and distribution assets, as well as control rooms supporting increasingly complex system states. The rapid expansion of virtual power grids with inverter-based resources, grid-scale batteries, distributed energy resources, and bi-directional energy flows has significantly increased the potential attack surface of Australia's energy and gas networks.

Quantum computing as a systemic risk

The combination of emerging AI threats and quantum computing poses a fundamental cybersecurity risk to widely used cryptographic algorithms, such as RSA and elliptic-curve cryptography, which underpin device identity and authentication for secure SCADA and operational communications. It also raises concerns about long-term consumer confidence in our government's ability to protect our way of life and exposes vulnerabilities in networks that will delay our pathway to being a world leader in renewable exports.



Regulatory imperative for post-quantum readiness

Alignment with AEMO's system security mandate

AEMO's statutory duty to operate secure, reliable, and resilient energy systems increasingly depends on proactive cyber risk management. Being quantum-resilient directly supports the prevention of future systemic cyber incidents, the protection of operational data and business-critical digital assets, and, in turn, the preservation of stakeholder and market confidence.



Critical infrastructure obligations

Energy systems are designated critical infrastructure under the Security of Critical Infrastructure (SOCI) Act. An unprotected control layer risks the availability and integrity of these networks. PQC adoption should be viewed as a stepping stone to future quantum security measures such as QKD, which complement existing cyber resilience and risk management obligations, rather than as an experimental technology or as a standalone solution. It should be supported by continuous testing of quantum-safe algorithms to stay ahead of any emerging quantum-decryption risks and ensure reliability in low-bandwidth networks, with eventual QKD deployment across all core networks.

IoTransit as a quantum-resilient communications layer

Overview

The Nisient IoTransit network is a globally distributed, real-time data network designed to support large-scale, geographically dispersed infrastructure environments and has already been deployed globally across business-critical infrastructure, including SCADA assets.

Unlike perimeter-based or VPN-centric models, IoTransit provides a purpose-built, secure communications platform optimised for high availability, remote operations, and future cryptographic resilience. While the Nisient IoTransit Network is agile PQC-secure today, Nisient's future is embedded in QKD-based quantum security.

Capabilities relevant to system operators

The Nisient IoTransit network offers agile post-quantum cryptography for data in transit for differing network topologies. It's also established a triple-redundant, geographically dispersed core infrastructure with offline-capable edge agents that enable ongoing operation during outages. Secure remote access provides an experience comparable to being on-site, along with real-time fine-grained access control for identity management and comprehensive audit logging.

Designed for zero-trust, automation-first operations, it aims to minimise manual intervention and errors, thereby reducing the need for manual or batch handling of critical infrastructure.

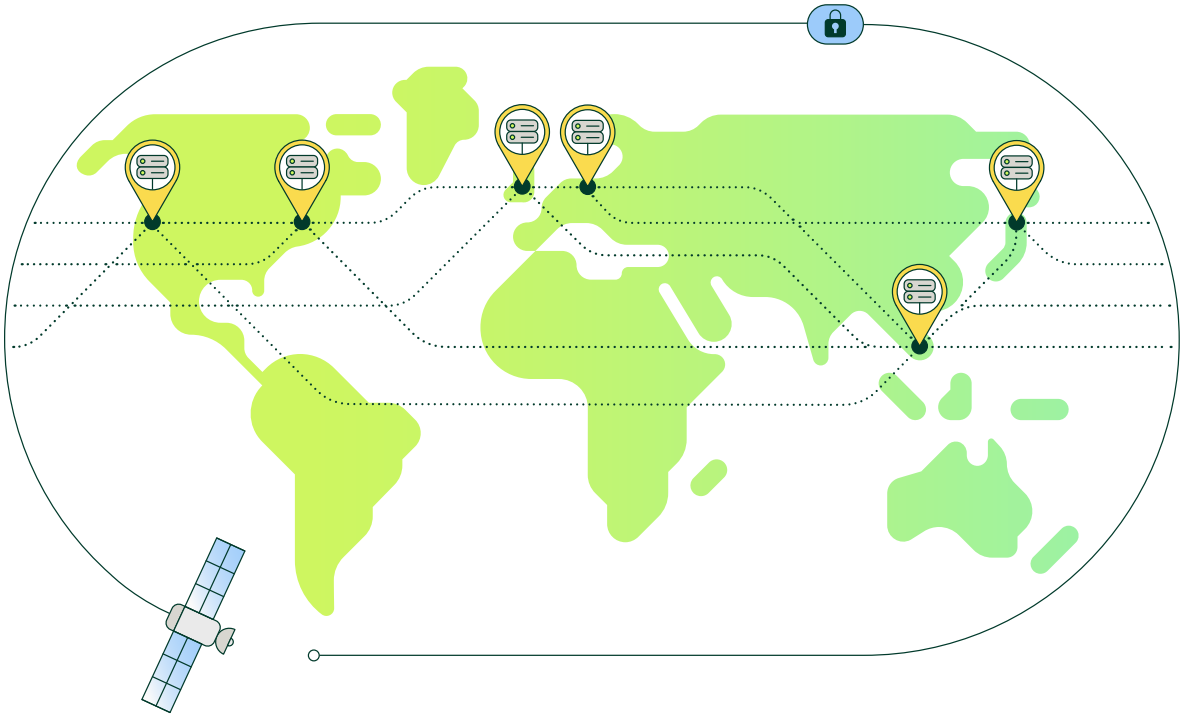


Figure 2

Core IoTransit database redundancy

Architecture aligned to energy system resilience

Zero-trust communications model

The Nisient IoTransit network enforces a zero-trust approach where every device connection operates over a PQC-agile authenticated network. Whether remote, on-site, or cloud-based. No device or digital asset is trusted without verification, and all communications are encrypted end-to-end using quantum-resilient algorithms that are continually tested against emerging threats. Our IoTransit Network is cryptographically agile, meaning that novel algorithms can be changed in real time over varying network topologies as conditions change.



Operational resilience under degraded conditions

Energy systems must operate reliably during extreme weather conditions, communication outages, and partial infrastructure failures. Therefore, the Nisient IoTransit network architecture is engineered to maintain functionality even when disconnected, securely synchronising once connectivity is restored. This triple-redundant configuration ensures control during major system events and routine, intermittent operations.

Application across the energy value chain

Generation, storage, and networks

Nisient can play a key role in securing renewable energy systems with quantum-safe encryption. By providing real-time monitoring and operations capabilities for critical network assets while enforcing the highest levels of security. Nisient enables the rapid, safe introduction of renewable energy generation into the power grid and secures existing ageing infrastructure. This allows cost savings to be directed toward advancing renewable exports.

By aligning secure data infrastructure with renewable energy optimisation, Nisient bridges energy transformation to embrace Distributed Energy Resources (DER), behind-the-meter Consumer Energy Resources (CER) and the potential inclusion of Vehicle-to-Grid (V2G) in the Australian energy network, delivering security and sustainability outcomes.

Market and operational systems

Telemetry is secured at the network layer using PQC-based encryption, ensuring that data flowing from field devices into control rooms is protected against interception or tampering. The Nisient IoTransit network is data-agnostic and supports all communication protocols, providing a single view of millions of device types.

Australian case study

In global business-critical deployments for some of the world's most recognised brands, the IoTransit network was implemented to secure legacy SCADA environments across heterogeneous network topologies. A single deployment now supports over 700,000 devices through a single operational view, improving resilience while embedding post-quantum security, remote operations and predictive analysis into daily operations.

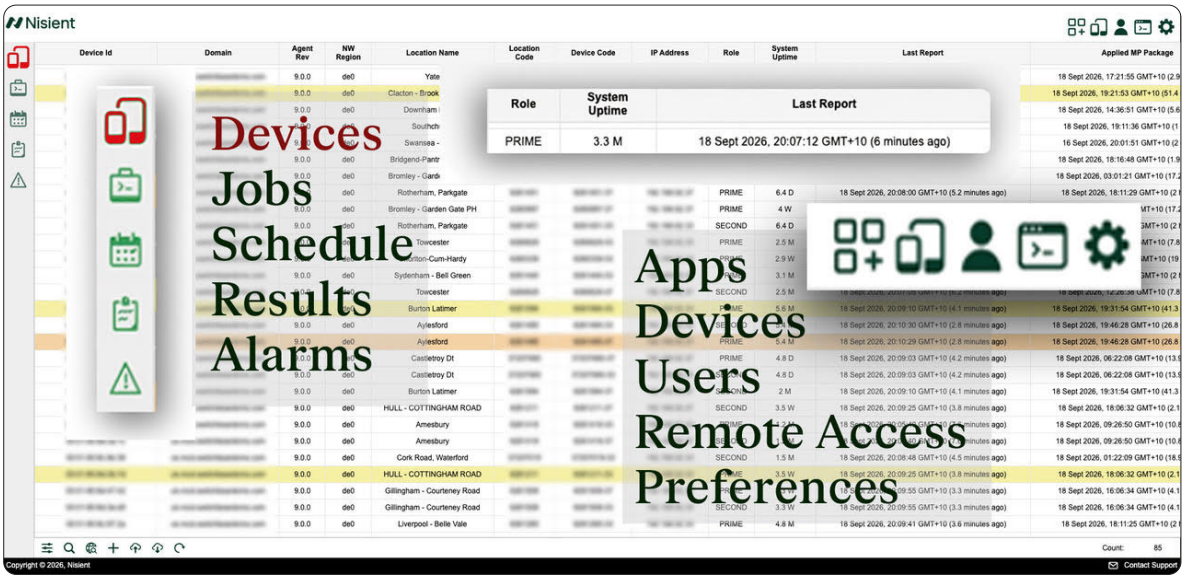


Figure 3

Nisient IoTransit device control

Bridging Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC)

Strategic objective: A practical path to future quantum-resilient operations

While post-quantum cryptography offers an immediately deployable, standards-aligned approach to address quantum risk, Nisient recognises that quantum-safe security will ultimately require multiple solutions to meet various operational requirements. For the security of digital assets on our network, the long-term gold standard will be Quantum Key Distribution (QKD), which leverages the fundamental quantum uncertainty principle and allows entangled qubits to collapse when observed, alerting the security layer to an attempted breach before access is granted.

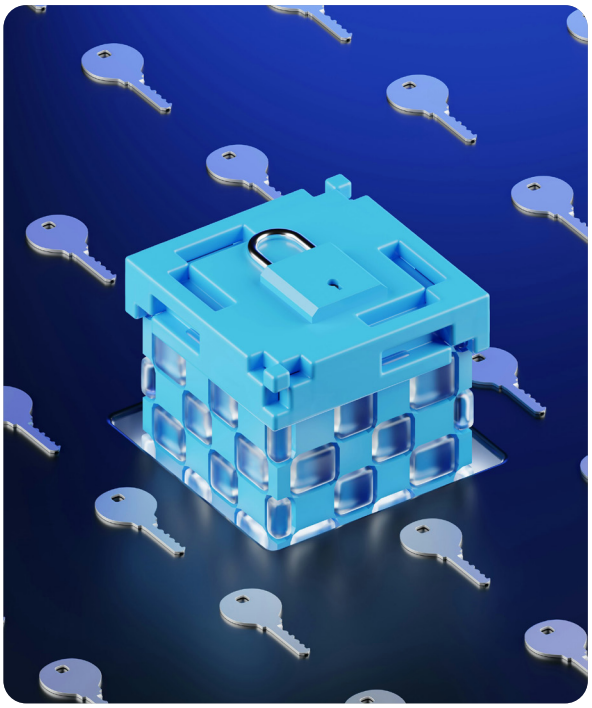
Over time, commercially viable quantum computers will enable hybrid CPU/GPU/QPU data centres, and Nisient have already partnered with NextDC and CDC to ensure the highest level of trust and dedicated space to commercialise what will become the gold standard of encryption.

Quantum Key Distribution (QKD) provides theoretically verifiable security, but its practical use is currently constrained by physical infrastructure requirements, distance limitations, cost, and operational complexity. Nisient's strategic objective is to bridge QKD and PQC, enabling customers to access quantum-resilient security now while remaining prepared to adopt QKD capabilities when they become operationally and financially feasible.

This approach reflects the operational realities of national energy systems, where assets are widely spread across remote areas, communications must traverse a mix of terrestrial, wireless, and satellite networks, and operations must continue even when connections are poor or non-existent. In this operational environment, energy, utilities, and critical infrastructure sectors must continually invest in forward-looking security measures to ensure resilience, uphold operational integrity, and protect essential services against ever-changing cyber threats.

PQC as the foundation layer

Within the IoTransit network, PQC serves as the fundamental security layer supporting all remote operations. By integrating both a hybrid of X-25519 and ML-KEM-768, as well as ML-KEM-1024 and AES-256, we safeguard both our customers' data and their global solutions across various network topologies. This hybrid, adaptable methodology ensures that device identity, authentication, and data-in-transit protection are defended against both current and emerging threats. Additionally, this strategy secures operational access channels, maintaining the integrity and confidentiality of command-and-control interactions within distributed energy environments.



Importantly, this architecture is inherently scalable, enabling consistent implementation of security controls across millions of assets without requiring specialised physical infrastructure.

By incorporating PQC at the network level, IoTransit offers immediate and practical risk mitigation while complying with existing regulatory standards and operational requirements, thereby establishing a future-proof foundation for secure communications within energy systems.

Bridging Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) (continued)

QKD as a complementary future capability

Nisient's strategic approach recognises that quantum key distribution (QKD) will assume a crucial and supplementary role in future secure communication infrastructures, especially in environments where its deployment is both technically feasible and economically justifiable.

Such environments include fixed, high-value control centres, dedicated fibre links across metropolitan or transmission corridors, and specialised communication and control systems for inter-agency or system operators.

Both QKD and PQC ultimately enable the secure generation and exchange of shared secret keys for symmetric encryption. QKD also offers the advantage of detecting eavesdropping, thus allowing immediate re-keying procedures to maintain optimal security standards. Conversely, PQC provides scalable, software-based, quantum-resistant protection across existing and diverse network environments, although it lacks detection capabilities. This distinction is significant, given that many current data networks are configured to support monitoring for testing and lawful control during emergency situations, which malicious actors could potentially exploit without detection.

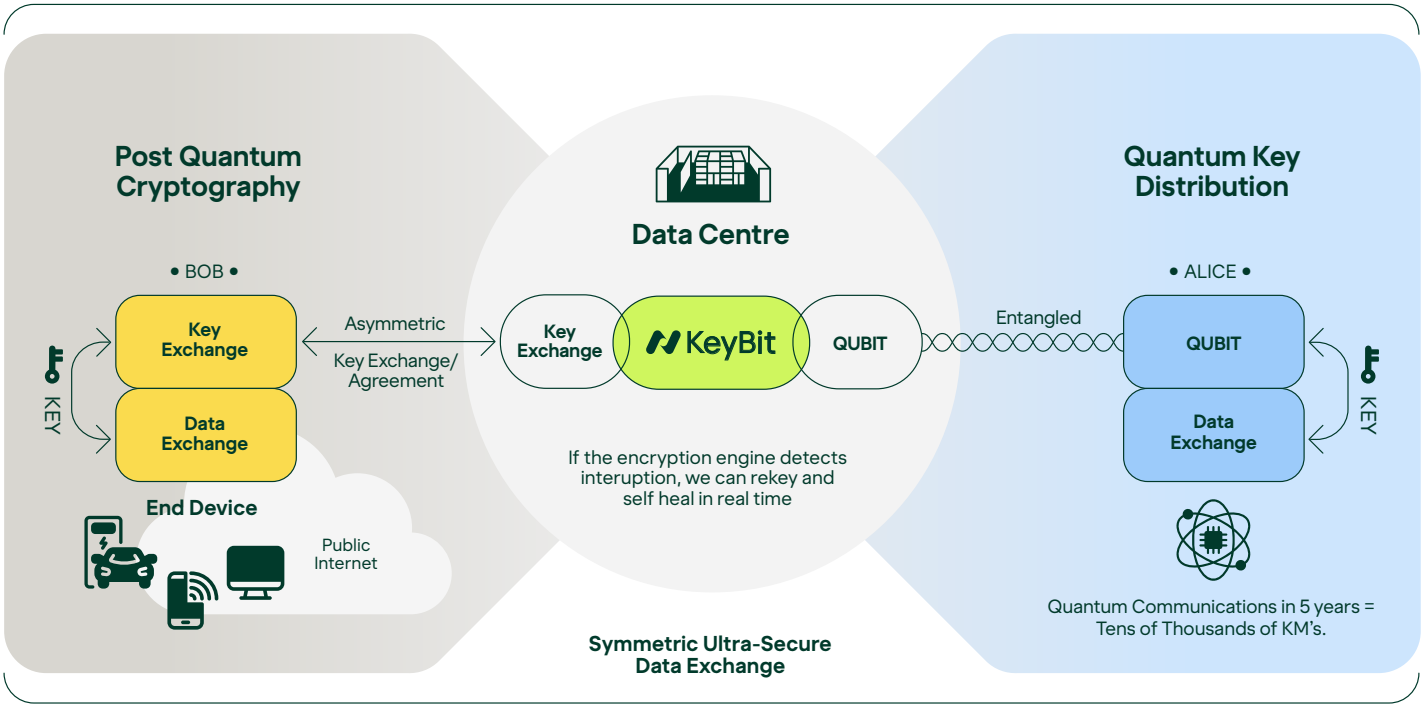
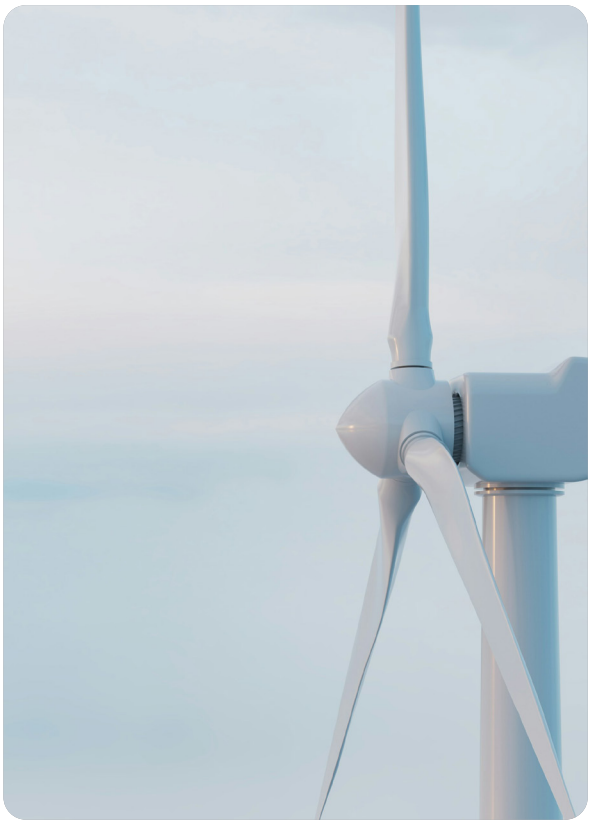


Figure 4

Nisient project KeyBit to integrate emerging QKD to PQC bridge

To address these challenges, Nisient is developing an integrated approach, called the Nisient ‘KeyBit’, that bridges the QKD and PQC domains to deliver true end-to-end security across hybrid network environments. This forward-looking model enables secure symmetric encryption keys to be generated and maintained across both quantum-secure and traditional networks without requiring decryption or re-encryption at network boundaries, thereby removing common points of vulnerability.

IoTransit’s cryptographic agility supports dynamic key management, including coordinated re-keying of PQC-secured links, and when integrated with QKD eavesdropping detection systems, enables simultaneous re-keying across both QKD and PQC pathways in response to detected threats. Recognising that modern cyber threats typically target multiple attack surfaces, this approach enables rapid key rotation and adaptation of emerging cryptographic methods as novel algorithms are tested over time. For critical infrastructure environments where the consequences of compromise are significant, this ensures a high level of resilience, operational continuity, and long-term security.



Governance, assurance, and oversight

Transparency and auditability

The Nisient IoTransit network incorporates comprehensive, enterprise-grade logging capabilities that provide full visibility across all operational and security-relevant activities within the network. This includes detailed records of user actions, device communications, and all configuration and control changes, captured consistently and in a tamper-evident manner. By maintaining a complete, auditable record of interactions across human and machine interfaces, the platform establishes a strong foundation for transparency, accountability, and operational governance.

These capabilities directly support regulatory oversight requirements, enabling organisations to demonstrate compliance with evolving cybersecurity and critical infrastructure standards. In the event of an incident, detailed, time-aligned logs facilitate efficient root cause analysis, forensic investigation, and response validation. Furthermore, Nisient's IoTransit network logging framework provides assurance to executive stakeholders, including boards, government agencies, and market bodies, by delivering clear evidence of control, traceability, and adherence to security best practices across complex and distributed energy environments.

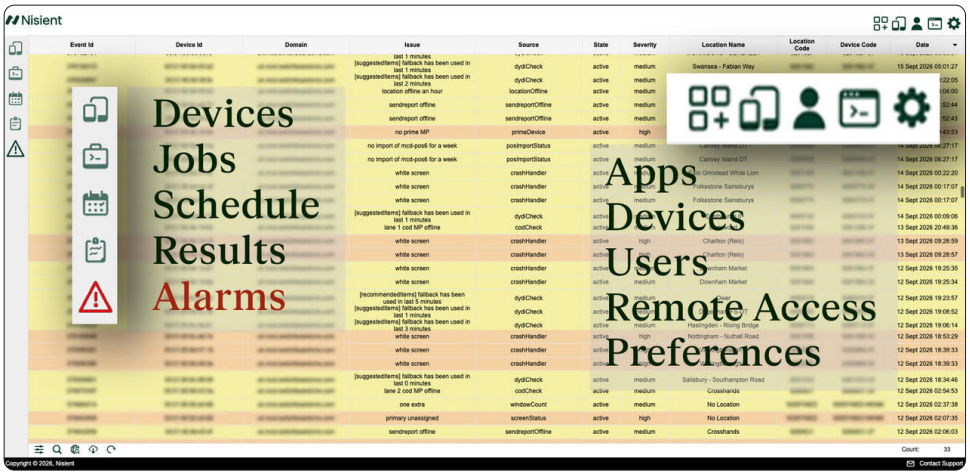
Supporting sector-wide cyber maturity

The platform is also designed to align with and support industry-wide cybersecurity uplift initiatives through a principled and forward-looking architecture. By embedding security through design at the core of its communications framework, IoTransit ensures that protection is not an overlay or afterthought, but an inherent characteristic of all data exchange and operational processes. This approach enables consistent enforcement of security controls across diverse environments, reducing complexity while strengthening overall system integrity.

In doing so, the platform reduces reliance on bespoke, asset-specific security solutions that are often costly, hard to scale, and difficult to maintain. Instead, IoTransit provides a unified and standardised security layer that can be applied across heterogeneous device fleets and network topologies. This creates a scalable, adaptable foundation that meets current and emerging regulatory requirements, positioning organisations to respond efficiently to evolving compliance obligations while maintaining operational resilience and long-term security assurance.

Figure 5

Nisient IoTransit device alarm centre



Conclusion: A forward-looking control for system security

Australia's energy transition currently relies on digital systems that must stay secure and trusted for many years; however, Quantum computing significantly changes the risk landscape of those systems.

From a regulatory and system-operator perspective, post-quantum-secure communications and strategic investment in quantum-enabled security should be regarded as preventive measures similar to redundancy, protection systems, and operational reserves.

Nisient's IoTransit network demonstrates that post-quantum security can be implemented today in production environments at scale, aligned with AEMO's operational and statutory responsibilities.

By intentionally integrating post-quantum cryptography (PQC) and quantum key distribution (QKD) rather than viewing them as competing methods, Nisient endeavours to provide a pragmatic, forward-looking security strategy that ensures ongoing protection throughout the quantum transition. Incorporating quantum-resilient communications now strengthens Australia's ability to maintain secure, reliable energy systems during and after the transition.

Nisient—supporting secure, resilient, and future-ready renewable energy systems



Nisient

Contact

For further information or advice on how to mitigate risk, manage transition and secure your energy assets in the evolving Quantum era:

enquiries@nisient.com

+61 7 5227 9613

nisient.com