Application Note

VIAVI Solutions

Future-Proofing Communications: The Rise of Quantum-Safe Technology

Exploring the security frameworks and validation tools that enable organizations to move quantum algorithms and architectures from theoretical models and lab environments into secure, real-world deployments.

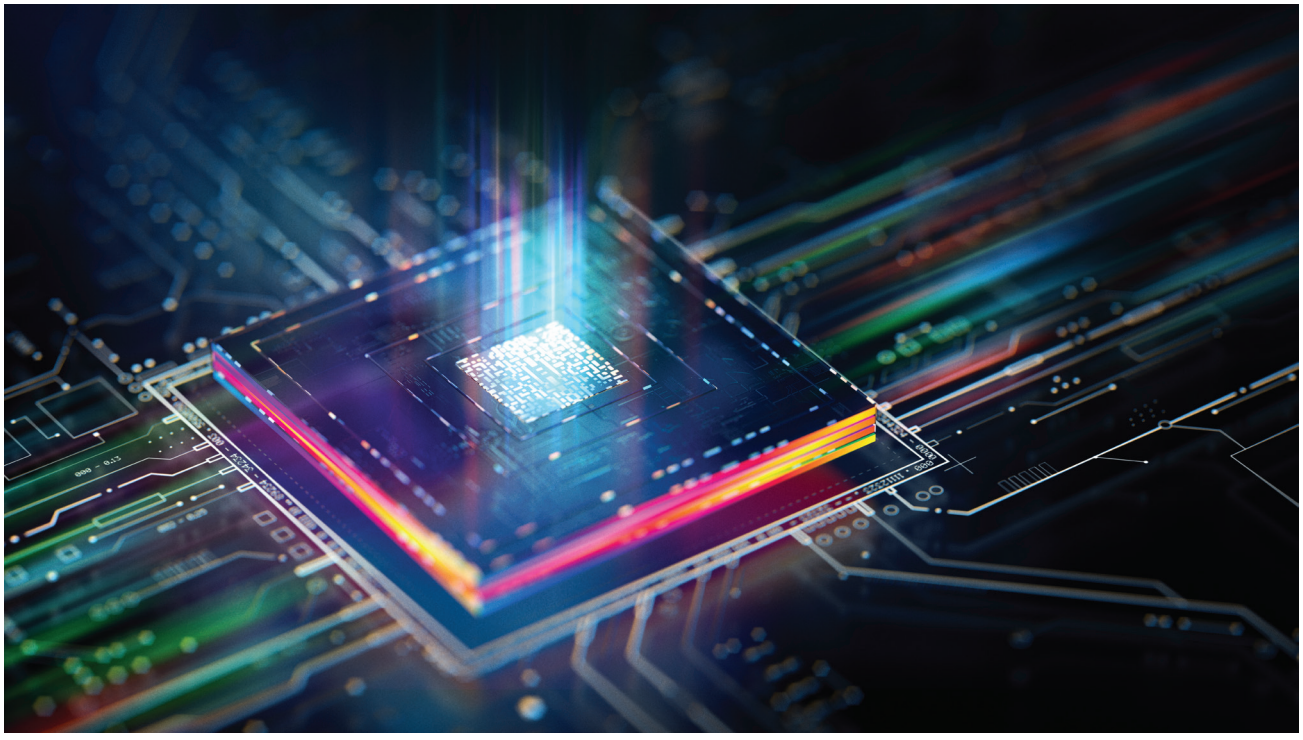
TABLE OF CONTENTS

Quantum-safe communication is no longer a distant goal—it's happening now. A diverse ecosystem of technologies is driving this progress, including Quantum Key Distribution (QKD), Post-Quantum Cryptography (PQC), end-to-end hybrid QKD-PQC models, satellite-based cryptography and key management, and transitional architectures that combine classical and quantum-safe systems. These innovations are transforming our understanding of secure communications in light of quantum computing's disruptive potential.

As these technologies develop, ensuring that architectures and system deployments operate with maximum resilience, security, efficiency, and real-world reliability becomes crucial. This is particularly important at the optical layer, where quantum technologies intersect with physical infrastructure. In many cases, the challenge is to transform quantum science—especially quantum optics—from experimental setups into reliable, field-ready solutions.

Standards and conformance are essential to this transition. But so too is a deep understanding of the infrastructure, especially the optical systems that underpin secure quantum transmission. Optics is not just a component; it is a cornerstone of quantum-safe communications.

Trusted partners with both quantum innovation and deep fiber expertise are essential for success. This paper examines the key factors for deploying quantum-safe technologies on a large scale. VIAVI is uniquely positioned at this nexus, combining decades of leadership in fiber optics with advanced quantum research. With over 30 years of experience in systems, physics, and lab validation, VIAVI offers a rare perspective on how to securely and efficiently transition photon-based communication from the lab to practical deployment.



1 INTRODUCTION

The anticipated explosion in quantum computing capabilities is poised to redefine the landscape of digital security. As quantum processors edge closer to practical realization, the cryptographic foundations that secure today's communications, financial systems, and digital identities face an existential threat. This looming milestone—often referred to as Q-Day—marks the point at which quantum computers will be capable of breaking widely used public-key cryptosystems such as RSA and Elliptic Curve Cryptography (ECC), rendering much of the world's encrypted data vulnerable to decryption.

While Q-Day has not yet arrived, the urgency to act is now. Data harvested today can be decrypted tomorrow, a threat known as "harvest now, decrypt later." In response, governments, standards bodies, and enterprises are accelerating efforts to adopt quantum-safe technologies that can withstand the computational power of quantum machines.

Standards and conformance testing are essential to this evolution. Without rigorous validation, even the most promising quantum-safe solutions risk failure in deployment. Infrastructure considerations, especially those involving fiber optics, photon transmission, and signal integrity, must be addressed with precision.

However, transitioning from theory to practice is a complex endeavor. Quantum-safe technologies must not only be secure: they must also be interoperable, resilient, migratable, and able to perform in real-world environments. This is especially critical at the optical layer, where quantum signals are transmitted and received as well as at the post-quantum key encryption layer. In many ways, the challenge is to move quantum technologies—particularly quantum optics—out of the lab and into the field, transforming them from scientific experiments into operational systems.

This is where VIAVI's expertise becomes indispensable. With over 30 years of leadership in fiber optics, systems engineering, and lab validation, VIAVI is uniquely positioned to support the quantum transition. Our quantum-safe testing suite offers a comprehensive platform for evaluating functionality, compliance, performance, and resilience of quantum-resistant technologies. Whether integrated into existing infrastructures or deployed in testbeds, VIAVI solutions empower stakeholders to confidently assess and deploy quantum-safe systems.

This paper examines the evolving landscape of quantum-safe communications, the technologies driving it, and the crucial role of testing and validation in ensuring a secure and seamless transition to a post-quantum world.

2 QUANTUM SAFE NETWORKS

2.1 Why needed

Digital encryption is a crucial component of any over-the-air communication systems like mobile telephony. Eavesdroppers can listen to calls and attempt to extract data, but encrypting the data eliminates this threat. Modern encryption methods are at risk of being broken with the rise of Quantum computers. Although quantum computers are still 5-10 years away, malicious actors can illegally capture data now and decrypt it later when quantum computers become functional. This threat is known as Harvest Now, Decrypt Later (HNDL), and it poses a significant concern for governments, military, and financial institutions. One solution to this issue is adopting PQC to safeguard sensitive data from the potential threats of quantum computing and stolen information.

The mobile standards body 3GPP is evolving its standards to incorporate PQC algorithms to defend against future quantum computer attacks. 3GPP relies on other standards bodies (i.e., National Institute of Standards and Technology (NIST)) for the standardized PQC algorithms. The concern about the potential attacks quantum computers may pose has prompted GSMA (Global System for Mobile Communications Association) to establish a Post-Quantum Telco Network Task Force (PQTN) to advise mobile operators on how to transition to post-quantum readiness.

Standardization efforts in QKD have been underway for over a decade, driven by the need to ensure interoperability, security assurance, and global adoption of quantum-safe communication systems. Organizations such as the European Telecommunications Standards Institute (ETSI), International Telecommunication Union (ITU-T), and ISO/IEC have led the charge in defining frameworks, protocols, and security requirements for QKD systems.

2.2 Standards

Each country or region has created a related forum for quantum technologies, such as QuIC (EU), QIC (Canada), Q-STAR (Japan), QED-C (US), UKQuantum (UK), KQIA (South Korea), NQSN (Singapore) and QIIA (China). However, they may have different motivations and goals. For example, the United States aims at the National Quantum Initiative Act promoting quantum technology research, talent development and industrial innovation. China aims for quantum dominance in specific application areas such as cryptography and materials science with the "Quantum Technology Roadmap" and adopting a multifaceted approach to research, human resources, and infrastructure. Japan aims to build a society where the use of quantum technology is accessible to everyone, promote the globalization of quantum technology, and support the creation of business opportunities by applying quantum technologies.

Europe emphasizes fundamental research with a focus on quantum communications, computing, and sensing, investing in quantum hardware, software, and algorithms to strengthen the ecosystem. This effort fosters research hubs for quantum computation, sensing, and communications.

ITU-T SG11, SG13, and SG17, along with ETSI ISG QKD, have been working on QKD and QKDN standardization. ISO/IEC/JTC1 specifies some evaluation methods for QKD modules. GSMA provides guidelines for PQC and hybrid scenarios in the telecom industry.

NIST is leading the way in defining PQC algorithms and has already released the first three algorithms in August 2024. These standards, based on the CRYSTALS-Kyber, CRYSTALS-Dilithium, and SPHINCS+ algorithms, are designed to ensure secure communication and data protection against future quantum computing capabilities. While NIST is a US agency establishing PQC standards, many countries have chosen to adopt NIST's recommendations, with a few deciding to create their own versions (i.e., China and Korea).

ETSI, ITU-T, and ISO/IEC have led the charge in defining frameworks, protocols, and security requirements for QKD systems. ETSI's Industry Specification Group for QKD (ISG-QKD) has been particularly influential, producing technical reports and specifications that address QKD components, network architectures, and integration with classical cryptographic systems. Meanwhile, ITU-T has worked on standardizing QKD network architecture and key management interfaces, aiming to harmonize global deployment strategies. Despite this progress, several critical challenges remain.

First, interoperability between QKD systems from different vendors is still limited, hindering large-scale, multi-vendor deployments. Second, scalability remains a concern, especially in extending QKD beyond point-to-point links to complex, meshed networks. Third, cost and infrastructure requirements—including the need for dedicated optical fibers or trusted nodes—pose barriers to widespread adoption. Additionally, security certification and conformance testing for QKD systems are still evolving, with no universally accepted benchmarks for performance and resilience under real-world conditions. Finally, integrating QKD with existing security infrastructures and aligning it with emerging post-quantum cryptographic standards presents both technical and strategic challenges.

2.3 QKD and PQC

When it comes to distributing post-quantum keys for systems to use, there are two planned methods: QKD and PQC. QKD relies on the properties of quantum mechanics to exchange keys, making it almost impossible to eavesdrop, as any detection of interference will cause a new exchange to take place. Both technologies will coexist because there are widely different use cases where quantum-resistant cryptography technology will be needed.

QKD involves exchanging encryption keys via optical means (terrestrial fiber, free-space optics, or satellite link) using Qubits or Quantum Units of Information. This method guarantees that we will know if an eavesdropper intercepts the key used to encrypt the data, making it essentially tamper-proof because it exploits a fundamental principle of quantum mechanics, namely, particle entanglement (typically photons). Any attempt to interfere with the transmission generates a disturbance that is immediately detected by the communication protocol, causing the communication to stop instantaneously. In such cases, a new key can be sent before any sensitive data is transmitted.

QKD has a high cost because it is hardware-based, so its best uses are in highly sensitive applications where secrecy must be maintained under all circumstances. These applications involve parties in fixed locations, and cost is not the primary concern. The markets where QKD can be most effectively used are the government, military, and certain areas of financial services, where the costs of a failure could be catastrophic.

PQC, on the other hand, is a software-based approach that uses algorithms based on new mathematical problems to replace existing key algorithms (RSA, ECC, etc.), which can be vulnerable to QC attacks. It is not known whether these algorithms will be breakable, so it is not 100% guaranteed. However, it is a low-cost solution compared to QKD and is expected to become the dominant choice.

In summary, both QKD and PQC have their pros and cons. Therefore, co-existence scenarios of QKD and PQC, as well as classical security mechanisms, must be considered for real networks and validation systems.

	QKD	PQC
Equipment	Optical fiber with dedicated transceiver	Software replacement
Security methodology	Quantum mechanical security	Computational security
Pros	Impossible for sniffing	Easier upgrade by software
Cons	Short distance (up to around 100 km, Satellite-based QKD could solve), high cost	Not 100% secure, performance concern, need time for migration
Standardization	ITU-T (Y.3800/X.1700 series), ETSI	IETF, NIST
Use case example	National security, dedicated lines	Massive communication, internet banking, corporate sites

The reality is, the quantum-safe ecosystem is inherently fragmented, with proprietary QKD protocols, differing PQC implementations, and divergent key management systems. Yet, there is an essential and strategic need to strengthen the worldwide supply chain for these technologies and provide a heterogeneous approach to implementation.

Interoperability testing and validation frameworks are essential to reduce risks in integration and to speed up the development of the ecosystem and adherence to standards. They serve a public good that individual vendor labs cannot provide or are not motivated to offer.

2.4 Impacts on Industry

Post-quantum readiness impacts all industries—government, financial, healthcare, military, telecom, and more. All personal, financial, and government data must be encrypted during digital transfer. Once quantum computers are available, bad actors could use them anytime and anywhere on any systems, so the race to protect data begins now. Even before quantum computers arrive, the risk of HNDL exists, where data can be intercepted now and stored until quantum decryption becomes possible, allowing access to sensitive information.

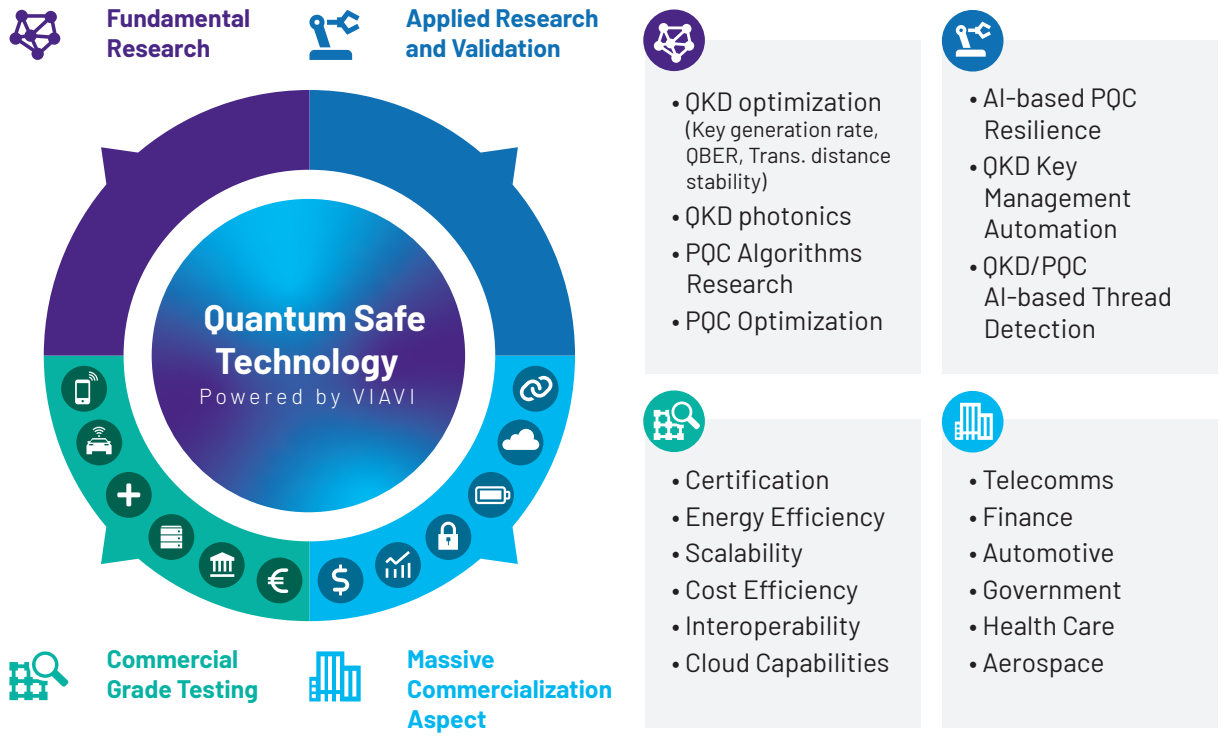
Each industry vertical manages its migration path to PQC separately but shares many common elements, such as the Migration Roadmap. For example, the Telecom governing body GSMA has published a report, *'Post Quantum Cryptography Guidelines for Telecom Use Cases.'* The Reserve Bank of India has released a white paper titled *'Securing the Indian Banking Sector in the Age of Quantum Computing.'*

However, there is a growing demand across all industries for a trusted validation platform that is essential for regulatory certifications, investor confidence, and cross-domain technology deployment. This platform should support a comprehensive hybrid environment and perform different validation scenarios, including (but no limited):

- Hybrid simulations combining PQC's scalability with QKD's information-theoretic security
- Layered testing from physical photon transmission to application-level handshake protocols
- HKMS testing for synchronization, fallback logic, prioritization, and key refresh behavior
- Chaos testing for hybrid resilience: assess continuity when QKD links fail or PQC degrades
- Digital Twin environments simulating hybrid classical-quantum networks across edge metro, cloud and satellite (including Non-Terrestrial Networks, or NTNs), free space optics and satellite-based QKD)
- Cost-performance benchmarking across deployment models: public vs private, core vs edge

3 QUANTUM SAFE TEST DOMAINS

Quantum safe networks are currently in a state of migration, creating the need for considering lifecycle management and a ramp to massive commercialization. VIAVI supports all the domains for testing:

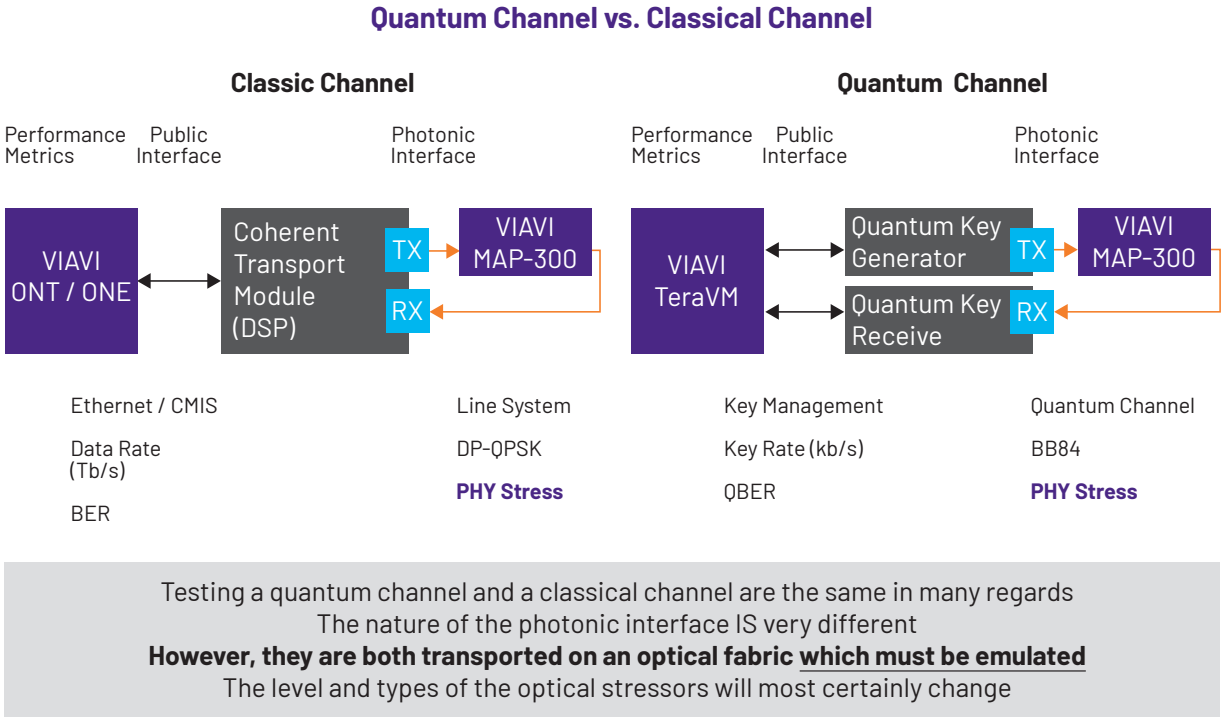


- Fundamental Research: QKD optimization, QKD photonics, PQC algorithms, PQC optimization, quantum security, quantum simulations
- Applied Research and Validation: QKD Key management automation, QKD/PQC AI-based Thread Detection, AI-based PQC resilience (including hybrid with non-PQC protocols), AI-based test automation for hybrid system
- Commercial Grade Testing: Certification, energy efficiency, scalability, cost efficiency, interoperability, cloud capabilities
- Massive Commercialization aspect/requirements: telecommunications, finance, automotive, government, health care, aerospace

This paper reviews, in context, each component of the VIAVI suite of products that support quantum safe testing:

Quantum Safe Network Function	VIAVI Product
Key Management System Test	TeraVM Security
PQC Performance Test	TeraVM Security, VAMOS, CyberFlood, TestCenter
QKD Quantum Channel Evaluation	MAP-300
Fiber Monitoring	ONMSi Remote Fiber Test
Fiber Sensing	FTH-DTSS
Network Observability	NITRO® AIOps, ONMSi
Fiber Infrastructure/Field Validation	OneAdvisor 800 INX 760
Operational Efficiency	NITRO AIOps
High-End Optics	Spectral Sensing Filters, Light Sensor Filters

The following figure shows the overall environment and where the VIAVI suite sits.



Testing a quantum channel and a classical channel are the same in many regards
The nature of the photonic interface IS very different
However, they are both transported on an optical fabric which must be emulated
The level and types of the optical stressors will most certainly change

1991.900.0725

3.1 Testing and Monitoring a QKD System

QKD systems have multiple fundamental test requirements. These include:

- QKD impairment by creating a flexible, reconfigurable photonic system that emulates a broad range of power and spectral loading scenarios representative of live production networks. This can be used to validate the performance or applicability of new QKD systems or subcomponents.
- Evaluating the resiliency of the QKD system based on types of fibers, magnitude and location of DWDM signals (if any), transient conditions as wavelengths are added or removed, and qualification of new optical devices in the P2P link (optical switches for example)
- Stress testing over P2P links to generate a range of controlled optical stress such as in-band/out-of-band noise from amplifiers, polarization disturbances from moving cables, dithers or stability from active optical elements (switches, attenuators, wavelength switches), single or multiple reflection events due to optical connectors.
- ETSI GS QKD 014 compliance testing towards service layer. The QKD Key Management System layer is tested for resiliency, i.e., on how efficiently it can service the L3 VPN Application layers with respect to retrieving Post-Quantum Pre-shared Keys (PPKs) for establishing IKEv2 (RFC8784) IPSec VPN Tunnel. This is more relevant when frequent key rotation of the VPN link is configured for advanced post-quantum security. TeraVM IKEv2 Client emulation has ETSI GS QKD 014 API support to fetch the PPKs from the KMS/QKD layer and can test QoE under load when keys are continuously rotated in a post-quantum safe IKEv2 VPN tunnel with PPK authentication.
- Physical attack testing against fiber cables such as temperature and strain and unauthorized evacuation works.

Quantum Channel Evaluation

Quantum channel evaluation in test environments measures how well a quantum communication link preserves qubit integrity under real or simulated conditions. This ensures that the channel supports secure quantum protocols before deployment. Quantum channel evaluation in test environments also involves characterizing the behavior of a quantum communication link, typically to assess its suitability for QKD or other quantum protocols.

The two major types of QKD are Discrete Variable QKD (DV-QKD) and Continuous Variable QKD (CV-QKD):

- DV-QKD: encodes information using discrete quantum states, such as polarization or discrete phases of photons, and requires precise clock synchronization for detecting photon arrival times. Protocols like BB84 and E91 fall into this category. Single-photon detectors (e.g., APDs, SNSPDs) are used.
- CV-QKD: uses continuous modulation of quadratures (amplitude and phase) of coherent laser light. Information is extracted through homodyne or heterodyne detection, often based on Gaussian modulation protocols like GG02. Less timing-sensitive but requires phase reference alignment (local oscillator calibration). Homodyne or heterodyne detectors (classical photodiodes) are used for detector.

DV-QKD offers higher security guarantees over long distances but involves complex hardware and lower key rates. CV-QKD is more practical for short-range, high-rate applications using standard telecom components. Testing approaches must account for their distinct physical and protocol characteristics, with special focus on noise, synchronization, and component calibration.

In test environments, the tools and methods for quantum channel evaluation include single-photon detectors, quantum light sources, OTDRs and other classic fiber tools, tomography tools, and simulators such as noise injection. Key measurements include Quantum Bit Error Rate (QBER), which measures the error rate of transmitted quantum bits (qubits). A high QBER may indicate noise or eavesdropping. Additional measurements include loss/attenuation (dB/km), coherence time/polarization stability, channel fidelity, and timing jitter and synchronization.

Tests include lab bench testing for short-range tests with optical tables and precision components; simulations across "real world" distances (10 km, 50 km, etc.); in field trials with installed fiber, and satellite or airborne tests (free-space optics).

For quantum safe, channel evaluation may focus on specific aspects, including:

- Side-Channel Attack Resistance: Testing ensures that quantum safe cryptographic implementations are not vulnerable to side-channel attacks, which exploit unintended information leaks such as power consumption or electromagnetic emissions
- Quantum safe Encryption Validation: Organizations evaluate quantum safe encryption methods to protect critical infrastructure from emerging threats
- Performance and Compatibility Testing: Quantum safe cryptographic solutions are tested for efficiency and integration with existing IT systems to ensure seamless transitions

These evaluations help prepare for the quantum era by ensuring their communication channels remain secure against future quantum-based cyber threats.

In general, test setups also undergo iterative optimization to reduce error sources like misalignment, temperature drift, and detector dark counts, with the goal of maximizing key rate while keeping QBER below a secure threshold (usually <11% for BB84 QKD).

VIAVI Solution: MAP-300

Quantum Testing requires labs that are comprised of switches, wavelength management tools, Erbium-Doped Fiber Amplifiers (EDFA), and attenuators to manage various quantum experimental conditions. QST will build networks for quantum techniques trials/evaluations. The VIAVI MAP-300 is a modular, dense, and easily reconfigurable Optical Test Platform with remote and automated capabilities. It effectively explores the limits of quantum in computing, networking, encryption, and cryptography.

MAP-300 supports QKD impairment by creating flexible, reconfigurable photonic system that emulates a broad range of power and spectral loading scenarios representative of live production networks. This can be used to validate the performance or applicability of new QKD systems or subcomponents. Research could also be performed to define (standardize even) on the matrix of conditions one needs to demonstrate that the QKD system can survive based on the following:

- Types of fibers
- Magnitude and location of DWDM signals (if any)
- Transient conditions as wavelengths are added or removed
- Qualification of new optical devices in the P2P link (optical switches for example)

The creation and insertion of all-optical elements in the QKD P2P link to generate a range of controlled optical stress.

- In-band and out of band noise from amplifiers
- Polarization disturbances from moving cables
- Dithers or stability from active optical elements (switches, attenuators, wavelength switches)
- Single or multiple reflection events due to optical connectors.
- Research on developing error correction mechanisms for QKD in different levels of noise and disturbances. Study on current techniques and development of better methodologies.

Fiber Monitoring

Fiber monitoring can play an important role in quantum safe communications by detecting potential physical layer attacks. For example, fiber tapping could compromise the security of QKD or other quantum safe protocols. QKD relies on the fundamental properties of quantum mechanics—specifically, that measuring a quantum system disturbs it. However, if an attacker physically taps the fiber, they might try to intercept signals without detection.

In the fiber tapping scenario, fiber monitoring helps detect anomalies like increased signal loss, backscatter, or time delays, alert the central office of unauthorized access attempts, and generally maintain the integrity of the physical transmission medium.

Fiber monitoring also enhances overall quantum safe security. Even when not using QKD, PQC algorithms rely on secure physical infrastructure. If someone can passively tap a fiber, they might collect encrypted data today and break it later with a quantum computer (HNDL). Fiber monitoring thus acts as a first line of defense, stopping passive eavesdropping and complementing quantum safe cryptography with physical layer security by ensuring the integrity and security of optical communication networks through:

- Quantum-secured encryption: fiber monitoring helps maintain secure data transmission by integrating QKD and PQC into optical networks. This ensures that sensitive information remains protected against quantum-era cyber threats.
- Ultra-secure quantum communication: researchers have successfully transmitted quantum information over long distances using fiber-optic networks, demonstrating the feasibility of quantum-secure messaging without requiring expensive cryogenic cooling.[1] This advancement enhances the security of financial transactions, healthcare data, and government communications.
- Low-latency fiber for quantum cryptography: some organizations are testing new fiber-optic technologies, such as hollow-core fiber, to improve the efficiency of quantum cryptography[2]. These innovations help extend the distance over which quantum-secure encryption can be applied, making it more practical for real-world deployment.

As with, and coupled with, fiber sensing, in quantum safe environments fiber monitoring can ensure secure and resilient communication networks.

[1] https://techblog.comsoc.org/2025/05/03/ultra-secure-quantum-messages-sent-a-record-distance-over-a-fiber-optic-network/?copilot_analytics_

[2] https://www.luxquanta.com/luxquanta-collaborates-in-test-of-low-latency-fibre-in-data-centers-led-by-lyntia-n-71-en?copilot_analytics_

VIAVI Solution: ONMSi Remote Fiber Test System (RFTS) with Fiber Test Heads (FTH)

ONMSi is an optical network monitoring system that expands network visibility right from the core across the PON and into the premises—improving operational support and quality-of-service (QoS) for any type of network. ONMSi is a remote fiber test system that scans the fiber network 24/7 and automatically detects and locates faults without having to dispatch technicians in the field. Based on industry-leading VIAVI optical technologies, Fiber Test Heads (FTHs) integrating an optical time domain reflectometer (OTDR) and an optical switch constantly compares data to a baseline and sends alarms if any fiber degradation occurs.

Fiber Sensing

Fiber sensing can enhance quantum safe communications by acting as a real-time intrusion detection system for the physical layer of a quantum or post-quantum secure network. In the simplest terms, fiber sensing turns optical fibers into distributed sensors by analyzing how light reflects or scatters along the fiber. This can be performed through Rayleigh scattering (for vibration or acoustic sensing), Brillouin scattering (for strain and temperature), and Raman scattering (for temperature profiling), all of which can detect even tiny changes over long distances.

Fiber sensing supports quantum safe security by offering:

- Tamper Detection for QKD Links: QKD assumes that physical intrusion will disturb the quantum state. Fiber sensing adds another layer by detecting attempts to tap, bend, or cut the fiber before any significant compromise. For example, if someone tries to bend the fiber to siphon photons, fiber sensing can detect strain or vibration and trigger alerts.
- Monitoring for Delayed Eavesdropping: in PQC, attackers might tap fibers now and store encrypted data to decrypt it later with a quantum computer. Fiber sensing detects this kind of passive eavesdropping, making it harder for attackers to remain undetected.
- Enhanced Situational Awareness: fiber sensing can detect vibrations, environmental disturbances, and unauthorized construction, which might threaten critical quantum safe infrastructure. It provides a security perimeter, especially for underground or exposed fiber runs.

Fiber sensing strengthens quantum safe systems by providing early warnings of physical attacks and complementing quantum cryptography with real-time, distributed monitoring, protecting both QKD and PQC from physical-layer vulnerabilities. It can serve a crucial role in quantum safe environments by enabling secure and precise measurements while maintaining data integrity against potential threats. For example, by providing secure quantum remote sensing (SQRS) over long distances (i.e., 50 km of optical fiber) without relying on entanglement, or through fiber-based quantum sensing for environmental monitoring, disaster response, and military surveillance, ensuring that transmitted data remains confidential and resistant to eavesdropping.

These advancements highlight the growing potential of fiber sensing in quantum-secure applications, paving the way for more resilient and scalable quantum technologies.

VIAVI Solution: FTH-DTSS

VIAVI Fiber Test Head Distributed Temperature and Strain Sensing (FTH-DTSS) monitors temperature and strain of power cables, pipelines and telecom cables with the most versatile optical fiber sensing solutions on the market. The FTH-DTSS, part of the NITRO Fiber Sensing solution, provides continuous monitoring of fiber cables and fiber-enabled assets. This utilizes fiber optic cables to provide continuous and real-time information about temperature and strain exerted by the environment in and around your assets, with immediate detection and localization. Some of the capabilities of FTH-DTSS are:

- Designed for industries that demand high precision and reliability, our innovative technology delivers Distributed Temperature and Strain Sensing (DTSS) for absolute measurements of temperature and strain along extensive lengths of fiber optic cable, making it an indispensable tool for numerous applications
- Capable of detecting anomalies in diverse applications such as critical infrastructure (power utilities), pipelines (oil, gas, water, etc.), telecom networks (Data Center Interconnects – DCI) and beyond
- Proactive monitoring tracks changes in temperature and strain, information which can be used to improve operational efficiency and responsiveness and allow for preemptive/proactive actions to be taken to mitigate potential damage or outages

3.2 Testing PQC Performance

When it comes to migrating existing encryption algorithms to post-quantum algorithms one thing being highlighted is the effect of much longer encryption keys. Furthermore, adopting PQC across various components of a mobile system may introduce performance and architectural impacts, particularly on user terminals where wireless bandwidth is limited. It is essential to thoroughly test both Terrestrial Networks (TN) and NTNs under PQC-enabled configurations. Here are just some of the concerns being voiced from the telecom industry:

Company	PQC Migration Concern
SKT	Developing quantum cryptography network integration technologies such as Q-SDN and QKDN Federation to enable integrated operation and control of quantum cryptography networks between different manufacturers' equipment, between operators, and between countries.
Vodafone	Vodafone and IBM have announced a collaboration to integrate IBM Quantum Safe technology into Vodafone Secure Net, the company's all-in-one digital security service. The proof of concept aims to protect smartphone users from future quantum computing threats by implementing PQC standards.
Softbank	When cryptographic protocols are deployed in data transmission infrastructure, they can place a significant load on communications and cause latency problems, resulting in poor quality and lower throughput.

Company	PQC Migration Concern
5G Americas	Potential performance and interoperability issues are anticipated, which will require thorough testing.
Indian Ministry dept. of Telecomms	As new PQC algorithms are operationally heavy, they may impact the organization's key operations. It is essential to continuously test new products or updated products and monitor their performances.
GSMA Guidelines for Telecom	It is imperative that deployments enter a testing phase to assess the viability of certain post-quantum cryptography algorithms to minimize the performance impact.
Reserve Bank of India	Some factors of concern include performance overhead and complex implementations suggesting extensive testing.
BIS	New cryptographic implementations must bethoroughly tested to ensure they function correctly within existing infrastructure, maintain performance levels, and do not compromise system integrity.

PQC Testing

The implementation of PQC protocols introduces additional network performance overhead, impacting end-user experience. Testing is essential for developing and deploying cryptographic systems, including PQC-based systems. PQC aims to create secure algorithms against quantum computer threats. Testing assists in several key areas for PQC:

- *Security Assurance*
  - Algorithm Resistance Testing verifies PQC algorithms' resistance against cryptographic attacks. This includes testing the algorithms under different scenarios, including those that utilize classical and quantum algorithms, to evaluate their resilience.
- *Performance Evaluation*
  - Computational Efficiency Testing evaluates PQC algorithms' computational efficiency. This includes measuring encryption/decryption speed, key generation speed, and overall system performance. Ensuring the efficiency of PQC algorithms is crucial for widespread adoption in practical applications.
- *Interoperability Testing*
  - Integration with Existing Systems: Cryptographic systems often require interaction with established infrastructure and protocols. Testing is essential to guarantee the seamless integration of PQC algorithms into diverse systems, avoiding compatibility issues.
- *Standardization Compliance*
  - Adherence to Standards: This testing confirms PQC algorithms' compliance with established cryptographic standards, promoting interoperability and consistent implementation across platforms.

VIAVI can also leverage a long history of VPN test experience that we will adopt to test PQC algorithms aimed at preventing the risk of 'store now, decrypt later' by bad actors. This includes:

- Post-Quantum (PQ) VPN Hybrid Testing: test IKEv2 peering with hybrid keys
  - Test PQ VPN Hybrid for initiator but not responder: ensure a classic IKEv2 tunnel is established if both parties don't support PQ VPN keys
  - Test Mismatched PQC KEM selections: test should fail if negotiation cannot find a matching cipher between initiator and responder
  - Stress Test PQ VPN Tunnel: transfer large data files between two PQC supporting sites over a long period to ensure file transmissions are complete on both sides
- IPSec VPN PQC Algorithm support:
  - NIST standardized KEM algorithms as well as several post-quantum algorithms are supported

VIAVI Solution: TeraVM Security

The best way to ensure systems are ready for PQC and will remain unaffected from a performance viewpoint is test. This is where VIAVI TeraVM comes in.

TeraVM is a software test tool which has been testing VPN performance for more than 20 years by emulating users and traffic and stressing VPN headends to their limits to measure the performance of the users while the VPN processes traffic and filters out malware. Expanding VPN test to PQC test is a simple extension to the existing software tool by encrypting the VPN tunnel with PQC-standardized algorithms. This would mean additional KPIs need to be measured such as: key size variations, re-keying rounds, hybrid keys, etc.

Many enterprise IT departments test a new feature before rolling it out company-wide. This could involve a small group of test personnel who log in from around the world to test the new feature. While this approach works for most upgrades and bug fixes, it falls short for changes involving additional compute overhead. In the U.S. alone, there are over 10,000 enterprises with more than 1,000 employees, making it essential to conduct a scale test to ensure a smooth transition to PQC.

TeraVM can emulate tens of thousands of employees and their location (remote, VPN, onsite, managed device, and more), then emulate their office traffic such as collaboration tools, video conferences, private application access and more. TeraVM can run traffic with increasing amounts of employees, simultaneously monitoring KPIs such as latency, throughput and MoS scores – ensuring confidence to launch live.

VIAVI Solution: CyberFlood Security and Performance Solutions

CyberFlood is a comprehensive, automated security and performance testing platform designed to validate how networks, applications, and devices behave under real world conditions. It enables teams to easily generate multiple 100s of Gbps of realistic traffic, emulate sophisticated cyberattacks, and assess system resilience and security efficacy at scale, helping organizations ensure that their infrastructure, services, and security controls can deliver reliable performance and robust protection in today's rapidly evolving threat landscape.

As organizations prepare their security infrastructures for PQC, they must validate not only the correctness of new cipher implementations, but also the impact of these algorithms on security inspection, interoperability, and overall network performance. This is where CyberFlood plays an important role.

CyberFlood provides advanced scale and performance testing for PQC-enabled environments, helping security teams assess how quantum-safe encryption affects firewalls, proxies, and other inspection-based security controls in pre-deployment settings. Because PQC algorithms often introduce larger key sizes and more computationally intensive processing, security infrastructure can experience added latency, reduced throughput, and increased hardware strain. CyberFlood helps organizations quantify these effects before live deployment.

CyberFlood supports testing of PQC cipher suites aligned with current NIST standards, including FIPS 203 key encapsulation mechanisms and FIPS 204 digital signatures. It also enables hybrid KEM testing, including validation of fallback behavior when PQC-capable systems interact with systems that do not fully support quantum-safe handshakes. This is essential for identifying interoperability issues and ensuring secure communications continue with minimal disruption during migration.

By integrating PQC cipher suites into realistic HTTP protocol traffic, applications, and threat emulations, CyberFlood allows security teams to validate quantum-safe deployments under production-like conditions. This helps confirm that inspection policies remain effective while encrypted traffic volumes, application sessions, and mixed cipher environments scale. CyberFlood is particularly valuable for testing man-in-the-middle inspection scenarios, where the burden of decrypting and analyzing PQC-protected traffic may significantly affect firewall and gateway performance.

With CyberFlood, organizations can:

- Validate security controls, performance, and interoperability across encrypted PQC traffic flows
- Assess firewall and inspection-system behavior under the added load of quantum-safe encryption
- Verify hybrid fallback mechanisms for communication with legacy or non-PQC-enabled systems
- Identify infrastructure gaps early to reduce migration risk, avoid unnecessary cost, and improve upgrade planning
- Gain the confidence needed to future-proof security operations against quantum-era threats

VIAVI Solution: TestCenter

TestCenter is a comprehensive, end to end network and cloud validation platform engineered to help service providers, data centers, and equipment vendors verify performance, reliability, and scalability across evolving architectures. Designed as a unified Layer 2–3 test environment, it delivers high capacity traffic generation, extensive protocol emulation, and real time analytics to support everything from traditional Ethernet validation to next generation AI data center fabrics. TestCenter's flexible portfolio, spanning hardware appliances, high speed Ethernet test modules, virtualized test environments, and AI scale workload emulation, enables customers to accelerate development cycles, optimize configurations, and ensure readiness for demanding multi vendor, high speed network deployments.

As networks evolve toward quantum resilient architectures, TestCenter provides a powerful and extensible foundation for validating next generation PQC capable network fabrics. TestCenter's unified Layer 2–3 design delivers high capacity traffic generation, deterministic measurements, and extensive protocol emulation, capabilities already trusted across service providers, hyperscalers, and cloud operators to validate high speed Ethernet environments at massive scale. With support for multi rate operation across rapidly evolving network designs, including high speed interfaces extending from 10G to 1.6T, TestCenter enables full scale stress and performance validation for fabrics preparing to carry the heavier payloads, cryptographic metadata, and latency sensitive exchange patterns introduced by PQC enhanced protocols.

As organizations modernize switching fabrics and cloud backbones to accommodate AI workloads and secure them against future quantum threats, TestCenter's proven strengths, such as massive traffic scalability, comprehensive protocol coverage, and real time analytics, are essential for verifying the resilience of these upgraded infrastructures. The platform's ability to emulate high density traffic patterns, validate interoperability across multi vendor environments, and assess network readiness under extreme load conditions provides a critical foundation for ensuring PQC algorithms can be deployed without compromising throughput or reliability. The same capabilities that support next generation AI data center validation, such as multi rate testing, congestion analysis, and workload emulation, translate directly into the performance baselines needed to evaluate PQC augmented transport, handshake, and key exchange mechanisms on high speed Ethernet fabrics.

By combining deterministic high performance traffic modeling with flexible hardware and virtual test environments, TestCenter enables engineering teams to accelerate their migration toward quantum safe network designs. TestCenter offers a future proof validation framework that helps ensure that high speed, cloud scale, and AI centric infrastructures remain reliable, interoperable, and secure in the quantum era.

VIAVI Automation Management and Orchestration System (VAMOS)

VAMOS is a unified, cloud-based platform that automates test campaigns, cases, and executions for VIAVI wireless testing products including TeraVM security. With customizable workspaces and configurations, VAMOS streamlines the entire testing workflow, enhancing resource utilization across teams and lab locations.

Shared tool testbeds and individual sandboxes support a wide range of testing needs, while robust analytics and reporting capabilities improve test precision and reliability.

By integrating AI, ML, and Lab-as-a-Service (LaaS), VAMOS significantly reduces operational costs—minimizing manual effort and accelerating fault analysis. The result: faster time to market, improved quality, and tighter control over budgets. Key benefits are shown below.

Reduce Operational Expenses

- Cut man hours through intelligent automation
- Accelerate time to market with optimized workflows
- Improve quality of service with precise and consistent testing

Maximize Lab Efficiency and Effectiveness

- Zero-touch automation for end-to-end test execution
- AI/ML-driven insights to shorten response times and amplify engineering expertise

Enable Test Execution Anywhere

- Global scheduling layer balances resources across lab locations
- Cost-optimized testing through location-independent execution
- Open, tool-agnostic automation frameworks with ready-to-use scheduling capabilities

Ensure Best-in-Class Tool Utilization

- Advanced tool selection and slip-through analysis to detect field-level issues
- Prioritize tools and processes that identify real problems early in the cycle

Leverage Hardware/Software Disaggregation on COTS Platforms

- Shared compute resources for diverse test scenarios
- Dynamic software tool provisioning in disposable, on-demand sandboxes
- Preference for pure software tools with flexible hardware plug-ins, replacing rigid appliances

3.3 Testing Hybrid Systems

Hybrid systems in quantum networks integrate classical networking components with quantum technologies like QKD, quantum repeaters, and PQC. Testing these systems requires a multi-dimensional approach involving functionality, performance, security, and environmental factors:

Migration Testing in Testbeds
Goal: Emulate migration scenarios required by service providers.

- Co-existence scenario of QKD, PQC and Classical security methods
- Fallback scenarios among QKD, PQC and Classical security methods

Functional Testing
Goal: Ensure classical and quantum components work together as intended.

- Quantum-Classical Interface Testing: validate timing and synchronization between quantum signals and classical systems; test QKD control protocols
- Protocol Stack Validation: ensure integration of QKD with IPsec, TLS, or PQC

Performance Testing
Goal: Measure and optimize throughput, latency, error rates, the number of sessions, and the session establishment time.

- Key Metrics: Quantum Bit Error Rate (QBER); secure key rate (bps); latency and jitter, number of sessions, session establishment time
- Use Case: measure secure key generation and consumption in hybrid encryption scenarios

Security Testing
Goal: Validate quantum safe and hybrid cryptography resilience.

- Simulate attacks like PNS, man-in-the-middle, and side-channel
- Verify secure fallback to PQC
- Test entropy quality of Quantum Random Number Generators (QRNG)

Environmental and Physical Layer Testing
Goal: Ensure robust performance under real-world conditions.

- Fiber testing for loss, dispersion, polarization effects
- Coexistence of quantum and classical traffic in DWDM
- Atmospheric testing for free-space optics (e.g., satellite links)

Integration Testing in Testbeds
Goal: Emulate production-like environments.

- Combine live fiber links with emulated quantum nodes
- Deploy in national or private quantum testbeds

AIOps and Monitoring Integration

Goal: Use AI/ML to monitor and adapt hybrid networks

- Analyze both classical and quantum metrics in real-time
- Use anomaly detection for tampering or degradation
- Real-time visualization and alarms for hybrid link health

Test Area	Classical Component	Quantum Component	Tools/Approaches
Migration	Combination of below components	Combination of below components	Combination of below components
Functional	Network stack, routing	QKD, QRNG	Protocol analyzers, QKD consoles
Performance	Bandwidth, jitter	QBER, key generation rate	Fiber testers, NetSquid, QuISP
Security	Firewall, VPN, PQC	Quantum attack simulations	Pen-testing, side-channel tools
Physical Layer	DWDM, fiber, RF	Photon transmission	OTDR, fiber sensing, polarization tools
Integration and Monitoring	Orchestration, AIOps	Key usage, fault detection	NMS, AIOps dashboards, VIAVI NITRO

By utilizing VIAVI test solutions provided in previous sections, several hybrid scenarios including migration can be tested.

3.4 KMS Interoperability Testing

A crucial new focus area is Key Management System (KMS) interoperability, which bridges the cryptographic control plane across QKD, PQC, and hybrid environments.

A key management system must exchange keys between disparate cryptographic domains (optical, lattice-based, or hybrid), interface with multiple standards (such as ETSI GS QKD 014, ITU-T Y.3805, and IETF draft KEMTLS), and operate across various vendors and protocols, ensuring consistent key lifetimes, rotation intervals, and distribution paths.

These factors mean that KMS interoperability requires the following evaluation, testing and validation:

- Cross-vendor compliance validation: verifying adherence to standards and ensuring consistent behavior under mixed vendor implementations.
- Resilience testing: simulating key delivery delays, corruption, or loss and verifying that applications automatically request new keys or revert to PQC.
- Scalability evaluation: ensuring the KMS can handle large-scale key distribution (e.g., millions of secure sessions) with deterministic latency and zero key collision.
- Security Testing: validating the secure handshake and authentication mechanisms between QKD nodes, KMS servers, and client applications, ensuring protection against replay or man-in-the-middle attacks.

4 ADDITIONAL CONSIDERATIONS

AIOps

Artificial Intelligence for IT Operations (AIOps) is already being applied in quantum safe environments to enhance security, automate threat detection, and optimize data transfer. It can enhance quantum safe security by proactively managing and securing the infrastructure that supports quantum and post-quantum cryptographic systems. AIOps is constantly evolving, but at the foundational level it provides multiple advantages:

1. Threat detection and anomaly response: quantum safe systems rely not just on cryptography, but also on secure and stable operations. AIOps can detect unusual behavior in data flows that might indicate eavesdropping, fiber tapping, or man-in-the-middle attacks. It can also analyze logs from QKD systems, detecting anomalies including spikes in Quantum Bit Error Rate (QBER), unexpected signal attenuation, and suspicious device re-authentications. AIOps does this by using machine learning models trained on normal operational behavior, helping flag outliers quickly.

2. Automated infrastructure monitoring: quantum safe systems often require low-latency, stable environments. AIOps helps maintain this by monitoring latency, jitter, and packet loss on quantum or hybrid networks; optimizing routing or switching based on real-time AI insights; and automatically responding to degradations that could affect quantum key exchanges or post-quantum encryption protocols.

3. Adaptive security posture: quantum safe implementations may involve hybrid systems (classic + quantum/post-quantum crypto). AIOps can dynamically adjust encryption strength or protocol use based on perceived threat level and then recommend quantum safe algorithm rollouts based on observed system performance and risk levels.

4. Cryptographic drift and compliance management: AIOps can track the use of legacy or non-compliant cryptographic libraries and therefore detect and flag the use of non-quantum safe algorithms (like RSA or ECC), then suggest automated replacements using PQC libraries (e.g., CRYSTALS-Kyber, Falcon).

Several key applications for AIOps exist in quantum safe environments, not the least of which is threat detection and response by monitoring network traffic for malicious activity, detecting potential quantum-era cyber threats before they can compromise sensitive data. It may also be used to assess cryptographic infrastructure and automate the transition to post-quantum cryptographic standards (thus ensuring long-term security).

In summary, AIOps enhances quantum safe systems by detecting threats and anomalies across the stack, ensuring operational integrity for QKD or PQC deployments, enabling dynamic defense, including automated encryption adjustments, and monitoring compliance with quantum safe standards.

VIAVI Solution: NITRO® AIOps

VIAVI offers NITRO AIOps, an advanced, end-to-end, top-down intelligent engine that serves as an umbrella solution that seamlessly integrates across multi-vendor, multi-technology, and multi-domain environments. The AI-driven capabilities of NITRO AIOps offer a unique opportunity to simplify NOC complexity and streamline operations. NITRO AIOps provides many benefits, including:

- TCO Reduction: Utilizing AI and predictive maintenance, NITRO AIOps effectively mitigates costly downtimes. Advanced AIOps capabilities in resource allocation, capacity planning, and optimization further enhance cost control, promoting sustainable network operations even in the most complex scenarios.
- OpEx Reduction: NITRO AIOps elevates network management, troubleshooting, and service assurance through automation, unlocking the full potential of zero-touch operations and enhancing operational efficiency.
- Digital Transformation — 5G Monetization: NITRO AIOps enables network digital transformation with real-time analytics and predictive maintenance, identifying issues before they impact users. Its self-healing capabilities optimize performance, ensuring a seamless user experience even during peak loads.

Field Testing Fiber in Quantum Networks

Fiber field testing is critically important in quantum networks because these networks rely on the extremely fragile quantum states for communication. Even minor imperfections or inconsistencies in the fiber infrastructure can disrupt or completely destroy the quantum signal.

Quantum safe networks over fiber are highly sensitive to physical layer conditions and depend on high fiber quality. Field testing ensures fiber supports secure quantum key exchange.

In hybrid networks, many quantum safe deployments will use existing telecom fiber, alongside classical data. Field testing verifies that fibers can handle both quantum and classical traffic, can operate securely without noise or interference, and that fibers comply with quantum safe deployment requirements.

Fiber field testing is therefore essential to quantum safe networking (especially QKD) because it ensures signal integrity for quantum key transmission, helps maintain low error rates critical to security, and detects vulnerabilities that could compromise quantum-proof encryption.

VIAVI Solution: OneAdvisor 800

The VIAVI OneAdvisor 800 is designed to simplify the evolving network test needs that are required to maintain a wide variety of wireline and wireless networks. The modular design of OneAdvisor 800 allows network technicians to easily switch between a multitude of test scenarios broadly grouped into three categories: wireless, transport, and fiber.

OneAdvisor 800 offers an intuitive touch gesture control user interface with assistant apps to guide techs through instrument usage; a wide range of modules and performance to match any network applications with fast, error-free testing; the ability to turn up and verify any new WDM service with confidence (CWDM, DWDM, MWDM, LWDM) and meet future requirements for high-speed service activation, OSA plus Ethernet/BERT test. Consolidated reporting reduces volume of test results to manage by 50%.

Fiber test capabilities include optical connector inspection, OTDR and PON-OTDR, FiberComplete PRO™ Bi-directional IL/ORL and OTDR (TruBIDIR), DWDM OTDR, optical spectral testing, and advanced dispersion testing for submarine cables qualification and troubleshooting, high speed DWDM terrestrial transport networks, Radio Access network for 4G/5G - Backhaul, midhaul and frontaul, data center, data center campus and interconnect (DCI) testing, FTTH/PON network testing (any standard, unbalanced/tapped or indexed topologies), DWDM access networks for DAA, R-PHY and C-RAN, and Enterprise/LAN.

For Transport testing, OneAdvisor 800 offers several benefits:

- **Conveniently Portable.** One of the smallest 400G/800G test devices available
- **Unmatched Cooling.** Best in class for 400G/800G portables – easy to cool ZR pluggables
- **Superior Battery Life.** Scalable to multiple batteries which enables hours of unconnected use
- **Broad Test Coverage.** Modularity delivers all-in-one solution across lines rates and protocols
- **Flexible.** Tests fiber (OTDR, OSA) and all Ethernet rates (800, 400, 200, 100, 50, 40, 25, 10, and 1)
- **Multiple Optics Support**. QSFP-DD800/QSFP-DD/QSFPx, OSFP800/OSFP, SFP-DD/SFPx enabled, and full coherent optic support

VIAVI Solution: INX™ 760

The INX 760 is the ultimate tool for field technicians, offering unparalleled efficiency in ensuring pristine fiber connections. As the culmination of over 25 years of pioneering innovation and expertise, it stands as the apex of next-generation fiber end face inspection and analysis. While fiber inspection has become a standard practice for many field technicians, contamination continues to be the #1 cause of optical network problems. With new connector types emerging, greater connector volumes used in the field, and an increase in new fiber technicians, the industry has reached an inflection point.

Optical Security and Performance

While this paper provides an overview of quantum network challenges and related VIAVI test solutions, VIAVI also provides industry-leading and unique optical coatings for quantum networks, including **Spectral Sensing Filters** and **Light Sensor Filters**. Founded in 1948 as Optical Coating Laboratory (OCLI), the VIAVI Optical Security and Performance (OSP) business has been the innovation leader in custom optics for 75 years. As a trusted advisor and long-term partner in the advancement of high-performance optics, we deliver premium solutions and an unparalleled customer-service experience. With strong roots in engineering, research, and applied knowledge, no other supplier can match VIAVI in meeting your optical challenges – simple or complex. From prototype to production, our expertise, technology, and processes give customers a competitive advantage.

OSP filter technology helps customers extract optical signals with the least amount of disruption and highest amount of fidelity possible, engineering surfaces with the highest precision available, at any required scale.

5 SUMMARY

As quantum computing advances, traditional encryption methods face increasing vulnerability. To address this, VIAVI has developed the TeraVM Security Test, a pioneering cloud-enabled platform designed to evaluate PQC implementations. This solution supports algorithms mandated by the U.S. NIST and assists organizations in transitioning to quantum-resistant security frameworks. Furthermore, VIAVI provides MAP-300 for quantum channel evaluation, ONMSi and FTH-DTSS for fiber monitoring and sensing, and a complete range of field testers for fiber network installation, troubleshooting,and maintenance.

Contact Us: +1 844 GO VIAVI | (+1 844 468 4284). To reach the VIAVI office nearest you, visit viavisolutions.com/contact

futureproofcomms-quantum-an-xpf-nse-ae
30194547 901 0426