VIAVI Solutions

Für eine zukunftssichere Kommunikation: die Entwicklung quantensicherer Technologien

Eine Untersuchung der Sicherheitsrahmen und Validierungstools, die die Unternehmen in die Lage versetzen, Quantenalgorithmen und Quantenarchitekturen von theoretischen Modellen und Laborumgebungen in sichere und praktische Anwendungen zu überführen.

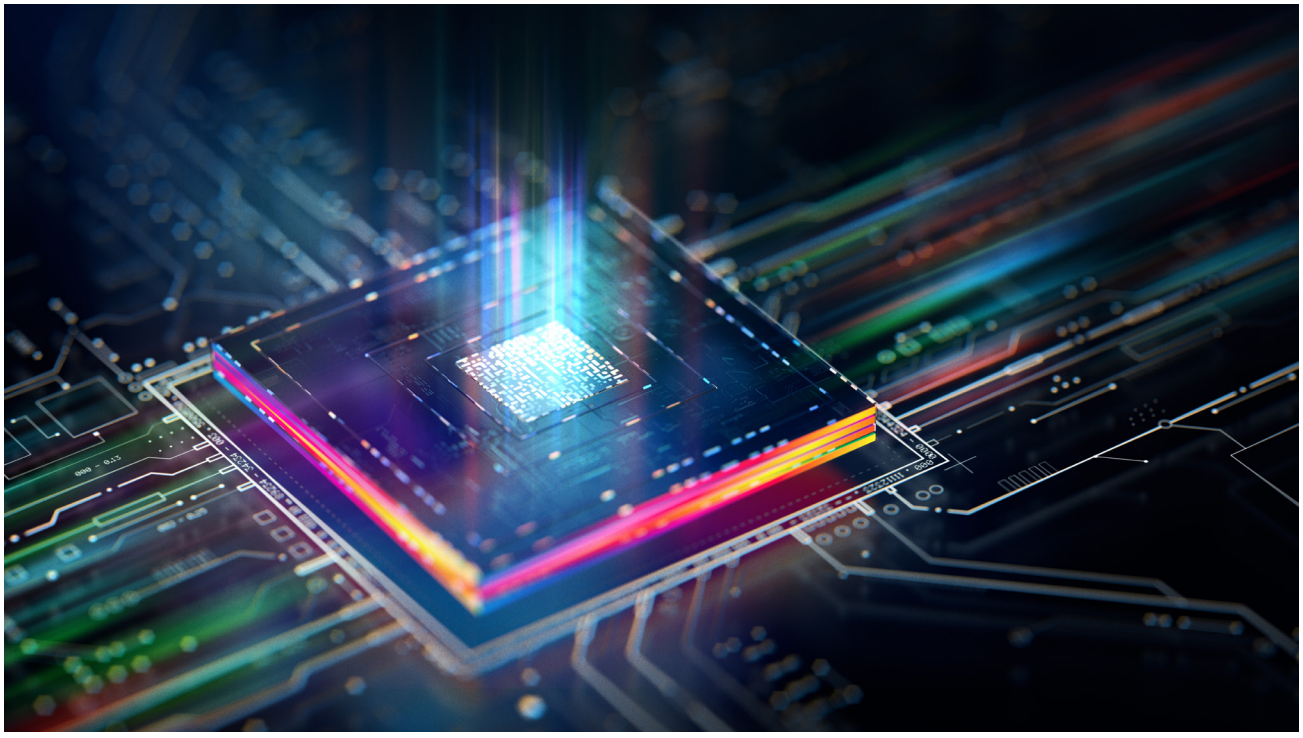
INHALTSVERZEICHNIS

Die quantensichere Kommunikation ist kein fernes Ziel, sondern ein aktuelles Anliegen. Ein Ökosystem unterschiedlicher Technologien, darunter die Quanten-Schlüsselverteilung (QKD), die Post-Quanten-Kryptographie (PQC), hybride Ende-zu-Ende QKD/PQC-Modelle, satellitenbasiertes Kryptographie- und Schlüsselmanagement sowie Übergangsarchitekturen, die klassische und quantensichere Systeme miteinander kombinieren, treibt diesen Prozess voran. Angesichts des disruptiven Potenzials der Quantencomputer verändern diese Innovationen unser Verständnis von sicherer Kommunikation.

Vor dem Hintergrund dieser sich immer weiter entwickelnden Technologien muss gewährleistet bleiben, dass bereitgestellte Architekturen und Systeme mit maximaler Resilienz, Sicherheit, Effizienz und praxisnaher Zuverlässigkeit betrieben werden können. Das ist insbesondere auf der optischen Schicht, auf der die Quanten-Technologie auf die physische Infrastruktur trifft, von Bedeutung. In vielen Fällen besteht die Herausforderung darin, die Quanten-Wissenschaft, insbesondere die Quantenoptik, aus dem Experimentalstadium in zuverlässige und feldtaugliche Lösungen zu überführen.

Bei diesem Übergang spielen Standards und Konformität eine wichtige Rolle. Ebenfalls wichtig ist jedoch ein tiefgehendes Verständnis für die Infrastruktur, vor allem der optischen Systeme als Grundlage der Quantenübertragung. Die Optik ist nicht einfach eine beliebige Komponente, sondern ein Eckpfeiler der quantensicheren Kommunikation.

Daher sind vertrauenswürdige Partner, die sowohl Quanten-Innovationen als auch eine tiefgehende Glasfaser-Kompetenz besitzen, eine Voraussetzung für den Erfolg. Diese Anwendungsbeschreibung untersucht die wichtigsten Faktoren, die bei der großflächigen Bereitstellung quantensicherer Technologien zu beachten sind. Hier ist VIAVI hervorragend positioniert, da wir unsere seit Jahrzehnten bestehende Führungsposition in der Glasfasertechnologie mit fortgeschrittener Quantenforschung verbinden. Mit mehr als 30 Jahren Erfahrung auf dem Gebiet der Systeme, Physik und Laborvalidierung bietet VIAVI einzigartige Einblicke in die Anforderungen der sicheren und effizienten Überführung der photonenbasierten Kommunikation aus dem Labor in die Praxis.



1 EINFÜHRUNG

Der erwartete explosionsartige Anstieg des Potentials der Quantencomputer wird die digitale Sicherheitslandschaft neu definieren. Da Quantenprozessoren sich ihrer praktischen Umsetzung nähern, sind die kryptographischen Grundlagen, die die heutigen Kommunikationsverbindungen, Finanzsysteme und digitalen Identitäten schützen, einer existentiellen Bedrohung ausgesetzt. Dieser drohende Meilenstein, der häufig als „Q-Day" bezeichnet wird, kennzeichnet den Punkt, an dem Quantencomputer in der Lage sein werden, weit verbreitete, auf öffentlichen Schlüsseln basierende Verschlüsselungsverfahren, wie RSA und die elliptische Kurven-Kryptographie (ECC), zu brechen. Damit wäre es jedoch möglich, einen Großteil der weltweiten verschlüsselten Daten zu entschlüsseln.

Auch wenn der Q-Day noch nicht da ist, besteht ein dringender Handlungsbedarf. Denn die heute abgeschöpften Daten könnten morgen entschlüsselt werden. Diese Bedrohung wird als „Harvest Now, Decrypt Later" (HNDL) bezeichnet. Daher intensivieren Regierungen, Standardisierungsgremien und Unternehmen ihre Anstrengungen zur Einführung quantensicherer Technologien, die der Rechenleistung der Quantencomputer die Stirn bieten können.

Bei dieser Entwicklung spielt das Testen der Standards und Konformität eine wichtige Rolle. Ohne eine strenge Validierung besteht das Risiko, dass selbst die vielversprechendsten quantensicheren Lösungen in der Praxis nicht bestehen. Aspekte der Infrastruktur, insbesondere wenn es um Glasfasern, die photonische Übertragung und die Sicherung der Signalintegrität geht, müssen sorgfältig geprüft werden.

Jedoch ist der Übergang von der Theorie zur Praxis ein komplexes Unterfangen. Quantensichere Technologien müssen nicht einfach nur sicher, sondern auch interoperabel, resilient, migrierbar und unter den praktischen Einsatzbedingungen funktionsfähig sein. Das gilt insbesondere für die optische Schicht, auf der die Quantensignale ausgesendet und empfangen werden, sowie für die Schicht der Post-Quanten-Schlüsselverschlüsselung. In vielerlei Hinsicht besteht die Herausforderung darin, die Quantentechnologien, insbesondere die Quantenoptik, aus dem Labor in das Feld, also aus dem Stadium der wissenschaftlichen Experimente in funktionsfähige Systeme zu überführen.

Genau hier ist VIAVI mit seiner führenden Kompetenz unverzichtbar. Seit mehr als 30 Jahren nimmt VIAVI eine Führungsposition auf den Gebieten der Glasfasertechnologie, der Systemtechnik und der Laborvalidierung ein und ist daher hervorragend positioniert, um den Quantenübergang zu unterstützen. Das angebotene quantensichere Testpaket stellt eine umfassende Plattform zur Bewertung der Funktionalität, Konformität, Leistung und Resilienz quantenresistenter Technologien zur Verfügung. Unabhängig davon, ob die Lösungen von VIAVI in bestehende Infrastrukturen integriert oder in Prüfständen eingesetzt werden, versetzen sie die Anwender in die Lage, quantensichere Systeme zuverlässig zu bewerten und bereitzustellen.

Diese Anwendungsbeschreibung untersucht die sich rasant entwickelnde Landschaft der quantensicheren Kommunikation, die sie vorantreibenden Technologien und die entscheidende Rolle der Testausführung und Validierung zur Gewährleistung des sicheren und nahtlosen Übergangs in eine Post-Quanten-Welt.

2 QUANTENSICHERE NETZWERKE

2.1 Notwendigkeit

Die digitale Verschlüsselung ist eine kritische Komponente eines jeden drahtlosen Kommunikationssystems, wie der Mobilfunktelefonie. Lauscher können Gespräche mithören und versuchen, Daten zu abzuschöpfen, wobei diese Bedrohung durch die Verschlüsselung der Daten gemindert wird. Vor dem Hintergrund der Entwicklung von Quantencomputern besteht bei unseren modernen Verschlüsselungsverfahren jedoch die Gefahr, dass sie gebrochen werden. Obgleich es Quantencomputer wohl erst in 5 oder 10 Jahren geben wird, können Betrüger heute schon Daten illegal speichern und diese später, wenn die benötigte Quanten-Rechenleistung verfügbar ist, entschlüsseln. Diese Bedrohung wird als Harvest Now, Decrypt Later (HNDL) bezeichnet und von den Regierungen, dem Militär und der Finanzwirtschaft mit großer Sorge beobachtet. Eine Lösung besteht darin, die Post-Quanten-Kryptographie (PQC) einzuführen, um sensible Daten vor der potentiellen Bedrohung durch Quantencomputer und Datendiebstahl zu schützen.

Das Mobilfunk-Standardisierungsgremium 3GPP entwickelt seine eigenen Standards weiter, um PQC-Algorithmen einzubinden und sich gegen zukünftige Quantencomputer-Angriffe verteidigen zu können. Dabei übernimmt das 3GPP PQC-Algorithmen, die bereits von anderen Gremien, wie dem National Institute of Standards and Technology (NIST) der USA, entwickelt wurden. Aufgrund der möglichen Gefährdung durch potentielle Quantencomputer-Angriffe hat der GSMA-Verband (Global System for Mobile Communications Association) unter der Bezeichnung Post-Quantum Telco Network Task Force (PQTN) eine Arbeitsgruppe eingerichtet, die die Betreiber von Mobilfunknetzen beim Übergang zur Post-Quanten-Bereitschaft berät.

Seit mehr als einem Jahrzehnt werden Anstrengungen zur Standardisierung der Quanten-Schlüsselverteilung (QKD) unternommen, um die Interoperabilität, Sicherheit und weltweite Einführung quantensicherer Kommunikationssysteme zu gewährleisten. Organisationen, wie das European Telecommunications Standards Institute (ETSI), die Internationale Fernmeldeunion (ITU-T) und die ISO/IEC, sind Wegbereiter bei der Formulierung von Rahmen, Protokollen und Sicherheitsanforderungen für QKD-Systeme.

2.2 Standards

Jedes Land bzw. jede Region hat ein entsprechende Forum für Quantentechnologien eingerichtet, wie QuIC (EU), QIC (Kanada), Q-STAR (Japan), QED-C (US), UKQuantum (GB), KQIA (Südkorea), NQSN (Singapur) und QIIA (China). Allerdings können die Motive und die Ziele durchaus unterschiedlich sein. Beispielsweise möchten die USA mit ihrem Gesetz zur „National Quantum Initiative" (NQI) die Forschung in der Quantentechnologie sowie die Entwicklung von Talenten und Innovationen in der Industrie fördern. China strebt mit seiner „Quantum Technology Roadmap" in bestimmten Anwendungsbereichen, wie der Kryptographie und der Materialwissenschaft, nach einer Quanten-Vorherrschaft und verfolgt bei Forschung, Humanressourcen und Infrastruktur ein vielseitiges Konzept. Japan möchte eine Gesellschaft aufbauen, in der die Quantentechnologie für jeden zugänglich ist, die Globalisierung der Quantentechnologie fördern und mit Hilfe der Quantentechnologie die Schaffung von Geschäftschancen unterstützen.

Europa betont die Grundlagenforschung mit Schwerpunktlegung auf Quanten-Kommunikation, -Computern und -Sensorsystemen und investiert in Quanten-Hardware, -Software und -Algorithmen, um das Ökosystem zu stärken. Diese Anstrengungen fördern Forschungsstandorte für Quanten-Computer, -Sensorsysteme und -Kommunikation.

Die Arbeitsgruppen ITU-T SG11, SG13 und SG17 sowie die ETSI ISG QKD arbeiten an der Standardisierung von QKD und von Quanten-Schlüsselverteilnetzen (QKDN). ISO/IEC/JTC1 spezifizieren Bewertungsmethoden für QKD-Module. Die GSMA stellt Leitlinien für hybride und PQC-Szenarien in der Telekommunikationsindustrie zur Verfügung.

Das NIST agiert als Wegbereiter, da es PQC-Algorithmen definiert und im August 2024 bereits die ersten drei Algorithmen veröffentlicht hat. Diese Standards, die auf den Algorithmen CRYSTALS-Kyber, CRYSTALS-Dilithium, und SPHINCS+ basieren, wurden entwickelt, um eine sichere Kommunikation und den Schutz der Daten vor dem Leistungspotenzial zukünftiger Quantencomputer zu gewährleisten. Obgleich das NIST die PQC-Standards als Bundesbehörde der USA festlegt, haben andere Länder sich entschlossen, die NIST-Empfehlungen zu übernehmen, wobei einige (wie China und Korea) ihre eigenen Versionen entwickeln.

Das ETSI, die ITU-T und die ISO/IEC sind führend bei der Festlegung von Rahmenwerken, Protokollen und Sicherheitsanforderungen für QKD-Systeme. Die Industry Specification Group for QKD (ISG-QKD) des ETSI ist besonders einflussreich, da sie technische Berichte und Spezifikationen formuliert, die sich mit den QKD-Komponenten, den Netzwerkarchitekturen und mit der Integration in klassische kryptographische Systeme befassen. In der Zwischenzeit arbeitet die ITU-T an der Standardisierung der QKD-Netzwerkarchitektur und der Schlüsselmanagement-Schnittstellen, um globale Bereitstellungsstrategien zu harmonisieren. Trotz der gemachten Fortschritte bleiben mehrere kritische Herausforderungen bestehen.

Erstens besteht zwischen den QKD-Systemen unterschiedlicher Anbieter eine eingeschränkte Interoperabilität, was großflächige Multivendor-Bereitstellungen behindert. Zweitens bleibt die Skalierbarkeit problematisch, insbesondere wenn es darum geht, die QKD-Verteilung über Punkt-zu-Punkt-Strecken hinaus in komplexe vermaschte Netze einzuführen. Drittens behindern die an die Kosten und die Infrastruktur gestellten Anforderungen, einschließlich der Notwendigkeit spezieller Glasfasern oder vertrauenswürdiger Knoten, die breitgefächerte Einführung. Außerdem befinden sich Zertifizierungs- und Konformitätsprüfungen für QKD-Systeme noch in der Entwicklung, ohne dass allgemein anerkannte Kennwerte für Leistung und Resilienz unter realen Einsatzbedingungen vorhanden sind. Zu guter Letzt stellen die Integration der QKD in bestehende Sicherheitsinfrastrukturen und deren Anpassung an neue PQC-Standards sowohl eine technische als auch eine strategische Herausforderung dar.

2.3 QKD und PQC

Für die Verteilung von Post-Quanten-Schlüsseln zur Systemnutzung stehen mit der QKD und der PQC zwei geplante Methoden zur Verfügung. Die QKD stützt sich beim Schlüsselaustausch auf die Eigenschaften der Quantenmechanik, sodass Lauschangriffe nahezu unmöglich sind, weil jede erkannte Störung dazu führt, dass ein neuer Schlüsselaustausch eingeleitet wird. Beide Technologien werden nebeneinander koexistieren, weil es sehr unterschiedliche Anwendungsfälle gibt, in denen die quantenresistente Kryptographie benötigt werden wird.

Bei der QKD werden die Verschlüsselungsschlüssel auf optischen Pfaden (terrestrische Glasfaser, optische Freiraumübertragung oder Satelliten-Verbindungen) in Form von Quantenbits (Qubit) als Maß für die Quanteninformation übertragen. Diese Methode garantiert, dass man weiß, wenn ein Lauscher den zum Verschlüsseln der Daten verwendeten Schlüssel abfängt. Dieses Konzept ist weitgehend manipulationssicher, weil es ein grundlegendes Prinzip der Quantenmechanik, nämlich die Verschränkung der Teilchen (typischerweise Photonen), nutzt. Jeder Versuch, in die Übertragung einzugreifen, erzeugt eine Störung, die umgehend vom Kommunikationsprotokoll erkannt wird und den sofortigen Abbruch der Kommunikation zur Folge hat. In diesen Fällen kann vor der Übertragung sensibler Daten ein neuer Schlüssel gesendet werden.

Weil die QKD auf Hardware basiert, ist dieses Verfahren mit hohen Kosten verbunden. Daher wird es vor allem in hochsensiblen Anwendungen zum Einsatz kommen, bei denen der Geheimnisschutz unter allen Umständen gesichert bleiben muss. Diese Anwendungen erfordern, dass sich die Parteien an festen Standorten befinden und Kostenaspekte keine große Rolle spielen. Die Märkte, auf denen die QKD am effektivsten einsetzbar wäre, sind Regierungen, Militär und einige Bereiche der Finanzwirtschaft, in denen ein Ausfall katastrophale Folgekosten haben könnte.

Die PQC ist andererseits ein softwarebasiertes Konzept, das Algorithmen nutzt, die sich auf neuen mathematischen Fragestellungen gründen, um vorhandene Schlüsselalgorithmen, wie RSA und ECC, die durch Quantencomputer-Angriffe gefährdet sein können, zu ersetzen. Da aber nicht bekannt ist, ob diese Algorithmen gebrochen werden können, gibt es keine 100%ige Sicherheit. Allerdings ist die PQC eine im Vergleich zur QKD kostengünstige Lösung und wird sich daher wohl als dominante Wahl durchsetzen.

Zusammengefasst lässt sich sagen, dass beide Methoden Vor- und Nachteile aufweisen. Daher wird bei realen Netzwerken und Validierungssystemen in Erwägung gezogen werden, die QKD und PQC sowie klassische Sicherheitsmechanismen nebeneinander bestehen zu lassen.

	QKD	PQC
Technische Ausstattung	Glasfaser mit speziellem Transceiver	Software-Ersatz
Sicherheitsmethode	Quantenmechanische Sicherheit	Berechnungssicherheit
Vorteile	Kein Sniffing möglich	Einfache Upgrades durch Software
Nachteile	Kurze Strecken (von etwa 100 km, satellitenbasierte QKD könnte die Lösung sein), geringe Geschwindigkeit, hohe Kosten	Keine 100%ige Sicherheit, Leistungsbedenken, Zeitaufwand für Migration
Standardisierung	ITU-T (Y.3800/X.1700 Series), ETSI	IETF, NIST
Anwendungsbeispiele	nationale Sicherheit, Standleitungen	massive Kommunikation, Online-Banking, Unternehmensstandorte

Es ist jedoch auch eine Realität, dass das quantensichere Ökosystem an sich fragmentiert ist, da proprietäre QKD-Protokolle, verschiedene PQC-Implementierungen und divergente Schlüsselmanagement-Systeme im Umlauf sind. Trotzdem besteht eine wichtige und strategische Notwendigkeit, die weltweite Lieferkette für diese Technologien zu stärken und ein heterogenes Implementierungskonzept zur Verfügung zu stellen.

Hier sind Interoperabilitätstests und entsprechende Validierungsrahmen unverzichtbar, um die Integrationsrisiken zu mindern und die Entwicklung des Ökosystems sowie die Einhaltung der Standards zu beschleunigen. Diese Maßnahmen dienen dem öffentlichen Wohl, das die Labore einzelner Anbieter nicht gewährleisten können bzw. wofür ihnen die Motivation fehlt.

2.4 Branchenumfassende Auswirkungen

Die Post-Quanten-Bereitschaft wirkt sich auf alle Branchen, darunter auf Regierungen, die Finanzwirtschaft, das Gesundheitswesen, das Militär und die Telekommunikation, aus. Sämtliche Mitarbeiter-, Finanz- und Behördendaten müssen für die digitale Übertragung verschlüsselt werden. Da Betrüger die Quantencomputer, sobald diese denn verfügbar sind, jederzeit und an jedem Ort nutzen sowie an allen Systemen einsetzen könnten, beginnt nun ein Wettlauf um den besten Datenschutz. Noch bevor Quantencomputer nutzbar sind, ist es möglich, Daten jetzt bereits abzuschöpfen und zu speichern, bis später die benötigte Quanten-Rechenleistung zur Verfügung steht, um sie zu entschlüsseln (HNDL), sodass Angreifer dann Zugang zu sensiblen Informationen erhalten.

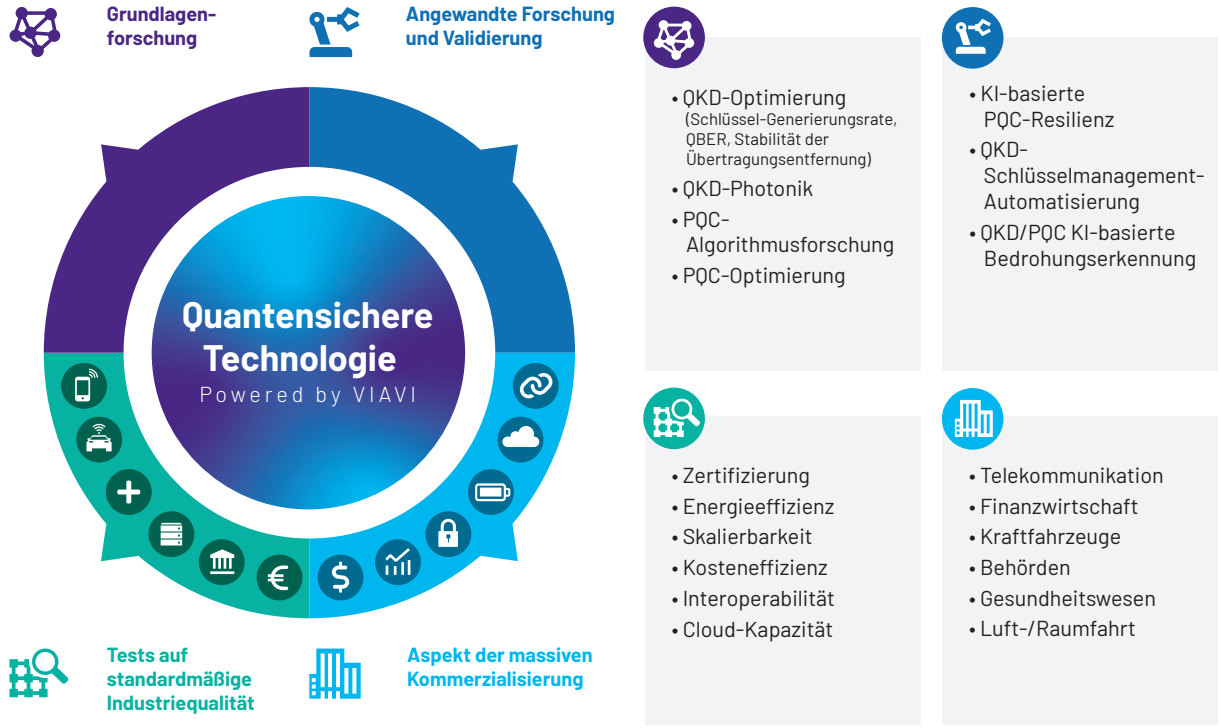
Obwohl jede vertikale Branche für das Management ihres eigenen PQC-Migrationspfads verantwortlich ist, gibt es doch viele gemeinsame Elemente, wie die Migration Roadmap. So hat die GSMA als Vereinigung der Mobilfunkanbieter mit den *Post Quantum Cryptography Guidelines for Telecom Use Cases* ihre Leitlinien zur PQC veröffentlicht. Die Reserve Bank of India hat ein Whitepaper mit dem Titel *Securing the Indian Banking Sector in the Age of Quantum Computing* erstellt.

Allerdings ist in allen Branchen ein wachsendes Interesse an einer vertrauenswürdigen Validierungsplattform, die für aufsichtsrechtliche Zertifizierungen, für das Vertrauen der Investoren und die bereichsüberschreitende Technologie-Bereitstellung unverzichtbar ist, zu verzeichnen. Diese Plattform müsste eine umfassende hybride Umgebung unterstützen sowie verschiedene Validierungsszenarien umsetzen, wie:

- hybride Simulationen, die die Skalierbarkeit der PQC mit der informationstheoretischen Sicherheit der QKD kombinieren.
- schichtenbasierte Tests, angefangen bei der physischen Photonen-Übertragung bis zu den Handshake-Protokollen auf der Anwendungsebene.
- HKMS-Tests für Synchronisation, Rückfall-Logik, Priorisierung und das Schlüssel-Aktualisierungsverhalten.
- Chaos-Tests für hybride Resilienz mit Bewertung des Durchgangs bei Ausfall von QKD-Strecken oder PQC-Verschlechterung.
- Digital-Twin-Umgebungen mit Simulation hybrider klassischer/Quanten-Netze in Edge-Metro-, Cloud- und Satelliten-Systemen, einschließlich nicht-terrestrischer Netze (NTN), optischer Freiraumübertragung (FSO) und satellitenbasierter QKD.
- Bewertung des Preis/Leistungsverhältnisses verschiedener Bereitstellungsmodelle, wie von öffentlich zu privat und Kernnetz zu Edge.

3 QUANTENSICHERE TESTBEREICHE

Aktuell befinden sich quantensichere Netzwerke im Stadium der Migration, so dass Überlegungen zum Lebenszyklusmanagement und zur schrittweisen massiven Kommerzialisierung notwendig sind. VIAVI unterstützt alle Testbereiche:



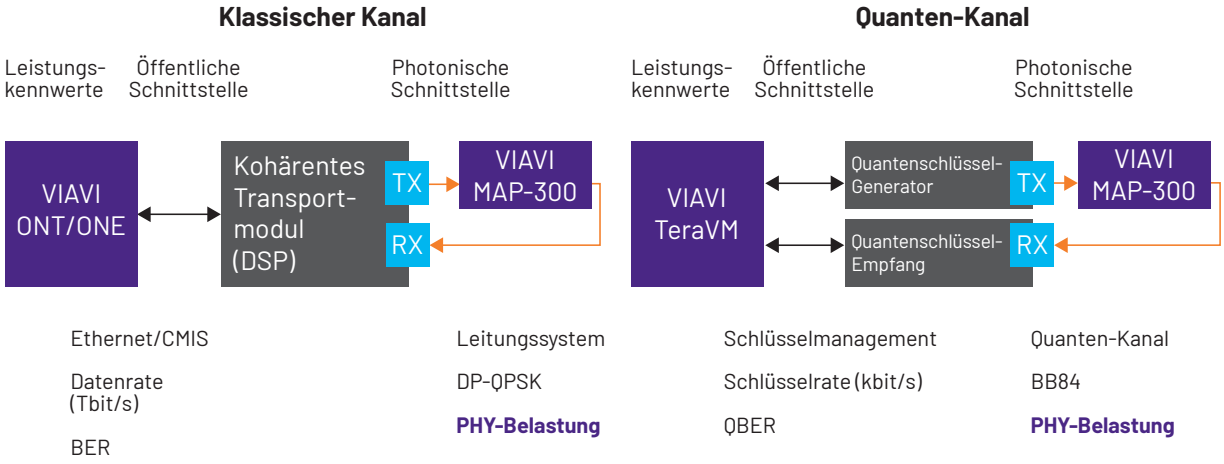
- Grundlagenforschung: QKD-Optimierung, QKD-Photonik, PQC-Algorithmen, PQC-Optimierung, Quantensicherheit, Quantensimulationen
- Angewandte Forschung und Validierung: Automatisierung des QKD-Schlüsselmanagements, QKD/PQC KI-basierte Bedrohungserkennung, KI-basierte PQC-Resilienz (einschließlich hybrid mit PQC-fremden Protokollen), KI-basierte Testautomatisierung für hybride Systeme
- Tests auf standardmäßige Industriequalität: Zertifizierung, Energieeffizienz, Skalierbarkeit, Wirtschaftlichkeit, Interoperabilität, Cloud-Kapazität
- Aspekte/Anforderungen für die massive Kommerzialisierung: Telekommunikation, Finanzen, Kraftfahrzeugindustrie, Behörden, Gesundheitswesen, Luft- und Raumfahrt

Diese Anwendungsbeschreibung untersucht im jeweiligen Kontext die einzelnen Komponenten der von VIAVI für quantensichere Tests angebotenen Produktpalette:

Quantensichere Netzwerkfunktion	VIAVI Produkt
QKD Schlüsselmanagement-Systemtest	TeraVM Security
PQC-Leistungstest	TeraVM Security, VAMOS
Quantenkanal-Bewertung	MAP-300
Glasfaser-Überwachung	ONMSi Remote Fiber Test System (RFTS)
Faseroptische Sensortechnologie	FTH-DTSS
Netzwerk-Beobachtbarkeit	NITRO® AIOps, ONMSi
Glasfaser-Infrastruktur/Feldvalidierung	OneAdvisor 800
Operative Effizienz	NITRO AIOps
Premium-Optik	Spektrale Sensorfilter, Licht-Sensorfilter

Die nachstehende Grafik gibt einen Überblick über die Testumgebung mit den empfohlenen Einsatzmöglichkeiten der Produktpalette von VIAVI.

Vergleich von Quantenkanal und klassischem Kanal



In vielerlei Hinsicht stellt die Testausführung an klassischen Kanälen und an Quanten-Kanälen identische Anforderungen.
Aber die photonische Schnittstelle IST sehr unterschiedlich.
Allerdings werden beide Kanäle über eine optische Struktur übertragen, die es zu emulieren gilt.
Die Pegel und die Arten der optischen Belastungsfaktoren werden sich dabei sicherlich ändern.

1991.900.0725

3.1 Test und Überwachung von QKD-Systemen

QKD-Systeme stellen verschiedene grundlegende Anforderungen an die Testausführung. Dazu zählen:

- Überprüfung der QKD-Schwächung durch Erstellung eines flexiblen, neukonfigurierbaren photonischen Systems, das eine breite Palette von leistungsbasierten und spektralen Lastszenarien emuliert, die für Live-Produktionsnetze repräsentativ sind. Diese Methode kann zur Validierung der Leistung oder Anwendbarkeit neuer QKD-Systeme oder Teilkomponenten genutzt werden.
- Bewertung der Resilienz von QKD-Systemen auf Grundlage der Fasertypen sowie ggf. der Leistung und Position von DWDM-Signalen, temporärer Bedingungen während des Hinzufügens/Entfernens von Wellenlängen sowie die Qualifizierung neuer optischer Geräte in der P2P-Strecke (beispielsweise optischer Schalter).
- Belastungstests über P2P-Strecken zur Erzeugung unterschiedlicher kontrollierter optischer Belastungsfaktoren, wie Imband-/Außerband-Rauschen von Verstärkern, Polarisationsstörungen durch Kabelbewegung, Dithering/Stabilität aktiver optischer Elemente, wie optische Schalter, Dämpfungsglieder, Wellenlängen-Schalter, oder durch optische Verbinder verursachte einzelne oder mehrfache Reflexionsereignisse.
- Konformitätsprüfung bis zur Diensteschicht gemäß ETSI GS QKD 014. Prüfung der QKD Schlüsselmanagement-Systemschicht auf Resilienz, d. h. wie effizient sie die VPN-Anwendungsschichten (L3) in Bezug auf die Abfrage von im Vorfeld ausgetauschten Schlüsseln (Post-Quantum Preshared Key, PPK) zum Aufbau von IPSec-VPN-Tunneln gemäß IKEv2 (RFC8784) bedienen kann. Das ist vor allem relevant, wenn eine häufige Schlüsselrotation der VPN-Strecke konfiguriert wurde, um eine bessere Post-Quanten-Sicherheit zu erzielen. Die TeraVM IKEv2 Client-Emulation wird von der ETSI GS QKD 014 API unterstützt, um die PPKs von der KMS/QKD-Schicht abzufragen und kann die QoE unter Last testen, wenn die Schlüssel kontinuierlich in einem Post-Quanten-sicheren IKEv2 VPN-Tunnel mit PPK-Authentifizierung rotiert werden.
- Tests auf physische Angriffe gegen Glasfaserkabel, wie Temperatur und Dehnung sowie unbefugte Schachtarbeiten.

Quantenkanal-Bewertung

Die Quantenkanal-Bewertung in Testumgebungen ermittelt, wie gut eine Quanten-Kommunikationsverbindung die Qubit-Integrität unter realen oder simulierten Bedingungen gewährleistet. Damit ist schon vor der Bereitstellung gewährleistet, dass der Kanal sichere Quantenprotokolle unterstützt. Diese Quantenkanal-Bewertung in Testumgebungen umfasst auch die Charakterisierung des Verhaltens einer Quanten-Kommunikationsverbindung und wird typischerweise zur Einschätzung ihrer Eignung für QKD- oder andere Quanten-Protokolle genutzt.

Die beiden Haupttypen der QKD unterscheiden sich nach der Nutzung diskreter Variablen (DV-QKD) und kontinuierlicher Variablen (CV-QKD):

- DV-QKD: Dieser Typ codiert Informationen mit Hilfe diskreter Quantenzustände, wie Polarisierung oder Phase einzelner Photonen, und erfordert eine präzise Uhren-Synchronisation, um die Ankunftszeiten der Photonen zu erkennen. In diese Kategorie gehören Protokolle wie BB84 und E91. Zur Detektion kommen Einzelphotonen-Detektoren, wie APD und SNSPD, zum Einsatz.
- CV-QKD: Dieser Typ nutzt die kontinuierliche Modulation von Quadraturkomponenten (Amplitude und Phase) von kohärentem Laserlicht. Die Information wird durch homodyne oder heterodyne Detektion extrahiert, die häufig auf Gauß'schen Modulationsprotokollen wie GG02 basieren. Diese Vorgehensweise ist weniger zeitkritisch, erfordert aber den Abgleich der Phasenreferenz (Kalibrierung des lokalen Oszillators). Zur Detektion kommen homodyne oder heterodyne Detektoren (klassische Fotodioden) zum Einsatz.

Die DV-QKD bietet über längere Strecken größere Sicherheitsgarantien, nutzt aber komplexe Hardware und niedrigere Schlüsselraten. Die CV-QKD ist besser für Anwendungen mit kurzen Strecken und hohen Raten geeignet und verwendet Standardkomponenten der Telekommunikation. Die Testkonzepte müssen die spezifischen physischen und Protokoll-Charakteristiken berücksichtigen und dabei den Schwerpunkt insbesondere auf Rauschen, Synchronisation und Komponenten-Kalibrierung legen.

Zur Quantenkanal-Bewertung kommen in Testumgebungen verschiedene Tools und Methoden zum Einsatz. Dazu gehören Einzelphotonen-Detektoren, Quanten-Lichtquellen, OTDRs sowie weitere klassische Glasfaser-Tester, Tomographie-Tools und Simulatoren, beispielsweise zur Rauscheinkopplung. Zu den wichtigsten Messungen zählt die Quantenbit-Fehlerrate (QBER), die die Fehlerhäufigkeit der übertragenen Quantenbits (Qubit) ermittelt. Eine hohe QBER-Rate kann auf Rauschen oder einen Lauschangriff hinweisen. Weitere Messungen betreffen die Dämpfung (dB/km), Kohärenzzeit/Polarisationsstabilität, Kanalgenauigkeit und Jitter sowie die Synchronisation.

Die Tests umfassen Prüfstand-Versuche im Labor für Kurzstrecken-Tests mit optischen Tischen und Präzisionskomponenten, die Simulation über „reale" Entfernungen von 10 km, 50 km und mehr, Felderprobungen mit installierten Glasfasern sowie Satelliten- oder Flugzeug-gestützte Tests (optische Freiraumübertragung, FSO).

Für die Quantensicherheit könnte sich die Kanalbewertung speziell auf die folgenden Aspekte konzentrieren:

- Resistenz gegen Side-Channel-Angriffe: Die Tests gewährleisten, dass quantensichere kryptographische Implementierungen nicht durch Side-Channel-Angriffe gefährdet werden, die unbeabsichtigte Informationsabflüsse, wie Stromverbrauch oder elektromagnetische Emissionen, ausnutzen.
- Validierung der quantensicheren Verschlüsselung: Unternehmen bewerten quantensichere Verschlüsselungsmethoden, um ihre kritische Infrastruktur vor neuen Bedrohungen zu schützen.
- Leistungs- und Kompatibilitätsprüfungen: Quantensichere kryptographische Lösungen werden auf ihre Effizienz und Integration in vorhandene IT-Systeme getestet, um einen nahtlosen Übergang zu gewährleisten.

Diese Bewertungen unterstützen die Vorbereitung auf die Quanten-Ära, indem sie dafür sorgen, dass die Kommunikationskanäle vor zukünftigen quantenbasierten Cyber-Bedrohungen geschützt bleiben.

Im Allgemeinen werden die Testkonfigurationen auch iterativ optimiert, um Fehlerquellen wie Fehlabgleich, Temperaturdrift und Detektor-Dunkelzähler zu verringern und damit die Schlüsselrate weitestgehend zu erhöhen sowie die QBER-Rate gleichzeitig unter einer sicheren Schwelle (zumeist < 11 % bei BB84 QKD) zu halten.

Lösung von VIAVI: MAP-300

Quanten-Tests setzen voraus, dass die Labore mit optischen Schaltern, Tools zum Wellenlängen-Management, EDFA-Verstärken und Dämpfungsgliedern ausgestattet sind, um die verschiedenen Quanten-Experimentalbedingungen schaffen zu können. QST baut Netzwerke zur Erprobung/Bewertung von Quantenverfahren auf. Das MAP-300 von VIAVI ist eine modulare, dichte und mühelos rekonfigurierbare optische Testplattform mit Fernbedienung und Automatikfunktionen. Sie untersucht effektiv die Grenzen der Quantentechnologie in den Bereichen Computing, Vernetzung, Verschlüsselung und Kryptographie.

Das MAP-300 unterstützt Tests zur Überprüfung der QKD-Schwächung durch Erstellung eines flexiblen, neukonfigurierbaren photonischen Systems, das eine breite Palette von leistungsbasierten und spektralen Lastszenarien emuliert, die für Live-Produktionsnetze repräsentativ sind. Diese Methode kann zur Validierung der Leistung oder Anwendbarkeit neuer QKD-Systeme oder Teilkomponenten genutzt werden. Es sind auch Untersuchungen möglich, um die Bedingungsmatrix zu definieren (sogar zu standardisieren), die benötigt wird, um die Funktionsfähigkeit des QKD-Systems anhand der folgenden Parameter nachzuweisen:

- Fasertypen
- Leistung und Position von DWDM-Signalen (wenn vorhanden)
- Temporäre Bedingungen während des Hinzufügens/Entfernens von Wellenlängen
- Qualifizierung neuer optischer Geräte auf der P2P-Strecke (beispielsweise optische Schalter)

Die Erstellung und Einfügung rein optischer Elemente in die QKD P2P-Strecke zum Erzeugen einer Reihe von kontrollierten optischen Belastungsfaktoren.

- Imband- und Außerband-Rauschen von Verstärkern
- Polarisationsstörungen durch Kabelbewegungen
- Dithering/Stabilität optischer Elemente (Schalter, Dämpfungsglieder, Wellenlängenschalter)
- Einzelne oder mehrfache Reflexionsereignisse durch optische Verbinder
- Untersuchungen zur Entwicklung von Fehlerkorrektur-Mechanismen für die QKD auf verschiedenen Rausch- und Störpegeln. Studien zu aktuellen Verfahren sowie zur Entwicklung besserer Methodologien.

Glasfaser-Überwachung

Die Glasfaser-Überwachung kann für die quantensichere Kommunikation eine wichtige Rolle spielen, da sie potentielle Angriffe auf der Bitübertragungsschicht (Physical Layer) erkennt. Beispielsweise könnte ein Abhörversuch („Anzapfen") die Sicherheit der QKD oder anderer quantensicherer Protokolle gefährden. Die QKD stützt sich auf die grundlegenden Eigenschaften der Quantenmechanik, insbesondere auf den Umstand, dass ein Quantensystem bei der Messung gestört wird. Wenn ein Angreifer sich jedoch einen physischen Zugang zur Glasfaser verschafft, könnte er versuchen, Signale unerkannt abzufangen.

Bei dieser Art von Abhörversuchen hilft die Glasfaser-Überwachung, Anomalien, wie eine höhere Signaldämpfung, Ruckstreuung oder zeitliche Verzögerungen zu erkennen, die Vermittlungsstelle (CO) über den unbefugten Zugriffsversuch zu informieren und ganz allgemein die Integrität des physischen Übertragungsmediums zu gewährleisten.

Weiterhin stärkt die Glasfaser-Überwachung die quantensichere Sicherheit insgesamt. Auch wenn die QKD nicht zum Einsatz kommt, sind die PQC-Algorithmen auf eine sichere physische Infrastruktur angewiesen. Wenn es einem Angreifer gelingt, eine Glasfaser passiv anzuzapfen, könnte er heute verschlüsselte Daten abschöpfen und das Verschlüsselungsverfahren später mit einem Quantencomputer brechen (HNDL-Angriff). Die Glasfaser-Überwachung ist also die erste Verteidigungslinie, die passive Abhörversuche verhindert und die quantensichere Kryptographie durch Sicherheit auf der Physical Layer ergänzt. Sie gewährleistet die Integrität und Sicherheit optischer Kommunikationsnetze durch:

- Quantensichere Verschlüsselung: Die Glasfaser-Überwachung hilft, eine sichere Datenübertragung aufrechtzuerhalten, indem sie die QKD und PQC in optische Netzwerke integriert. Damit ist gewährleistet, dass sensible Daten vor den Cyber-Bedrohungen der Quanten-Ära geschützt bleiben.
- Ultrasichere Quanten-Kommunikation: Forscher haben Quantendaten mit Hilfe von Glasfasernetzen erfolgreich über große Entfernungen übertragen und die Machbarkeit der quantensicheren Nachrichtenübermittlung ohne teure kryogene Kühlung nachgewiesen.[1] Dieser Fortschritt stärkt die Sicherheit von Finanztransaktionen, der Gesundheitsdaten und der behördlichen Kommunikation.
- Latenzarme Glasfasern für die Quanten-Kryptographie: Einige Unternehmen testen neue Glasfaser-Technologien, wie Hohlkernfasern (HCF), um die Effizienz der Quanten-Kryptographie zu verbessern[2]. Diese Innovationen tragen dazu bei, die Entfernung, auf der die quantensichere Verschlüsselung anwendbar ist, zu vergrößern, so dass sie den praktischen Anforderungen des Netzbetriebs besser gerecht wird.

Auch kann die Glasfaser-Überwachung in Verbindung mit faseroptischer Sensortechnologie in quantensicheren Umgebungen die Sicherheit und Resilienz von Kommunikationsnetzen gewährleisten.

[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_

Lösung von VIAVI: ONMSi Remote Fiber Test System (RFTS) mit Fiber Test Head (FTH)

Das ONMSi ist ein optisches Netzwerk-Überwachungssystem, das die Sichtbarkeit des Netzwerks vom Kernnetz über das PON bis zum Kundenstandort verbessert. So lassen sich in jedem Netzwerktyp die Betriebsunterstützung und die Dienstgüte (QoS) optimieren. Als optisches Ferntestsystem erkennt und lokalisiert das ONMSi Störungen im Glasfasernetz rund um die Uhr (24/7), ohne dass ein Techniker in den Feldeinsatz geschickt werden muss. Eine Glasfaser-Testkopf (Fiber Test Head, FTH), der von der branchenführenden Kompetenz von VIAVI bei optischen Technologien profitiert und ein optisches Reflektometer (OTDR) sowie einen optischen Schalter integriert, vergleicht kontinuierlich die aktuellen Faserdaten mit zuvor erfassten Referenzwerten und löst bei Abweichungen einen Alarm aus.

Faseroptische Sensortechnologie

Die faseroptische Sensortechnologie kann die quantensichere Kommunikation als Echtzeit-System zur Erkennung unbefugter Zugriffe (IDS) auf der Physical Layer eines quanten- oder post-quantensicheren Netzwerks stärken. In einfachen Worten wandelt diese Technologie die Glasfaser in ortsverteilte optische Sensoren um, die prüfen, wie das Licht entlang der Faserstrecke reflektiert oder gestreut wird. Diese Analyse kann auf Grundlage der Rayleigh-Streuung (für Schwingungsmessungen, also akustische Sensorik), der Brillouin-Streuung (für die Dehnungs- und Temperaturmessung) oder der Raman-Streuung (für die Erstellung von Temperaturprofilen) erfolgen. Alle diese Methoden erkennen selbst kleinste Veränderungen über lange Faserstrecken.

Die faseroptische Sensortechnologie unterstützt die quantensichere Sicherheit durch:

- Manipulationserkennung auf QKD-Strecken: Die QKD basiert auf der Annahme, dass ein physischer Zugriff den Quantenzustand stört. Die faseroptische Sensortechnologie fügt eine weitere Dimension hinzu, indem sie erkennt, wenn versucht wird, die Glasfaser abzuhören, zu krümmen oder zu trennen, noch bevor die Daten ernsthaft kompromittiert werden können. Wenn ein Angreifer beispielsweise die Glasfaser krümmt, um Photonen abzuschöpfen, kann diese Technologie die resultierende Dehnung oder Schwingung erkennen und einen Alarm auslösen.
- Überwachung auf zeitversetztes Abhören: Bei der PQC könnten Angreifer die Glasfaser heute abhören und die verschlüsselten Daten speichern, um sie später mit einem Quantencomputer (HNDL-Angriff) zu entschlüsseln. Die faseroptische Sensortechnologie erkennt diese Art von passiven Abhörversuchen und erschwert es den Angreifern, unerkannt zu bleiben.
- Verbessertes Lagebewusstsein: Die faseroptische Sensortechnologie kann Schwingungen, Umgebungsstörungen und unbefugte Bauarbeiten erkennen, die die Sicherheit kritischer quantensicherer Infrastruktur bedrohen könnten. Insbesondere für erdverlegte oder frei zugängliche Glasfaserstrecken stellt sie einen Sicherheitsumkreis (Perimeterschutz) zur Verfügung.

Die faseroptische Sensortechnologie stärkt quantensichere Systeme durch Frühwarnung vor physischen Angriffen und Ergänzung der Quanten-Kryptographie durch ein verteiltes Echtzeit-Monitoring, das sowohl die QKD als auch die PQC vor Angriffe auf der Physical Layer schützt. Sie kann in quantensicheren Umgebungen eine kritische Rolle spielen, da sie sichere und präzise Messungen ermöglicht und gleichzeitig die Datenintegrität vor potentiellen Bedrohungen schützt. So ermöglicht sie die sichere Quanten-Fernsensorik (Secure Quantum Remote Sensing, SQRS) über große Entfernungen, beispielsweise 50 km lange Glasfaserstrecken ohne Verschränkung. Ein weiteres Beispiel ist die faserbasierte Quanten-Sensorik für Umwelt-Monitoring, Katastrophenhilfe und militärische Überwachung, die gewährleistet, dass die übertragenen Daten vertraulich bleiben und gegen Abhörversuche resistent sind.

Diese Fortschritte unterstreichen das wachsende Potential der faseroptischen Sensortechnologie in quantensicheren Anwendungen und ebnen den Weg für resilientere und stärker skalierbare Quanten-Technologien.

Lösung von VIAVI: FTH-DTSS

Der von VIAVI angebotene Fiber Test Head (FTH) zur Temperatur- und Dehnungsmessung (FTH-DTSS) überwacht Stromkabel, Pipelines und Telekommunikationskabel mit den vielseitigsten faseroptischen Sensorlösungen auf dem Markt. Das FTH-DTSS ist Bestandteil der NITRO Fiber Sensing Lösung und gewährleistet die kontinuierliche Überwachung von Glasfaserkabeln und Glasfaser-konformen Ressourcen. Die Übermittlung kontinuierlicher Echtzeitdaten zur umgebungsbedingten Temperatur und Dehnung in und in Nähe des zu überwachenden Objektes mit Hilfe von Glasfaserkabeln ermöglicht die sofortige Erkennung und Lokalisierung der betreffenden Ereignisse. Die wichtigsten Leistungsmerkmale des FTH-DTSS auf einen Blick:

- Die FTH-DTSS-Lösung von VIAVI für die verteilte Temperatur- und Dehnungsmessung wurde für Branchen entwickelt, die auf eine hohe Präzision und Zuverlässigkeit angewiesen sind. Sie ermöglicht die Messung der absoluten Temperatur und Dehnung entlang großer Längen von Glasfaserkabeln. Damit erweist sie sich bei zahlreichen Anwendungen als unverzichtbar
- Sie ist in der Lage, in den verschiedensten Anwendungen, darunter an kritischer Infrastruktur (Energieversorger), Pipelines (Öl, Gas, Wasser usw.), Telekommunikationsnetzen (DCI-Zusammenschaltungen von Rechenzentren), Anomalien zu erkennen
- Die im Rahmen der proaktiven Überwachung festgestellten Temperatur- und Dehnungsänderungen können genutzt werden, um die betriebliche Effizienz und Reaktionsfähigkeit zu verbessern und präventive/proaktive Maßnahmen zur Minderung potenzieller Schäden oder Ausfälle zu ergreifen

3.2 Testen der PQC-Leistung

Wenn es darum geht, die vorhandenen Verschlüsselungsalgorithmen in Post-Quanten-Algorithmen zu migrieren, muss auf die Auswirkungen der deutlich längeren Verschlüsselungsschlüssel hingewiesen werden. Außerdem kann die Einführung der PQC in verschiedenen Komponenten eines Mobilfunksystems Auswirkungen auf die Leistung und die Architektur, insbesondere auf die Endgeräte der Nutzer, haben. Dies gilt vor allem, wenn die Bandbreite beschränkt ist. Daher ist es unverzichtbar, sowohl die terrestrischen Netze (TN) als auch die nicht-terrestrischen Netze (NTN) in PQC-konformen Konfigurationen zu testen. Die untenstehende Tabelle nennt einige von der Telekommunikationsindustrie geäußerte Bedenken:

Unternehmen	PQC-Migrationsbedenken
SKT	Die Entwicklung von Technologien zur Integration von Quanten-Kryptographie-Netzen, wie Q-SDN und QKDN Federation, um den integrierten Betrieb und die Kontrolle von Quanten-Kryptographie-Netzen zwischen den Geräten unterschiedlicher Hersteller, zwischen Netzbetreibern und zwischen Ländern zu ermöglichen.
Vodafone	IBM hat eine Zusammenarbeit mit Vodafone bekanntgegeben, um die IBM Quantum Safe Technologie in dessen umfassenden digitalen Sicherheitsdienst (Vodafone Secure Net) zu integrieren. Das Konzept zielt darauf ab, die Smartphone-Nutzer durch Implementierung von PQC-Standards vor zukünftigen Bedrohungen durch Quantencomputer zu schützen.
Softbank	Die Einführung kryptographischer Protokolle in die Infrastruktur zur Datenübertragung kann eine erhebliche Belastung der Kommunikationsverbindungen zur Folge haben und Latenzprobleme verursachen, die die Qualität verschlechtern und den Durchsatz senken.

Unternehmen	PQC-Migrationsbedenken
5G Americas	Es werden Probleme mit der Leistung und der Interoperabilität erwartet, die gründliche Tests erfordern.
Indisches Referat für Telekommunikation	Da neu entwickelte PQC-Algorithmen schwer zu handhaben sind, können sie die wichtigsten Betriebsabläufe der Unternehmen beeinträchtigen. Es ist wichtig, neue und aktualisierte Produkte kontinuierlich zu testen und deren Leistung zu überwachen.
GSMA-Leitlinien für die Telekommunikationsindustrie	Die Bereitstellungen müssen getestet werden, um die Tragfähigkeit bestimmter PQC-Algorithmen zu ermitteln und eine Beeinträchtigung der Leistung weitestgehend zu vermeiden.
Reserve Bank of India	Einige Bedenken betreffen den Performance-Overhead und komplexe Implementierungen, die umfangreiche Tests nahelegen.
BIS	Neue kryptographische Implementierungen müssen gründlich getestet werden, um deren einwandfreie Funktion in der vorhandenen Infrastruktur sicherzustellen, das Leistungsniveau aufrechtzuerhalten und die Systemintegrität nicht zu beeinträchtigen.

Die Testlösung TeraVM PQC Performance ist Bestandteil des RAN2Core Testpakets von VIAVI. Beispielsweise erlauben PQC-Tests, die in den UE-Emulator TM500 integriert sind, massive Netzwerktests durchzuführen und eine große Anzahl von Endgeräten unter anderem für TN, NTN und IoT mit PQC zu emulieren. Diese Lösung ermöglicht, einschließlich im Satelliten-Bereich einen quantensicheren digitalen Zwilling des Netzwerks zu erstellen.

Lösung von VIAVI: TeraVM Security

Gründliche Tests sind die beste Möglichkeit, um die PQC-Bereitschaft von Systemen zu gewährleisten und sicherzustellen, dass ihre Leistung nicht beeinträchtigt wird. Genau hier kommt TeraVM von VIAVI ins Spiel.

TeraVM ist ein Software-Testtool, das bereits seit mehr als 20 Jahren die VPN-Leistung ermittelt, indem es Nutzer und Verkehr emuliert sowie VPN-Kopfstellen bis an ihre Grenzen belastet, um die Leistung der Nutzer zu testen, während das VPN den Verkehr verarbeitet und Malware herausfiltert. Um PQC-Tests zu den VPN-Tests hinzuzufügen, ist nur eine einfache Erweiterung des vorhandenen Software-Tools erforderlich, um den VPN-Tunnel mit PQC-standardisierten Algorithmen zu verschlüsseln. In diesem Fall müssten zusätzliche KPIs, wie Schwankungen der Schlüssellänge, Schlüsselerneuerungsrunden und hybride Schlüssel, gemessen werden.

Viele IT-Abteilungen testen ein neues Leistungsmerkmal, bevor sie es im gesamten Unternehmen einführen. Dafür melden sich beispielsweise einige Mitglieder des Test-Teams weltweit im System an, um die neue Funktion zu überprüfen. Obgleich dieses Konzept für die meisten Upgrades und Bugfixes in Ordnung ist, versagt es bei Veränderungen, die zusätzliche IT-Overhead beinhalten. Allein in den USA gibt es über 10.000 Unternehmen mit mehr als 1.000 Beschäftigten, sodass ein skalierbarer Test erforderlich ist, um einen reibungslosen Übergang zur PQC sicherzustellen.

TeraVM von VIAVI kann nicht nur Zehntausende Mitarbeiter und deren Standort (extern, VPN, lokal, Managed Device und mehr), sondern auch deren Büro-Verkehr, wie Kollaborationstools, Video-Konferenzen und Zugang zu privaten Anwendungen, emulieren. TeraVM kann Verkehr mit einer steigenden Anzahl von Mitarbeitern übertragen und gleichzeitig KPIs, wie Latenz, Durchsatz und MOS-Score, überwachen. Damit kann sich der Anwender sicher sein, dass die Überführung in die Praxis reibungslos erfolgen wird.

Testen von PQC-Systemen

Die Implementierung von PQC-Protokollen führt zusätzliche Performance-Overheads ins Netzwerk ein, die die Erlebnisqualität der Endnutzer beeinflusst. Hier sind Tests unverzichtbar, um die kryptographischen Systeme, einschließlich neuer PQC-basierter Anwendungen, erfolgreich entwickeln und in der Praxis bereitstellen zu können. Die PQC verfolgt das Ziel, sichere Algorithmen zur Abwehr von Bedrohungen durch Quantencomputer zu schaffen. Die Durchführung von Tests unterstützt dieses Vorhaben in mehreren PQC-Schlüsselbereichen:

- Sicherheitsbewertung
  - Resistenz-Tests überprüfen die Widerstandsfähigkeit der PQC-Algorithmen gegen kryptographische Angriffe. Dazu gehört das Testen der Algorithmen unter verschiedenen Szenarien, einschließlich mit Nutzung von klassischen und Quanten-Algorithmen, um deren Resilienz einschätzen zu können.
- Leistungsbewertung
  - Berechnungseffizienz-Tests bewerten die Effizienz der von den PQC-Algorithmen ausgeführten Berechnungen. Darin eingeschlossen sind die Überprüfung der Geschwindigkeit der Verschlüsselung/Entschlüsselung und der Schlüsselgenerierung sowie der Systemleistung insgesamt. Die Sicherung der Effizienz von PQC-Algorithmen ist die Voraussetzung für deren weitverbreitete Einführung in praktischen Anwendungen.
- Testen der Interoperabilität
  - Integration in vorhandene Systeme: Häufig werden kryptographische Systeme mit bereits eingeführten Infrastrukturen und Protokollen zusammenwirken müssen. Hier sind Tests unverzichtbar, um die nahtlose Integration der PQC-Algorithmen in vielfältige Systeme garantieren zu können und Kompatibilitätsprobleme zu vermeiden.
- Testen der Konformität
  - Einhaltung von Standards: Diese Tests weisen die Konformität der PQC-Algorithmen mit etablierten kryptographischen Standards nach, fördern die Interoperabilität sowie die konsistente plattformübergreifende Implementierung.

VIAVI kann auf langjährige Erfahrungen beim Testen von VPN-Netzen verweisen, die auf das Testen von PQC-Algorithmen übertragbar sind, um eine Gefährdung durch HNDL-Angriffe zu verhindern.
Zu diesen Tests zählen:

- Hybride Post-Quanten (PQ) VPN-Tests: Testen des IKEv2-Peering mit hybriden Schlüsseln
  - PQ VPN Hybrid-Tests für den Initiator, nicht den Responder: Gewährleistung des Aufbaus klassischer IKEv2-Tunnel, wenn keine der beiden Parteien PQ-VPN-Schlüssel unterstützt.
  - Test einer nicht angepassten PQC KEM-Auswahl: Der Test sollte fehlschlagen, wenn die Negotiation keine passende Chiffre zwischen Initiator und Responder finden kann.
  - Belastungstest des PQ VPN-Tunnels: Übertragung großer Datendateien zwischen zwei PQC-unterstützenden Standorten über einen langen Zeitraum, um sicherzustellen, dass die Dateiübertragungen auf beiden Seiten korrekt abgeschlossen werden.
- Unterstützung des IPSec VPN PQC-Algorithmus:
  - Es werden NIST-standardisierte KEM-Algorithmen sowie mehrere Post-Quanten-Algorithmen unterstützt.

VIAVI Automation Management and Orchestration System (VAMOS)

VAMOS ist eine einheitliche cloudbasierte Plattform, die Testkampagnen, Fälle und Ausführungen für Mobilfunk-Testprodukte von VIAVI, einschließlich TeraVM Security, automatisiert. Mit individuell anpassbaren Arbeitsbereichen und Konfigurationen rationalisiert VAMOS den gesamten Test-Workflow und verbessert die Auslastung der Ressourcen der einzelnen Teams und Laborstandorte.

Gemeinsam genutzte Prüfstände und individuelle Sandboxes unterstützen eine breite Palette von Testanforderungen, während robuste Analyseverfahren und Berichtsfunktionen die Präzision und Zuverlässigkeit der Tests verbessern.

Durch die Integration von KI, ML und Lab-as-a-Service (LaaS) ermöglicht VAMOS eine deutliche Senkung der Betriebskosten, eine weitestgehende Verringerung des manuellen Arbeitsaufwands und die Beschleunigung der Fehleranalyse. Das Ergebnis sind eine kürzere Time-to-Market, eine bessere Qualität und eine bessere Budget-Kontrolle. Nachstehend folgt ein Überblick über die wichtigsten Vorteile:

Senkung der Betriebskosten

- Einsparung von Mannstunden durch intelligente Automatisierung
- Kürzere Time-to-Market mit optimierten Workflows
- Bessere Dienstgüte (QoS) durch präzise und konsistente Testausführung

Maximierung der Effizienz und Effektivität des Labors

- Zero-Touch-Automatisierung für die Ende-zu-Ende Testausführung
- KI/ML-basierte Einblicke zur Verkürzung der Reaktionszeiten und Stärkung der technischen Kompetenz

Ermöglichung einer standortunabhängigen Testausführung

- Globale Planungsschicht zur gleichmäßigen Auslastung der Ressourcen in den Laboren
- Kostenoptimierte Tests durch standortunabhängige Ausführung
- Offene, Tool-unabhängige Automatisierungsrahmen mit einsatzbereiten Planungsfunktionen

Sicherung der Nutzung branchenführender Tools

- Anspruchsvolle Tool-Auswahl und Slip-Through-Analyse zum Erkennen übersehener Fehler auf Ebene des Feldeinsatzes
- Priorisierung von Tools und Prozessen für die frühzeitige Identifikation tatsächlicher Probleme

Nutzung der Hardware/Software-Disaggregation auf handelsüblichen Plattformen

- Gemeinsam genutzte Rechenressourcen für verschiedene Testszenarien
- Dynamische Einrichtung des Software-Tools in temporären On-Demand Sandboxes
- Bevorzugung reiner Software-Tools mit flexiblen Hardware-Plugins als Ersatz für unflexible Geräte

3.3 Testen von hybriden Systemen

In Quantennetzen kombinieren hybride Systeme klassische Netzwerk-Komponenten mit Quanten-Technologien, wie QKD, Quanten-Repeater und PQC. Um diese Systeme testen zu können, wird ein mehrdimensionales Konzept benötigt, das die Funktionalität, Leistung, Sicherheit und Umgebungsfaktoren berücksichtigt:

Migrationstest in Prüfständen
Ziel: Emulation der von Serviceprovidern benötigten Migrationsszenarien.

- Koexistenz-Szenario von QKD, PQC und klassischen Sicherheitsmethoden
- Rückfall-Szenarien für QKD, PQC und klassische Sicherheitsmethoden

Funktionsprüfungen
Ziel: Sicherung der gewünschten Interoperabilität von klassischen und Quanten-Komponenten.

- Testen der Schnittstelle zwischen klassischen und Quanten-Komponenten: Validierung der Zeitsynchronisation zwischen Quantensignalen und klassischen Systemen sowie Testen der QKD-Steuerprotokolle
- Validierung des Protokollstapels: Sicherung der Integration von QKD in IPsec, TLS oder PQC

Leistungstest
Ziel: Messung und Optimierung von Durchsatz, Latenz, Fehlerraten, Anzahl der Sitzungen und Sitzungsaufbauzeit.

- Wichtige Kennwerte: Quanten-Bitfehlerrate (QBER), sichere Schlüsselrate (Bit/s), Latenz und Jitter, Anzahl der Sitzungen, Sitzungsaufbauzeit
- Anwendungsfall: Messung der sicheren Schlüsselgenerierung und des Schlüsselverbrauchs in hybriden Verschlüsselungsszenarien

Sicherheitstest
Ziel: Validierung quantensicherer und hybrider Kryptographie-Resilienz.

- Simulation von Angriffen, wie PNS, Man-in-the-Middle und Side-Channel
- Prüfung des sicheren Rückfalls auf PQC
- Testen der Entropie-Qualität von Quanten-Zufallsgeneratoren (QRNG)

Testen der Umgebungsschicht und der Physical Layer
Ziel: Sicherung einer robusten Leistung unter praktischen Einsatzbedingungen.

- Testen der Glasfaser auf Dämpfung, Dispersion und Polarisationseffekte
- Koexistenz von klassischem und Quanten-Verkehr in DWDM-Systemen
- Atmosphärische Tests für die optische Freiraumübertragung (FSO), z. B. Satelliten-Strecken

Integrationstest in Prüfständen
Ziel: Emulation produktionsnaher Umgebungen.

- Kombination von Live-Faserstrecken mit emulierten Quanten-Knoten
- Bereitstellung in nationalen oder privaten Quanten-Prüfständen

Integration von AIOps und Monitoring
Ziel: Nutzung von KI/ML zur Überwachung und Anpassung hybrider Netzwerke

- Echtzeit-Analyse sowohl klassischer Kennwerte als auch von Quanten-Kennwerten
- Nutzung der Anomalie-Erkennung zur Ermittlung von Manipulationen oder Leistungsverschlechterungen
- Echtzeit-Visualisierung und -Alarme zur Ermittlung des Status hybrider Übertragungsstrecken

Testbereich	Klassische Komponente	Quanten-Komponente	Tools/Konzepte
Migration	Kombination der unten stehenden Komponenten	Kombination der unten stehenden Komponenten	Kombination der unten stehenden Komponenten
Funktion	Netzwerkstapel, Streckenführung	QKD, QRNG	Protokollanalysatoren, QKD-Konsolen
Leistung	Bandbreite, Jitter	QBER, Schlüsselgenerierungsrate	Fasertester, NetSquid, QuISP
Sicherheit	Firewall, VPN, PQC	Simulation von Quanten-Angriffen	Penetrationstest, Side-Channel-Tools
Physical Layer	DWDM, Glasfaser, HF	Photonen-Übertragung	OTDR, faseroptische Sensortechnologie, Polarisations-Tools
Integration und Monitoring	Orchestrierung, AIOps	Schlüsselnutzung, Fehlererkennung	NMS, AIOps-Dashboards, VIAVI NITRO

Der Einsatz der oben genannten, von VIAVI angebotenen Testlösungen erlaubt, mehrere hybride Szenarien, darunter die Migration, zu testen.

4 ZUSÄTZLICHE ÜBERLEGUNGEN

AIOps

Die künstliche Intelligenz für IT-Operationen (Artificial Intelligence for IT Operations, AIOps) wird bereits in quantensicheren Umgebungen angewendet, um die Sicherheit zu stärken, die Bedrohungserkennung zu automatisieren und den Datentransfer zu optimieren. AIOps kann die quantensichere Sicherheit durch das proaktive Management und die proaktive Sicherung von Infrastrukturen, die Quanten- und Post-Quanten-kryptographische Systeme unterstützen, stärken. Dieses Tool wird kontinuierlich weiter entwickelt und bietet auf funktionaler Ebene mehrere Vorteile:

1. Bedrohungserkennung und Reaktion auf Anomalien: Quantensichere Systeme stützen sich nicht nur auf die Kryptographie, sondern auch auf sichere und stabile Betriebsabläufe. AIOps kann ungewöhnliches Verhalten in Datenflüssen erkennen, die möglicherweise auf einen Lauschangriff, einen physischen Abhörversuch (Anzapfen) an der Glasfaser oder auf Man-in-the-Middle Angriffe hinweisen. Ebenfalls analysiert werden können Log-Protokolle von QKD-Systemen um Anomalien, wie Spitzen bei QBER-Messungen, überraschende Signaldämpfungen und verdächtige Neu-Authentifizierungen von Geräten. Zu diesem Zweck führt AIOps ML-Modelle aus, die an normalem Betriebsverhalten trainiert wurden und helfen, Ausreißer umgehend anzuzeigen.

2. Automatische Infrastruktur-Überwachung: Quantensichere Systeme erfordern häufig latenzarme und stabile Umgebungen. Zu deren Aufrechterhaltung trägt AIOps bei, indem dieses Tool die Latenz, Jitter und Paketverluste in hybriden oder Quanten-Netzwerken überwacht, Routing oder Switching auf Grundlage echter KI-Einblicke optimiert und automatisch auf Verschlechterungen, die den Austausch der Quantenschlüssel oder Post-Quanten-Verschlüsselungsprotokolle beeinträchtigen könnten, reagiert.

3. Adaptive Sicherheitslage: Quantensichere Implementierungen können hybride Systeme (klassische sowie Quanten-/Post-Quanten-Kryptographie) umfassen. AIOps kann die Verschlüsselungsstärke oder Protokollnutzung dynamisch an die wahrgenommenen Bedrohungsstufe anpassen und dann auf Grundlage der beobachteten Systemleistung und des Risikoniveaus die Einführung quantensicherer Algorithmen empfehlen.

4. Kryptographisches Drift- und Compliance-Management: AIOps kann die Nutzung von Legacy- oder nichtkonformen kryptographischen Bibliotheken überwachen und so den Einsatz nichtquantensicherer Algorithmen, wie RSA und EC, anzeigen und den automatischen Ersatz durch PQC-Bibliotheken, wie CRYSTALS-Kyber und Falcon, vorschlagen.

In quantensicheren Umgebungen sind mehrere wichtige Anwendungen für AIOps verfügbar. Dazu gehört die Erkennung und Reaktion auf Bedrohungen durch Überwachung des Netzwerkverkehrs auf böswillige Aktivitäten, um potentielle Cyber-Bedrohungen der Quanten-Ära zu erkennen, noch bevor sensible Daten kompromittiert werden können. Eine weitere Anwendung ist die Bewertung der kryptographischen Infrastruktur und die Automatisierung des Übergangs zu PQC-Standards zur Gewährleistung der langfristigen Sicherheit.

Zusammengefasst lässt sich sagen, dass AIOps quantensichere Systeme stärkt, indem dieses Tool Bedrohungen und Anomalien im Stapel erkennt, die operationale Integrität von QKD- oder PQC-Bereitstellungen gewährleistet, eine dynamische Verteidigung, einschließlich der automatischen Anpassung der Verschlüsselung, ermöglicht sowie die Einhaltung quantensicherer Standards überwacht.

Lösung von VIAVI: NITRO® AIOps

NITRO AIOps von VIAVI ist eine erweiterte, intelligente Ende-zu-Ende, Top-Down-Engine, die sich als übergreifende Lösung nahtlos in Umgebungen mehrerer Anbieter, Technologien und Bereiche integrieren lässt. Die KI-gestützten Funktionen von NITRO AIOps bieten eine einzigartige Gelegenheit, die Komplexität des NOC zu reduzieren und den Betrieb zu rationalisieren. NITRO AIOps bietet zahlreiche Vorteile, darunter:

- Senkung der Gesamteinsatzkosten (TCO): Durch den Einsatz von KI und vorausschauender Wartung verringert NITRO AIOps effektiv kostspielige Ausfallzeiten. Erweiterte AIOps-Funktionen in den Bereichen Ressourcenzuweisung, Kapazitätsplanung und Optimierung verbessern die Kostenkontrolle zusätzlich und fördern einen nachhaltigen Netzbetrieb selbst in den komplexesten Szenarien.
- Senkung der Betriebskosten (OPEX): NITRO AIOps verbessert das Netzwerkmanagement, die Fehlerdiagnose und -behebung und die Service-Assurance durch Automatisierung, wodurch das volle Potenzial von Zero-Touch-Operationen ausgeschöpft und die betriebliche Effizienz gesteigert werden.
- Digitale Transformation/5G-Monetarisierung: NITRO AIOps ermöglicht die digitale Transformation des Netzwerks durch Echtzeitanalysen und vorausschauende Wartung, indem Probleme erkannt werden, bevor sie den Nutzer beeinträchtigen. Seine Selbstheilungsfähigkeiten optimieren die Leistung und gewährleisten selbst bei Spitzenlasten ein nahtloses Nutzererlebnis.

Feldtests der Glasfaser in Quanten-Netzwerken

Die Ausführung von Feldtests an der Glasfaser spielt eine sehr wichtige Rolle in Quanten-Netzwerken, da diese sich bei der Sicherung der Kommunikation auf die extrem instabilen Quantenzustände stützen. Selbst kleinste Mängel oder Unstimmigkeiten in der Glasfaser-Infrastruktur können das Quantensignal unterbrechen oder komplett zerstören.

Glasfaserbasierte quantensichere Netzwerke reagieren äußerst empfindlich auf Störungen auf der Physical Layer und sind von einer hohen Faserqualität abhängig. Im Feld ausgeführte Tests stellen sicher, dass die Glasfaser den sicheren Austausch der Quantenschlüssel unterstützt.

In hybriden Netzwerken werden viele quantensichere Bereitstellungen die vorhandenen Glasfasern, die bereits für die Telekommunikation mit klassischen Daten genutzt werden, verwenden. Feldtests verifizieren, dass die Glasfasern sowohl klassischen als auch Quanten-Verkehr bewältigen, sicher und ohne Rauschen oder Interferenzen betrieben werden können sowie die Anforderungen erfüllen, die an die quantensichere Bereitstellung gestellt werden.

Daher sind Feldtests an der Glasfaser für die quantensichere Vernetzung, insbesondere für die QKD, unbedingt erforderlich, da sie die Signalintegrität für die Übertragung der Quantenschlüssel gewährleisten, zu einer für die Sicherheit unverzichtbaren niedrigen Fehlerrate beitragen und Schwachstellen aufzeigen, die die quantensichere Verschlüsselung kompromittieren könnten.

Lösung von VIAVI: OneAdvisor 800

Der OneAdvisor 800 von VIAVI wurde mit dem Ziel entwickelt, die sich immer weiter entwickelnden Netzwerk-Tests zu vereinfachen, die benötigt werden, um den Betrieb einer Vielzahl unterschiedlicher drahtgebundener und drahtloser Netzwerke aufrechtzuerhalten. Das modulare Design der Plattform OneAdvisor 800 versetzt die Netzwerktechniker in die Lage, mühelos zwischen eine Vielzahl unterschiedlicher Testszenarien, die grob nach den drei Kategorien Mobilfunk, Transport und Glasfaser unterschieden werden, zu wechseln.

Der OneAdvisor 800 besitzt eine intuitive Benutzeroberfläche mit Berührungssteuerung und unterstützenden Apps, die die Techniker durch die Bedienung führen. Hinzu kommen verschiedene Module und Leistungsmerkmale für alle Netzwerkanwendungen zur schnellen und fehlerfreien Testausführung, zur zuverlässigen Einrichtung und Überprüfung neuer WDM-Dienste (CWDM, DWDM, MWDM, LWDM) sowie zur Einhaltung zukünftiger Anforderungen für die Highspeed-Aktivierung von Diensten, für die optische Spektrumanalyse (OSA) sowie für Ethernet/BERT-Tests. Zusammenfassende Berichte halbieren den Umfang der zu bearbeitenden Testergebnisse.

An Glasfasern werden zahlreiche Tests ausgeführt, wie die Inspektion der optischen Verbinder, OTDR und PON-OTDR, bidirektionale IL/ORL und OTDR (TruBIDIR) mit FiberComplete PRO™, optische Spektralmessungen mit einem DWDM OTDR sowie erweiterte Dispersionsmessungen für Qualifizierungen und Fehlerdiagnosen an Seekabeln, terrestrischen DWDM Highspeed-Transportnetzen, Funkzugangsnetzen (RAN) für 4G/5G (Backhaul, Midhaul, Fronthaul), Tests von Rechenzentren, Campus-Netzen und der DCI-Zusammenschaltung von Rechenzentren, von FTTH/PON-Netzen (alle Standards, unsymmetrische oder indexierte Topologien), DWDM-Zugangsnetze für DAA, R-PHY und C-RAN sowie Enterprise/LAN-Netze.

Für das Testen von Transportnetzen bietet der OneAdvisor 800 unter anderem diese Vorteile:

- **Leicht und handlich:** Einer der kleinsten 400G/800G-Tester auf dem Markt.
- **Beispiellose Kühlung:** Branchenführend bei portabler 400G/800G-Technik für mühelos zu kühlende ZR-Steckmodule.
- **Lange Akkulaufzeit:** Für stundenlangen netzunabhängigen Betrieb auf mehrere Akkus skalierbar.
- **Breites Testspektrum:** Die Modularität ermöglicht den Aufbau einer Komplett-Testlösung für verschiedene Leitungsraten und Protokolle
- **Flexibel:** Testet Glasfaser (OTDR, OSA) und alle Ethernet-Raten (800G, 400G, 200G, 100G, 50G, 40G, 25G, 10G und 1G).
- **Für verschiedene Optiken:** Bereit für QSFP-DD800/QSFP-DD/QSFPx, OSFP800/OSFP, SFP-DD/SFPx sowie Unterstützung von voll-kohärenter Optik.

Lösung von VIAVI: INX™ 760

Das Glasfaser-Prüfmikroskop INX 760 ist ideal für Servicetechniker geeignet, da es mit seiner beispiellosen Effizienz stets makellose Glasfaseranschlüsse gewährleistet. Dieses Mikroskop ist das Ergebnis von mehr als 25 Jahren wegweisender Innovation und Erfahrung und setzt neue Maßstäbe für die Inspektion und Analyse der Faserendflächen der nächsten Generationen. Obgleich die Faserinspektion bei vielen Feldtechnikern inzwischen zur Standardvorgehensweise gehört, stellen Verunreinigungen weiterhin die Hauptursache für Störungen in optischen Netzen dar. Da immer mehr neue Verbindertypen auf den Markt gebracht werden, die Anzahl der im Feldeinsatz verwendeten Steckverbindungen steigt sowie neue Glasfasertechniker die Arbeit aufnehmen, steht die Branche vor einem Wendepunkt.

Optical Security and Performance (OSP)

Diese Anwendungsbeschreibung gibt einen Überblick über die mit quantensicheren Netzwerken verbundenen Herausforderungen sowie die von VIAVI empfohlenen Lösungen. Darüber hinaus bietet VIAVI auch beispiellose branchenführende optische Beschichtungen für Quanten-Netzwerke, wie **spektrale Sensorfilter** und **Licht-Sensorfilter** an. Der Geschäftsbereich VIAVI Optical Security and Performance (OSP) wurde 1948 als Optical Coating Laboratory (OCLI) gegründet und hat sich in den mehr als 75 Jahren zum Innovationsführer für individuell angepasste Optik entwickelt. Als vertrauenswürdiger Berater und langfristiger Partner für die Weiterentwicklung leistungsstarker Optik stellen wir Premium-Lösungen zur Verfügung und schaffen ein herausragendes Kundendienst-Erlebnis. Mit unseren Wurzeln in der Ingenieurwissenschaft, der Forschung und dem angewandten Wissensmanagement ist kein anderer Anbieter in der Lage, die optischen Herausforderungen, von einfach bis komplex, mit denen Sie konfrontiert, mit der Kompetenz von VIAVI bewältigen. Angefangen bei Prototypen bis zur Produktion verschaffen unsere Expertise, Technologie und Prozesse unseren Kunden einen wichtigen Wettbewerbsvorteil.

Die OSP-Filtertechnologie hilft unseren Kunden, optische Signale mit der geringstmöglichen Störung und der bestmöglichen Genauigkeit zu extrahieren sowie Oberflächen mit der größtmöglichen Präzision und in jedem geforderten Umfang zu fertigen.

5 ZUSAMMENFASSUNG

Angesichts der bei Quantencomputern gemachten Fortschritte sind die traditionellen Verschlüsselungsmethoden immer stärker gefährdet. Daher hat VIAVI mit TeraVM Security Test eine wegweisende Cloud-konforme Plattform zur Bewertung von PQC-Implementierungen entwickelt. Diese Lösung unterstützt die vom US-amerikanischen NIST geforderten Algorithmen und die Unternehmen beim Übergang zu quantenresistenten Sicherheitsrahmen. Darüber hinaus bietet VIAVI mit seiner Plattform MAP-300 zur Bewertung von Quantenkanälen, dem ONMSi zur Glasfaser-Überwachung und dem FTH-DTSS zur faseroptischen Dehnungs- und Temperaturmessung eine lückenlose Palette von Feldtestern zur Installation, Fehlerdiagnose und -behebung sowie Wartung in Glasfasernetzen an.

Kontakt: +49 7121 86 2222. Sie finden das nächstgelegene VIAVI-Vertriebsbüro auf viavisolutions.de/kontakt

© 2025 VIAVI Solutions Inc. Die in diesem Dokument enthaltenen Produktspezifikationen und Produktbeschreibungen können ohne vorherige Ankündigung geändert werden.

futureproofcomms-quantum-an-xpf-nse-de
30194749 900 0825