HITACHI
Inspire the Next

Mission-critical communication networks are at high risk due to the rising number of attacks, attempts at manipulation and espionage. Hitachi Energy is a leading mission-critical communications systems supplier with trusted solutions for effective cybersecurity.

SECU1

Quantum-safe encryption card

Hitachi Energy

Security in mission-critical systems

Security is a basic requirement of mission-critical communications systems. But mission-critical communication networks are at high risk due to the rising number of attacks, attempts at manipulation and espionage.

Networks and dedicated lines are susceptible to attack in many ways. Optical networks in particular are not secure. Without encryption systems, these networks and lines would be easy prey to hackers. Attacks are possible with a minimum of technical expertise. The optical fiber can be cut (spliced), the splitter coupler method applied (i.e., by bending the line), or non-touching methods can be used where all of the data traffic is read by highly sensitive photo detectors. Afterwards, all the information collated is analyzed. Active attacks like denial-of-service, spoofing, forging and improper usage, viruses, worms and Trojans enhance the options of passive attacks and risk the security of the infrastructure.

Hitachi Energy Trusted Security

Hitachi Energy is a leading mission-critical communications systems supplier. Our “Hitachi Energy Trusted Security” comprises several key elements:

- Complying with all applicable security requirements within our global production facilities
- Security-screened and certified employees
- Central network management
- Deployment of encryption technology with encryption hardware, key management and generation

Hitachi Energy also offers additional security improvements with its SECU1 encryption card for the XMC20 platform. It reinforces the security mindset of integrity, trust, authorization and authentication, and ensures that data, communications, devices and services can be verified.

Quantum-safe and secure communications

SECU1 is the first encryption card for mission-critical infrastructure with truly random numbers based on quantum physics. It improves the cybersecurity of operational communication networks by applying wire speed encryption suitable for real-time applications. The interface card ensures the quantum-safe encryption of mission-critical communications that control and monitor critical infrastructure networks.

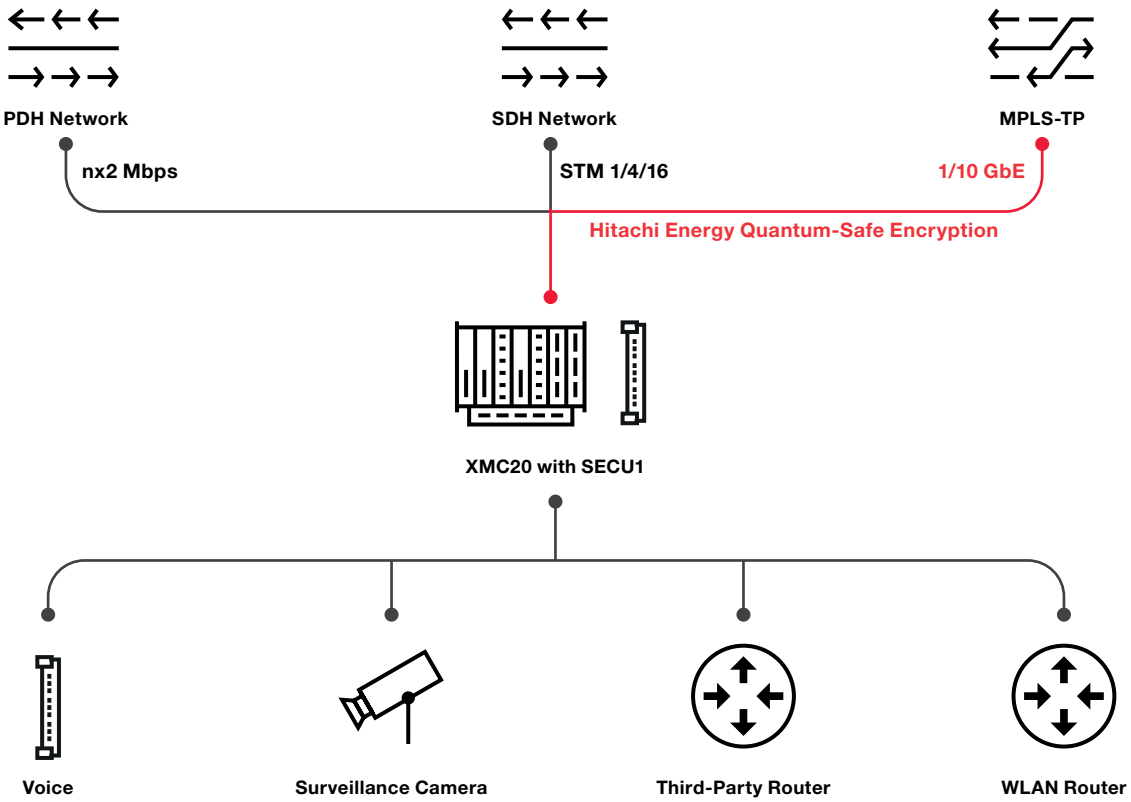
The XMC20 encryption solution, SECU1, ensures uncompromising real-time performance and quantum-safe security. It relies on a physical quantum random number generator (QRNG) as the source for symmetrical cryptographic key generation. The secure key generation mechanism and implemented crypto-agility is termed “quantum-safe.”

The integrated end-to-end data encryption of the XMC20 does not affect critical parameters such as requirements for latency, jitter and asymmetric delay and has no adverse effect on resiliency (OAM protocol) and network timing and synchronization precision (PTP IEEE1588v2 protocol). The SECU1 solution in Hitachi Energy’s MPLS-TP-based wide area communication networks improves the security of operational networks.

By using the SECU1 encryption card in the XMC20, MPLS-TP networks can be operated securely in a node.

The world’s first quantum-safe encryption card that meets the real-time requirements of mission-critical applications.

Encryption of packet-based applications



SECU1 encryption card features

- Offers end-to-end encryption against cyber attacks in packet-based transport networks (MPLS-TP)
- Causes near zero delay in PTP (Precision Time Protocol IEEE1588) packets
- 4 or 8 x SFP+ 1/10 GbE ports per unit
- It offers tamper-protected features to prevent mechanical manipulation
- Also comes with an integrated physical quantum random number generator (QRNG)

Existing XMC20 MPLS-TP infrastructure can be retrofitted with the SECU1 encryption solution.

Layer-2.5 encryption

The Hitachi Energy SECU1 encryption card encrypts all network traffic on Layer-2.5 in the unit. Layer-2.5 encryption has two major advantages over Layer 3-based encryption with IPSec: a 62% savings on overheads and low latency of under four microseconds instead of several milliseconds or even seconds.

Advantages of Layer-2.5 encryption:

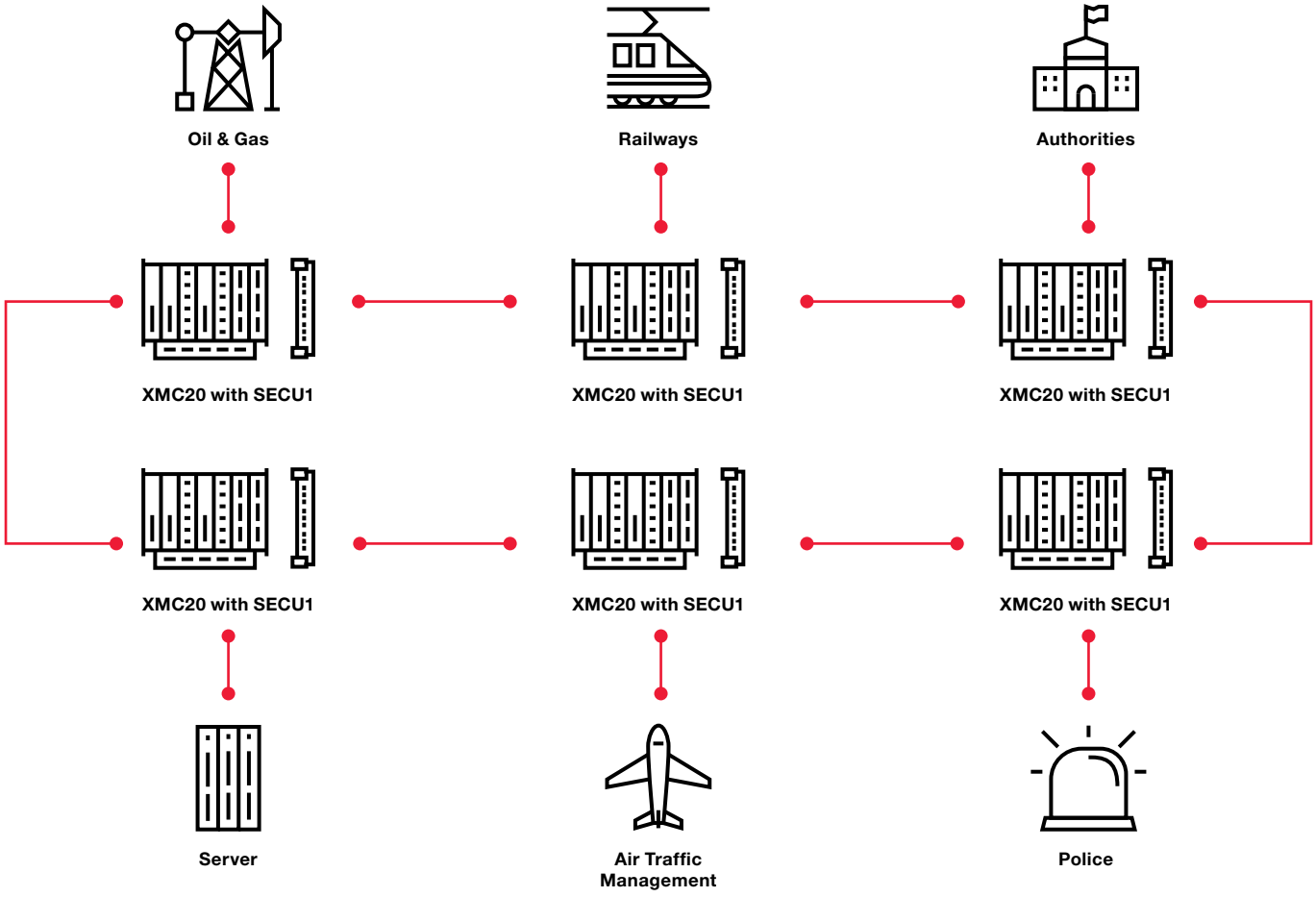
- Minor impact on network performance
- Low latency of under four microseconds
- Transparency of voice, data, video, etc.
- Data throughput of up to 10 Gbps
- Less configuration required due to low complexity

Hitachi Energy offers an encryption solution that doesn't risk availability in mission-critical systems – which is a crucial factor.

Key management

The purpose of key management is to allocate a protected and secure key and to generate and manage the master keys used.

Secure communication in mission-critical communication networks

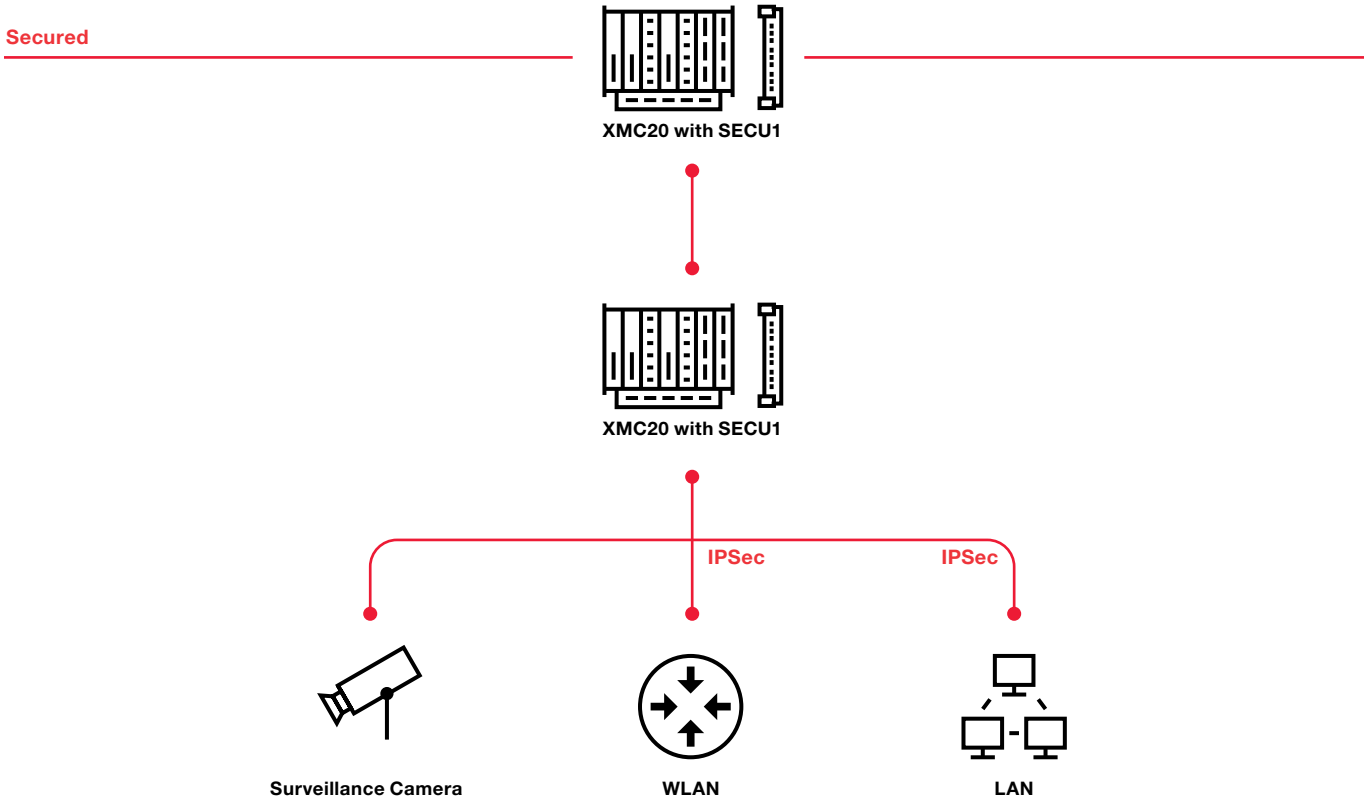


In the case of central key management, key distribution and management is performed with a secure, hardware-based QRNG random number generator via the Post-Quantum Cryptography ready key management server.

The independent network management software monitors the hardware. This process merely checks the signals on the card (keep alive, alarm monitoring, checking redundancy etc.).

The management software can't access the card itself directly. The keys must be distributed in a way that is highly trustworthy and protected. This can also be done by generating the keys locally. The decentralized approach specifies that all nodes must be able to communicate with one another. In decentralized systems there is no single-point-of-failure because of dependence on infrastructure. This method prevents the creation of network islands.

Encryption without changing the main assembly



Quantum-safe

Encryption is only as secure as the random numbers generated and the key it‘s accessed with. To maintain confidentiality and integrity in communications securely, the encryption technology is very important for the operators of mission-critical communication networks. Conventional mathematical keys are often not sufficient to guarantee adequate protection.

For the SECU1 encryption card on the XMC20 platform, Hitachi Energy uses a hardware-based QRNG to generate highly secure keys that really are random. This technology uses a method that incorporates the physical properties of light to generate truly random encryption keys

An IDQ quantum key distribution (QKD) server can be optionally added to the XMC20 solution. The key exchange is executed via the QKD server which is connected via dark fibres. As a result, a man-in the-middle attack is prevented completely, as the mere attempt at reading the key will involve a change in the polarisation condition of the photons and the attack will be noticed.

Trustworthiness

Encryption and authentication is done through the most secure, state-of-the-art, verified and recommended algorithms currently available to guarantee maximum security.

- Master Key (session key encryption)
- Session Key (user traffic encryption)
- The Atomic master key exchange without interruption.

For symmetrical encryption, the AES-GCM (Galois Counter Mode) encryption and authentication algorithm with a key length of 256 bit is applied. The session keys are updated every 60 seconds and offer fully automatic key management based on the “deploy and forget” principle.

Quantum-safe secure communications

The world's first encryption card that meets the real-time requirements of mission-critical applications

Deploy & forget

Without changing the network infrastructure, the SECU1 can be integrated into the existing network easily. This is called "bump-in-the-wire deployment". The unit is operated in a free slot on the XMC20 subrack and connected with the core unit via an SFP. As a result, no changes on further end devices nor a reorganisation of the network are required. IPSec installations on the other hand are complex and time-consuming.

Failsafe operation

Failsafe operation plays a vital role in missioncritical networks. Therefore the unit can be installed in a redundant failsafe setup.

Flexibility

Programmable FPGAs allow maximum operational flexibility. The technology offers better customisation and is ideal for high-speed encryption with a data throughput of up to 10 Gbps. Therefore, the solution can be adapted to future changes or expansion, offering optimum, long-term protection of investments.

Compatibility

Encryption in the node means that existing terminal equipment that supports no or weak encryption can still be used. This saves significant network-expansion costs. The Hitachi Energy cyber protection solution offers highly secure end-to-end encryption for MPLS-TP-based infrastructure and can be added to existing networks.

Backdoor-free

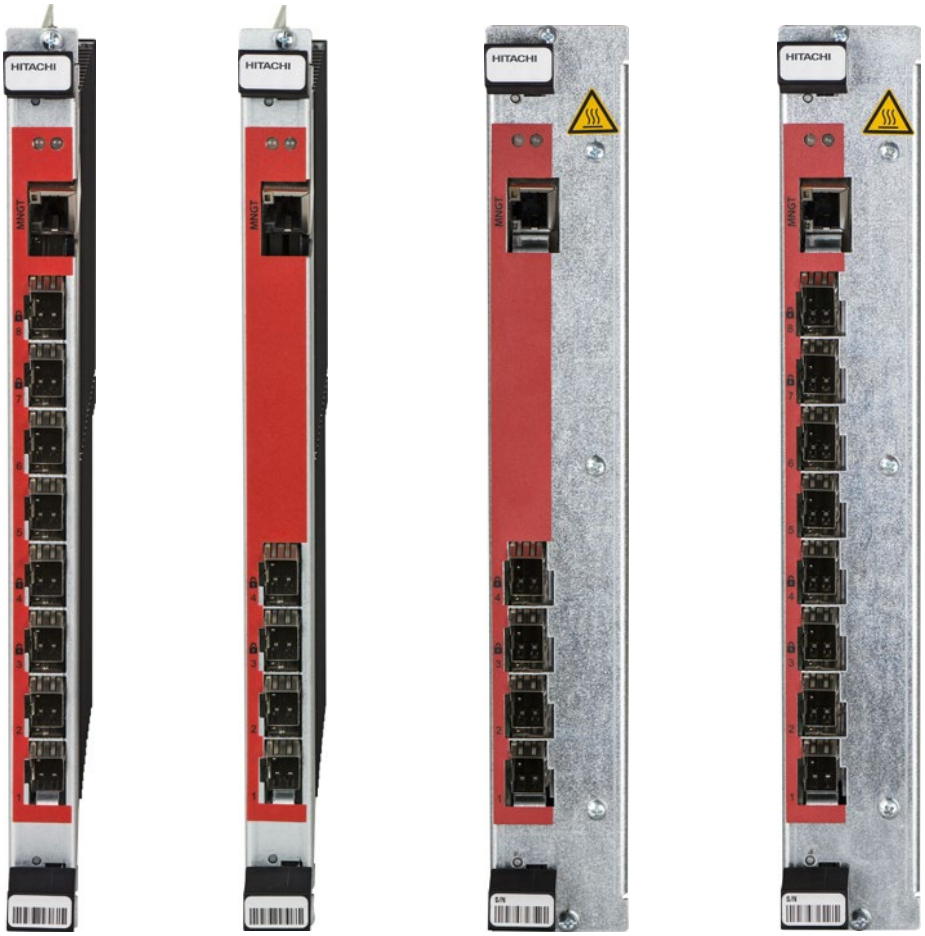
Hitachi Energy guarantees a backdoor- and bug-free solution. The products are made and developed in Switzerland and Europe.

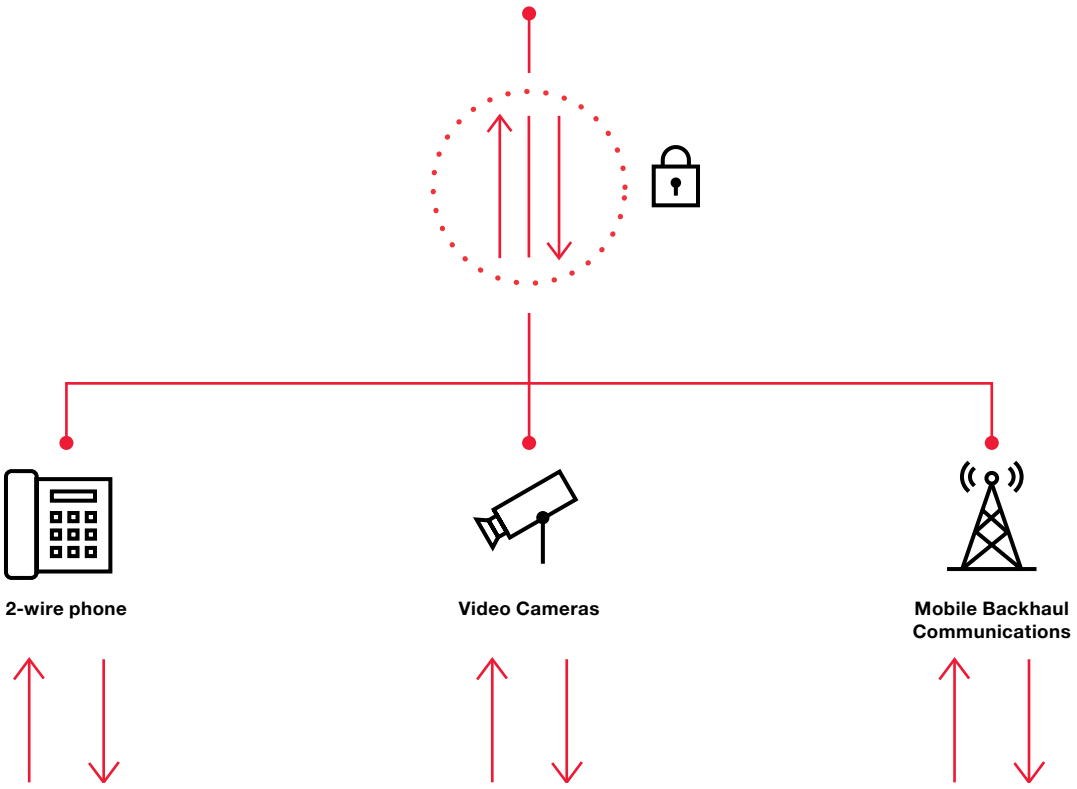
Future-proof cybersecurity

Hitachi Energy has redefined security in mission-critical systems (MCS) by integrating strong encryption into the XMC20 platform and by partnering with ID Quantique from Switzerland. IDQ is the leading manufacturer of quantum-safe network encryption, quantum key generation (QRNG) and quantum key distribution (QKD) devices.

Hitachi Energy's cybersecurity solution offers a future-proof way of safeguarding investments thanks to its robustness and ability to adapt. Hitachi Energy's specialists in the cybersecurity competence centre are ready to support customers from the planning phase to operation of the infrastructure.

SECU1 Quantum-safe encryption card





Hitachi Energy
marketing-update@hitachienergy.com
hitachienergy.com

4CAE000841