CERTIFIKOVANÉ KRYPTOGRAFICKÉ PROSTŘEDKY JAK PRO OCHRANU UI, TAK PRO KRITICKOU INFRASTRUKTURU

SCADA SECURITY KONFERENCE 15. 5. 2025

PAVEL KOTYK
Rohde & Schwarz - Praha, s.r.o.

ROHDE&SCHWARZ
Make ideas real

NÁRODNÍ KRYPTO

- Národní politika kryptografické OUI 11/2024 pro roky 2024-2030 (výňatky)
  - Zvýšení podílu národních kryptografických prostředků
  - Následný dokument „Implementační plán ….“
  - Pokročilé technologie umožňují vytvářet KP s vysokou komplexitou, ale:
    - Riziko „zadních vrátek“
    - Spolehlivost FW
  - Post kvantová kryptografie
  - Vývoj národních algoritmů je extrémně náročný
  - U komerčních subjektů je vývoj KP vnímán jako nerentabilní
  - Bez dotací ze státního rozpočtu je takový vývoj nemožný

NÁRODNÍ KRYPTO

- Národní politika kryptografické OUI 11/2024 pro roky 2024-2030 (výňatky)
  - Zajištění KOUI v KIS se v současnosti týká především státní správy a to v oblastech obrany, bezpečnosti a zahraniční politiky
  - V ostatních oblastech státní správy a v komerční sféře je KOUI využívána ve velmi malém rozsahu
  - Další potřebu aplikace KOUI lze oprávněně očekávat zejména s prohlubujíc se digitalizací státu i společnosti
  - Právě rostoucí závislost společnosti na KIS s sebou přináší hrozby, které mohou výrazně ohrozit bezpečnost a funkčnost všech oblastí státu.

GEOPOLITIKA PO LEDNU 2025

- Dodatelnost
- Technologická závislost
- MAGA nebo MEGA
- Zámořské, národní nebo EU řešení

AGENDA 15/5 SCADA

- Národní „T“ krypto
  - Rodina ED7
  - SW definované krypto s velkým potenciálem
  - Vlastní/ modifikované algoritmy
  - Zkušenost z minulosti ED6-2 a nacionalizace pro ČR
- „V“ šifrátory L2 vrstva
  - Modulární rodina SITLineETH
  - Základní charakteristiky
  - Případové studie
  - Zařízení pouze pro OUI?

ZÁKLADNÍ CHARAKTERISTIKA SPOLEČNOSTI R&S

- Německá rodinná firma (90+ let od založení)
  - Plně nezávislá
  - Dostatečně velká a stabilní (11 000 zaměstnanců, 3mld€ obrat, 10%+ zisk)
- Široký technologický záběr:
  - Měřící technika
  - Radiomonitoring
  - COMINT/ ELINT
  - Zabezpečené spojení…

ZÁKLADNÍ CHARAKTERISTIKA SPOLEČNOSTI R&S

- Široký obchodní záběr:
  - Státní instituce
  - Soukromý sektor
  - Německý trh
  - Evropský trh
  - Celosvětový trh
- Strategický partner německého státu v řadě oblastí:
  - Vojenské spojení
  - Bezpečnostní skenery
  - Satelitní monitoring (FR dcera)
  - COMINT/ELINT
  - Šifrátory….

AGENDA 15/5 SCADA

- Národní „T“ krypto
  - Rodina ED7
  - SW definované krypto s velkým potenciálem
  - Vlastní/ modifikované algoritmy
  - Zkušenost z minulosti ED6-2 a nacionalizace pro ČR

ELCRODAT 7
MODULAR HIGH SECURITY CRYPTO PLATFORM

- Since 2016 development of new high secure crypto platform together with Bundeswehr
- All new Rohde & Schwarz crypto devices are based on the ELCRODAT 7 platform
- ELCRODAT 7 platform consists of a great number of highly innovative features:
  - Software defined crypto
  - Maximum flexibility to address different form factors
  - Interoperability between all ELCRODAT 7 devices
  - Interoperability to all relevant NATO crypto standards
  - Quantum Computer resistant algorithms (PQC)
  - IP capability
  - Highly integrated, SoC based design
  - Unified management system

ELCRODAT 7 CRYPTO PLATFORM
CRYPTO DEVICES

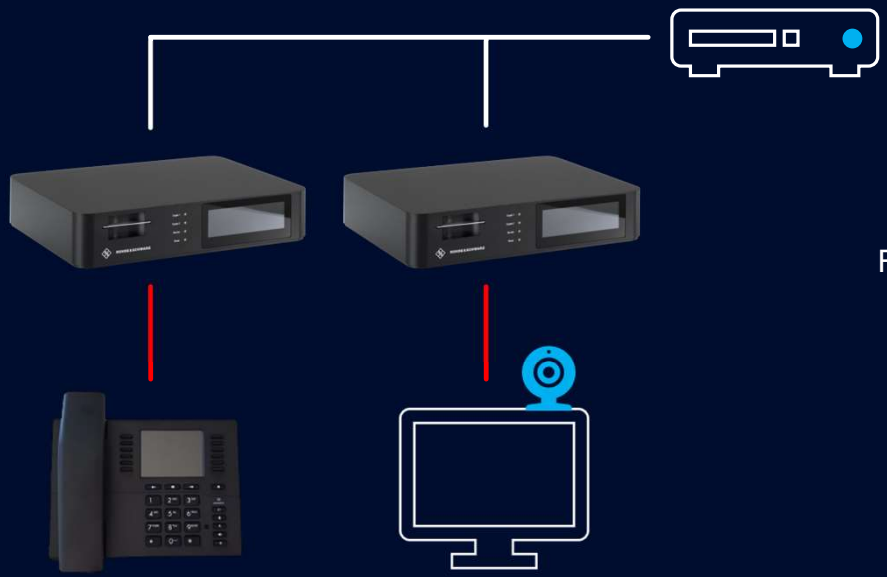
- **R&S®ELCRODAT 7-FN (Flexible Network)**
  - Successor of the R&S® ELCRODAT 6-2 crypto device
  - IP-capable software defined crypto device for E2E-encryption of realtime information (voice, video)
  - Selected for German Governmental crypto modernization program R-VSK
- **R&S® ELCRODAT 7-CT (Crypto Telephone)**
  - Successor of the R&S® ELCRODAT 5-4 crypto telephone
  - IP-capable software defined multi crypto telephone with integrated end device and additional red payloa
  - Developed as next-generation crypto telephone for German Bundeswehr
- **R&S® ELCRODAT 7-MC (Military Crypto)**
  - Successor and form-fit-function replacement of the military crypto device R&S® ELCRODAT 4-2
  - Tactical software defined crypto device with IP- and legacy interfaces
  - Selected as next-generation standard encryption unit for German Bundeswehr
- **Additional form factors**
  - R&S® ELCRODAT 7-DC (Data Center, 19“ rack device)

R&S®ELCRODAT 7-FN CRYPTO SYSTEM

- All-IP crypto system for encrypted transmission of voice, video and data
  - According NATO standard SCIP (Secure Communications Interoperability Protocol)
  - End-to-End encryption between users by using the SCIP standard
- Solution for High-Grade encrypted real-time communications
  up to GEHEIM, NATO SECRET (planned), EU SECRET/SECRET EU (planned)
- Software-based crypto applications SCIP & NINE
- Quantum computer resistant algorithms

R&S®ELCRODAT 7-FN USE CASES

- Connection of a single device
  - Office scenario
  - Phone or video conference system



- Multiple user devices at one R&S®ELCRODAT 7-FN (multi channel mode)
  - Internal red network
  - Up to 1 Gbit/s bandwidth
  - Usage with red telephone switching system

AGENDA 15/5 SCADA

- „V“ šifrátory L2 vrstva
  - Modulární rodina SITLineETH
  - Základní charakteristiky
  - Případové studie
  - Zařízení pouze pro OUI?

SITLINE ETH NG LAYER 2 NETWORKENCRYPTION

Sales presentation

ROHDE&SCHWARZ

Make ideas real

Produktportfolio Netzwerkverschlüsselung

R&S®SITLINE ETH

VS-NfD,
EU RESTRICTED,
NATO RESTRICTED

SecurITy made in Germany

- Secure data transfer in Ethernet networks
- Scalable for a variety of use cases (2 x 100 Gbit/s)
- Highly available and secure key management
- Hardly noticeable latency and maximum bandwidth utilization
- Economic efficiency due to optimal cost-benefit ratio
- Space & cost saving due to maximum port density on one height unit
- Simple and efficient handling through intuitive central management system

R&S®SITLINE ETH NG - ENCRYPTION

R&S®SITLine ETH-S

R&S®SITLine ETH-L

R&S®SITLine ETH-XL

1 - 10 Gbit/s	4 x 1 - 10 Gbit/s	2 x 100 Gbit/s

SITLINE ETH-S

- **Silent Fanless**
- **Small Form Factor**
- **Variant 1G**
  for lines from 10 Mbit/s to 1 Gbit/s
- **Variant 10G**
  for lines with 10 Gbit/s

R&S®SITLine	ETH-S 1G	ETH-S 10G
Number of encryption lines	1 line 2 data ports	
Throughput	10, 100, 1000 Mbit/s	10 Gbit/s
Data Ports MediaType	exchangeable: SFP	exchangeable: SFP+
Management Port	electrical built-in	
Cryptography	AES 256 bit key, Elliptic curve cryptography with 384 bit keys, Strong Random PTG.3	
Power supply	Redundant AC/DC, external	
Fans	Fanless	
Form factor	Rack format (⅓ 19“, 1 RU)	

SITLINE ETH-L

- **Multiple lines on 1 RU - 19-inch rack**
- **High reliability**
  Redundant fans
  Redundant
  power supplies
- **Variant 4 x 1G**
  Four lines each from 10 Mbit/s to 1 Gbit/s
- **Variant 4 x 10G**
  Four lines each 10 Gbit/s

R&S®SITLine	ETH-L 4 x 1G	ETH-L 4 x 10G
Number of encryption lines	4 lines 8 data ports	
Throughput	10, 100, 1000 Mbit/s	10 Gbit/s
Data Ports MediaType	exchangeable: SFP	exchangeable: SFP+
Management Port	exchangeable: SFP (electrical SFP included)	
Cryptography	AES 256 bit key, Elliptic curve cryptography with 384 bit keys, Strong Random PTG.3	
Power supply	Redundant AC/DC, Hot Swap	
Fans	2 x Chassis fans, Hot Swap	
Form factor	Rack format (19‘‘, 1 RU)	

SITLINE ETH-XL

- **Multiple lines on 1 RU - 19-inch rack**
- **High reliability**
  Redundant fans
  Redundant
  power supplies
- **Variant 100G**
  Single line with 100 Gbit/s
- **Variant 2 x 100G**
  Two lines each 100 Gbit/s

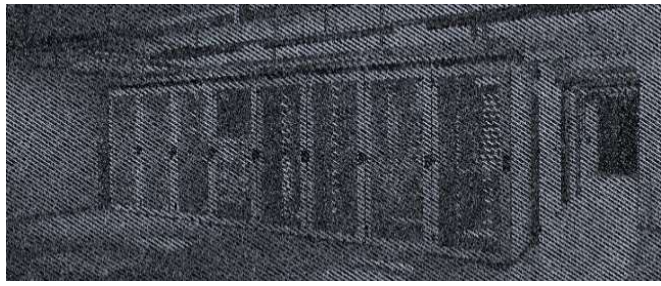
R&S®SITLine	ETH-XL 100G	ETH-XL 2 x 100G
Number of encryption lines	1 line 2 data ports	2 lines 4 data ports
Throughput	100 Gbit/s	2 x 100 Gbit/s
Data Ports MediaType	Optical, exchangeable: QSFP28	
Management Port	exchangeable: SFP (SFP **not** included)	
Cryptography	AES 256 bit key, Elliptic curve cryptography with 384 bit keys, Strong Random PTG.3	
Power supply	Redundant AC/DC, Hot Swap	
Fans	2 x Chassis fans, Hot Swap	
Form factor	Rack format (19‘‘, 1 RU)	

SECURE AND FAST ENCRYPTION NEEDS SPECIALIZED HARDWARE

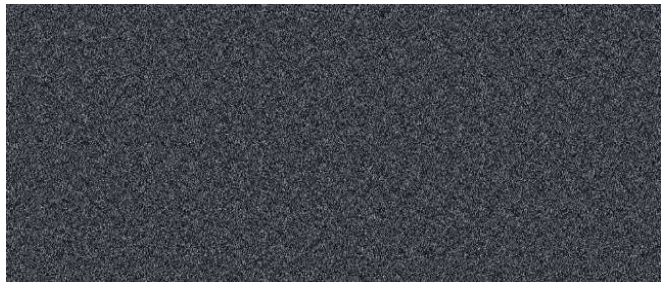
- FPGA architecture for encryption
  - Hardware encryption in microseconds (µs)
  - Utilization of the full bandwidth without performance losses
  - Performance for Big Data and real time applications
- Direct negotiation of security relationships between SITLines
- SITLine is using strong random generated by a PTG.3 card
- Physical tamper protection

Original

Weak Encryption



Strong Encryption



R&S®SITLine ETH

CENTRAL MANAGEMENT

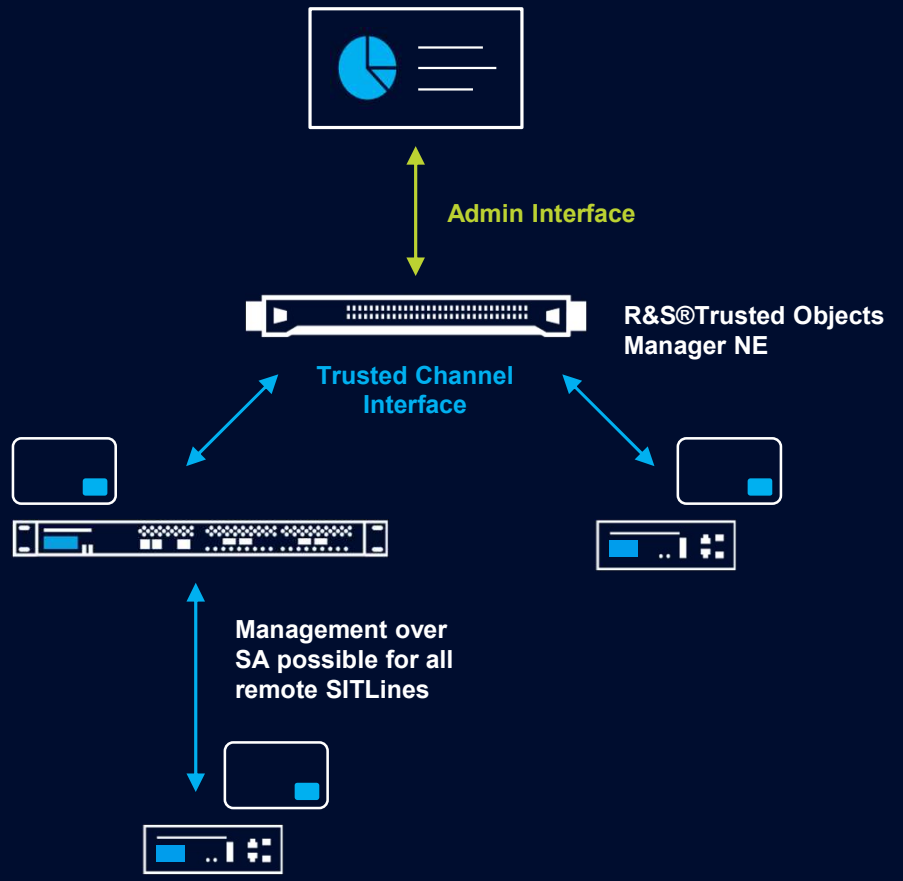
SECURE MANAGEMENT SYSTEM TRUSTED OBJECTS MANAGER NE

- Central core management is the R&S®Trusted Objects Manager
  - Server appliance with hardened OS
  - On-Premise local hosted
  - Trusted Boot with TPM (tamper-resistant)
- IPv6 Support
- VLAN Support
- Change of root certification
- Certificate based login for users
- LDAP / Active Directory
- REST-Interface enables modulations
- Optional Geo redundancy

MANAGEMENT SYSTEM CONCEPT

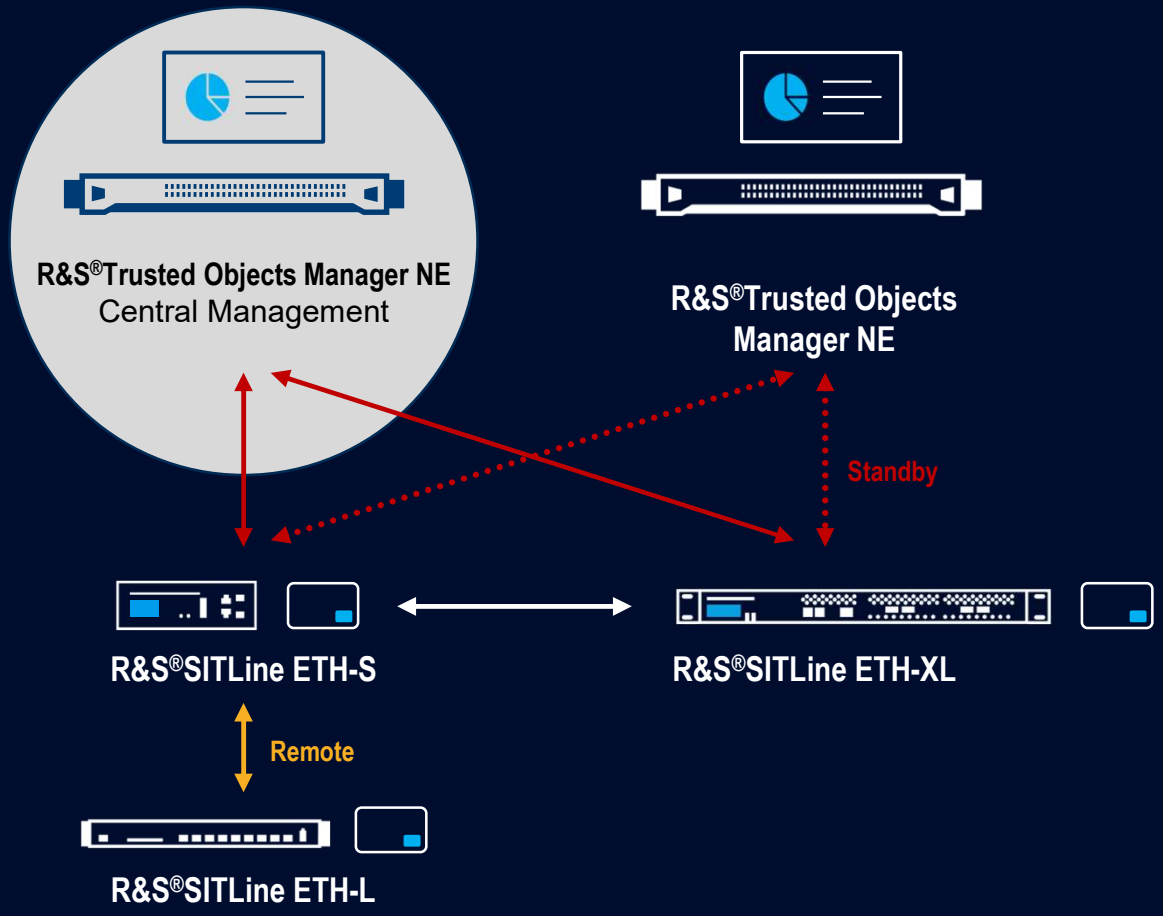
►Two physical separated zones / interfaces:

- **"Admin Interface":** administrable over GUI
- **"Trusted Channel Interface":** Device management
  - SSL/TLS
  - Key size: 512 Bit ECC (Brainpool) to authenticate TLS-connections to the TOM
  - Hash: SHA-512 to authentication TLS-connections to the TOM



R&S®TRUSTED OBJECTS MANAGER NE

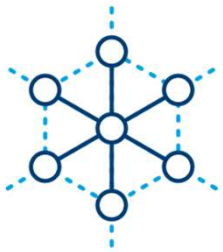
- Comprehensive management of different device families
- Remote management possible without direct connection
- Simple key management via smartcards
- Redundant configuration possible



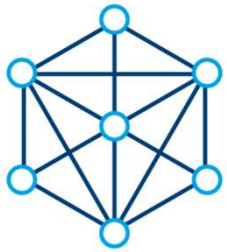
Rohde & Schwarz Cybersecurity

SECURE NETWORKS - POSSIBLE APPLICATIONS

DEPLOYMENT SCENARIOS

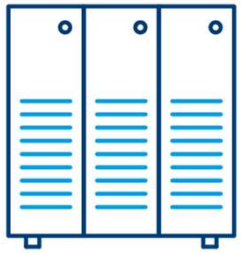


POINT-TO-MULTIPOINT OVER ETHERNET / LAYER 2 - SERVICES



FULLY MESHED MULTIPOINT OVER ETHERNET / LAYER 2 - SERVICES

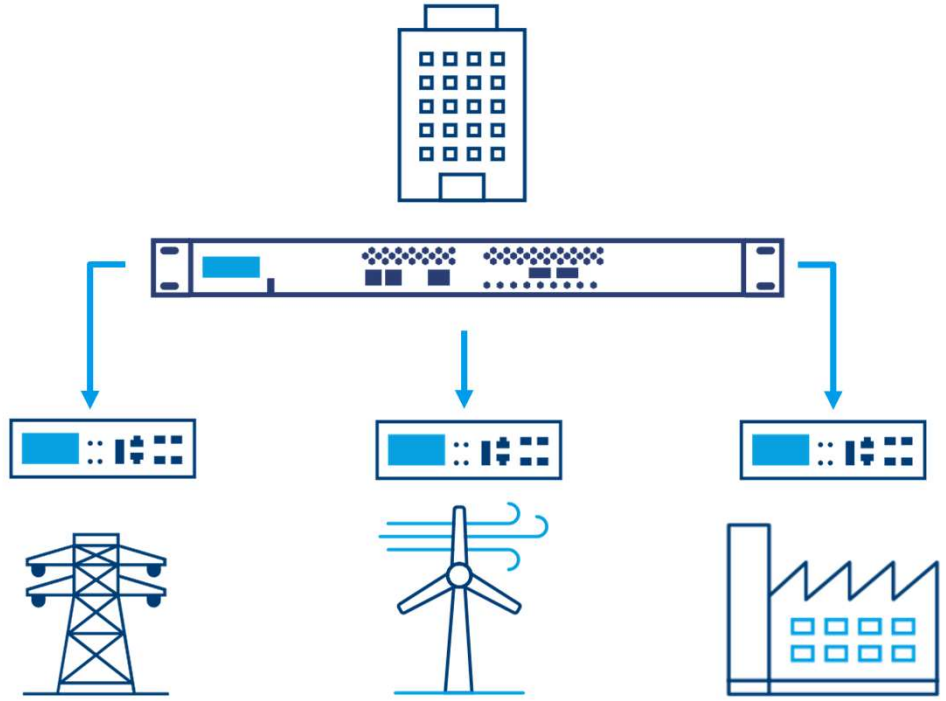
POINT-TO-POINT SERVICES



COUPLING OF DATA CENTERS

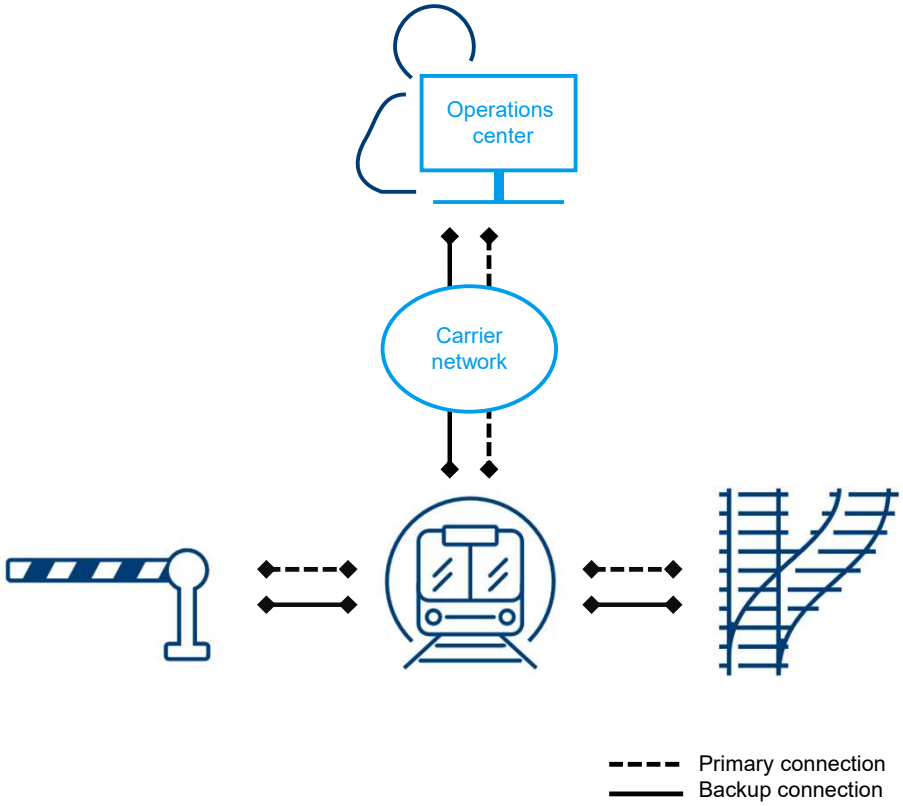
SECURING OF CRITICAL INFRASTRUCTURE

- Example: Securing substations, wind turbines, or remote locations
- Protection of network infrastructure between sites connected via private or public networks
- Resistance to tampering
- High authentication encryption
- Robust devices

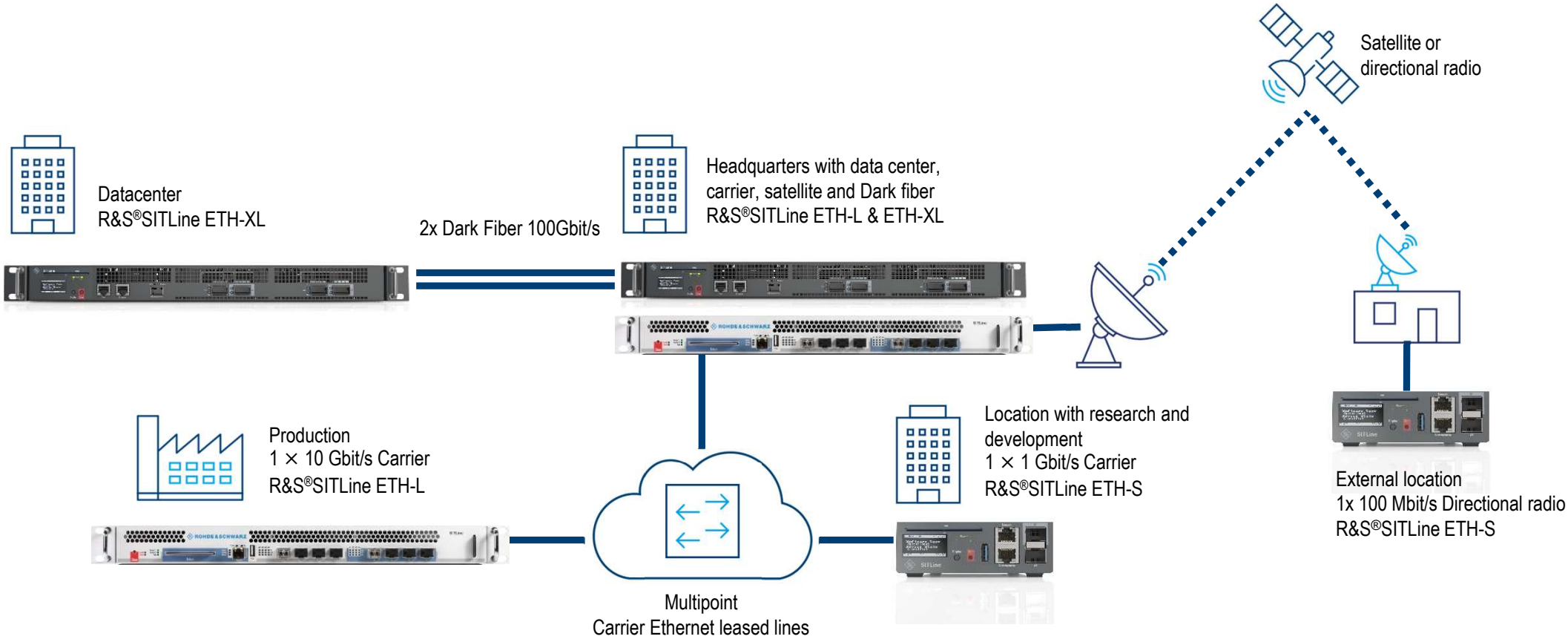


ENCRYPTION FOR SIGNAL AND RAILROAD SWITCH

- Security requirements for control and safety systems, e.g., rail traffic
  - Redundancy
  - Non-interference
  - CRC checksums against transmission errors
- Resistance to tampering
  - Integrity protection
  - Encryption with strong authentication



FOR ALL BANDWIDTHS AND TRANSPORT NETWORKS



MANAŽERSKÉ SHRNUTÍ

- Existuje potřeba definovaná NÚKIB:
  - Národní krypto
  - Šifrovat i mimo oblast státní správy a rámec zákona o OUI
  - Aktuálně nasazené technologie jsou převážně zahraniční, dílem zámořské a vzniká riziko:
    - Dodatelnosti
    - „zadních vrátek“
    - Dlouhodobé podpory
- Vybrané dvě technologie nabízí bázi pro diskusi o řešení shora uvedených problémů

► Kontakt:

Pavel.Kotyk@rohde-schwarz.com

+420 224 323 015

Evropská 2590/33c, Praha 6