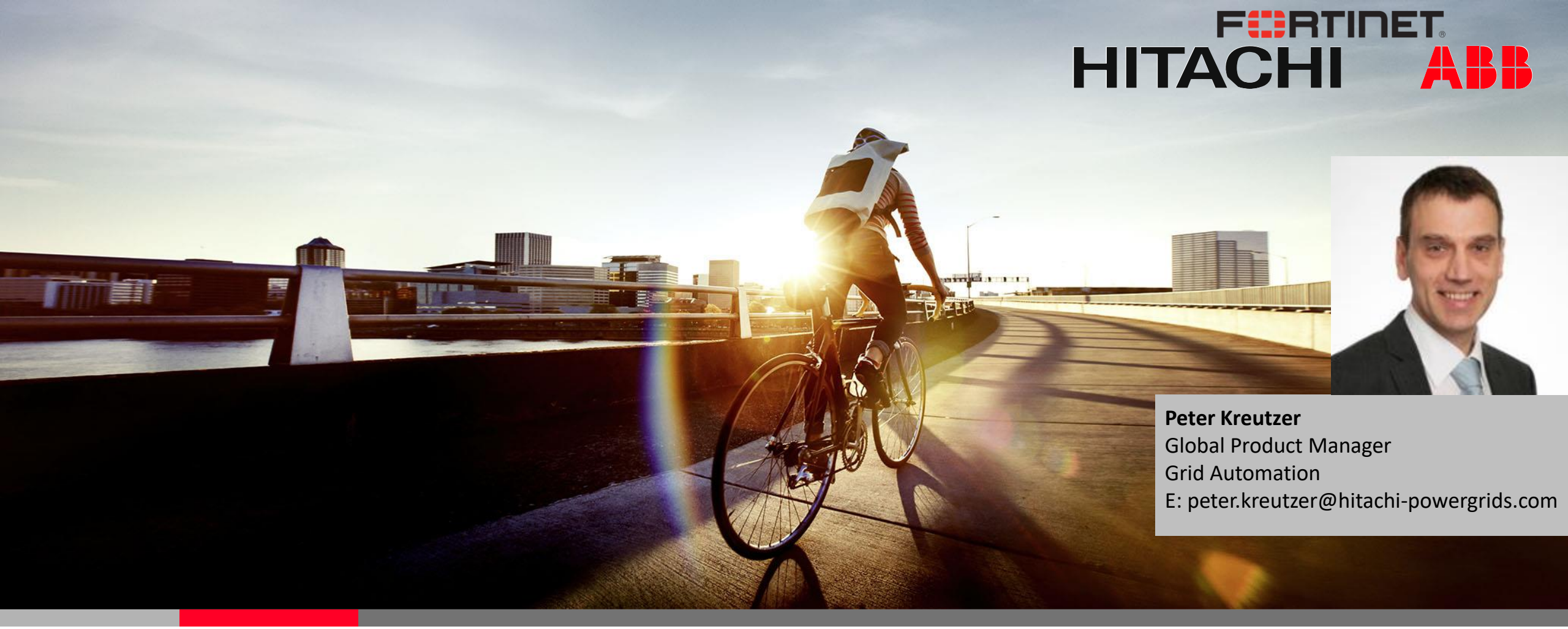


Peter Kreutzer
Global Product Manager
Grid Automation
E: peter.kreutzer@hitachi-powergrids.com

Technology Innovation Panel Session

Incorporating security into the design process to better meet utility requirements

The growing impact of cyber security

Today’s challenges and changes for critical infrastructure

- **Remote working coinciding with a surge in cyber security threat levels compounds cyber security risks**
- **Mitigation: secure operations and infrastructure and embrace the opportunities of the “new normal”**

Cyber related risks have been steadily increasing and COVID-19 malicious cyber activity ongoing

Increased dependency on digital infrastructure to ensure collective resilience

Rapid, unplanned digitization increases the risk and impact of cyberattacks.

COVID-19 is accelerating the digital transformation of businesses and move to cloud

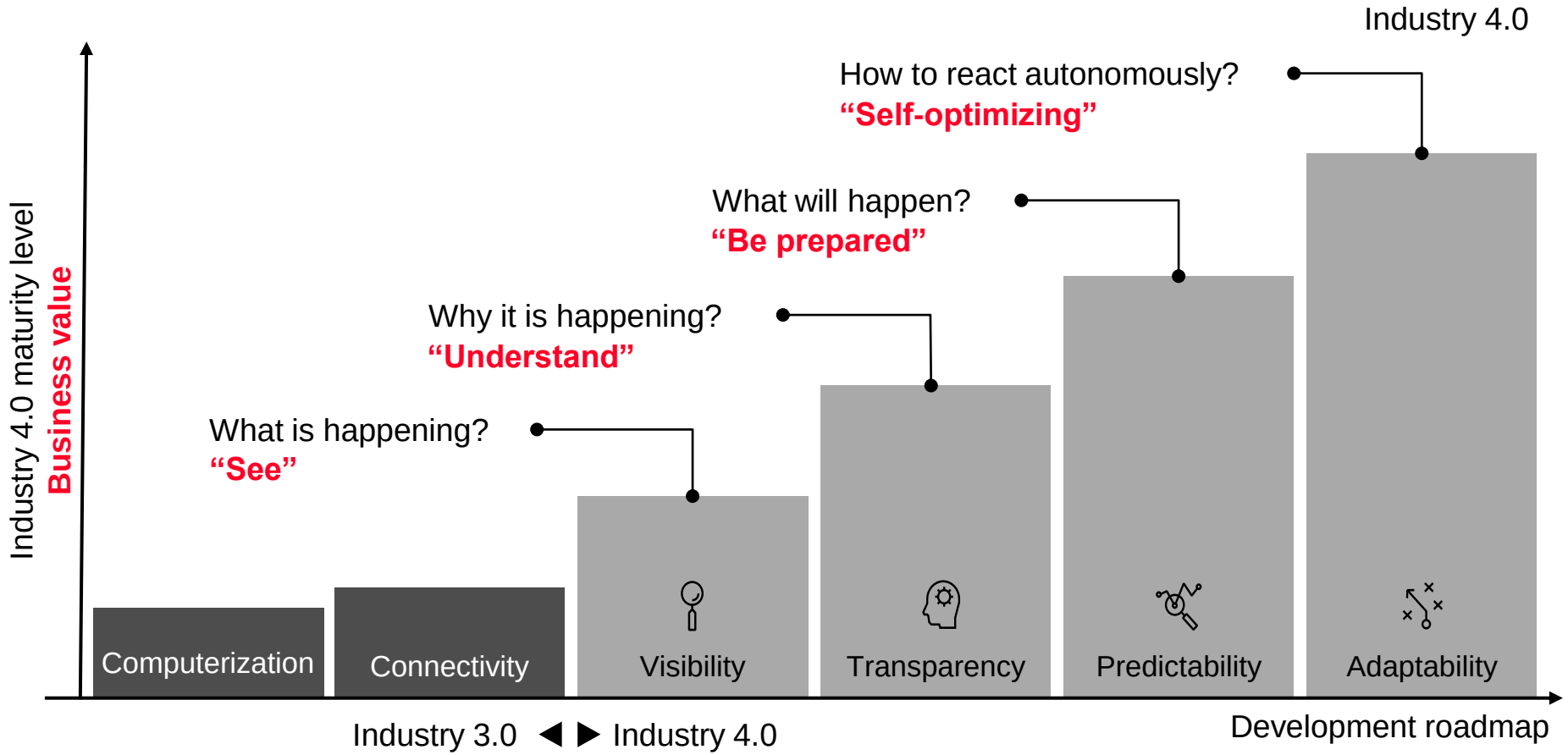
Project execution under increasing cost and time pressure due to social distancing, broken supply chains, fragmented workforces and the rise of video meetings

Remote work as the new norm—country-mandated lockdowns

HITACHI ABB POWER GRIDS

Digital transformation in energy sector

The power of data analysis

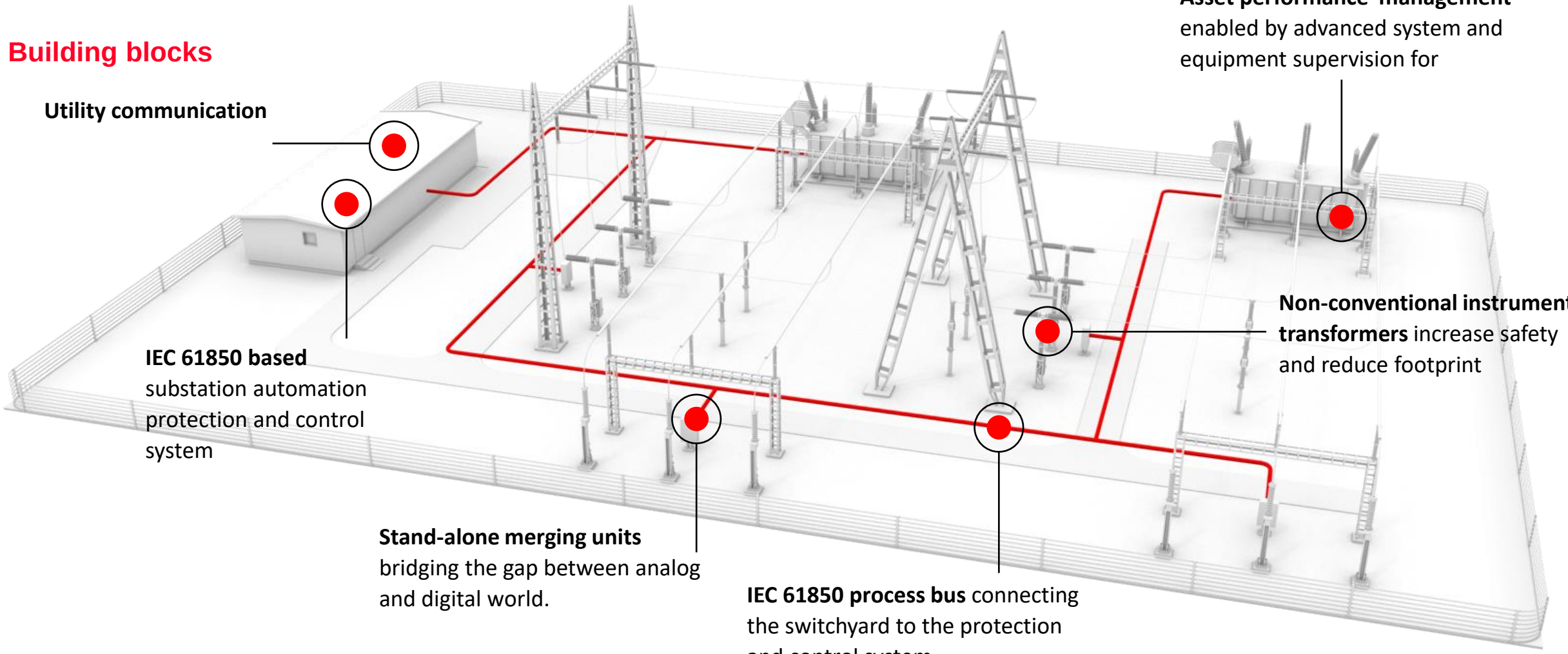


Source: Reinhart, Gunther; 2017; Handbuch Industrie 4.0

HITACHI ABB POWER GRIDS

What is a digital substation

Building blocks



Utility communication

IEC 61850 based substation automation protection and control system

Stand-alone merging units bridging the gap between analog and digital world.

IEC 61850 process bus connecting the switchyard to the protection and control system

Non-conventional instrument transformers increase safety and reduce footprint

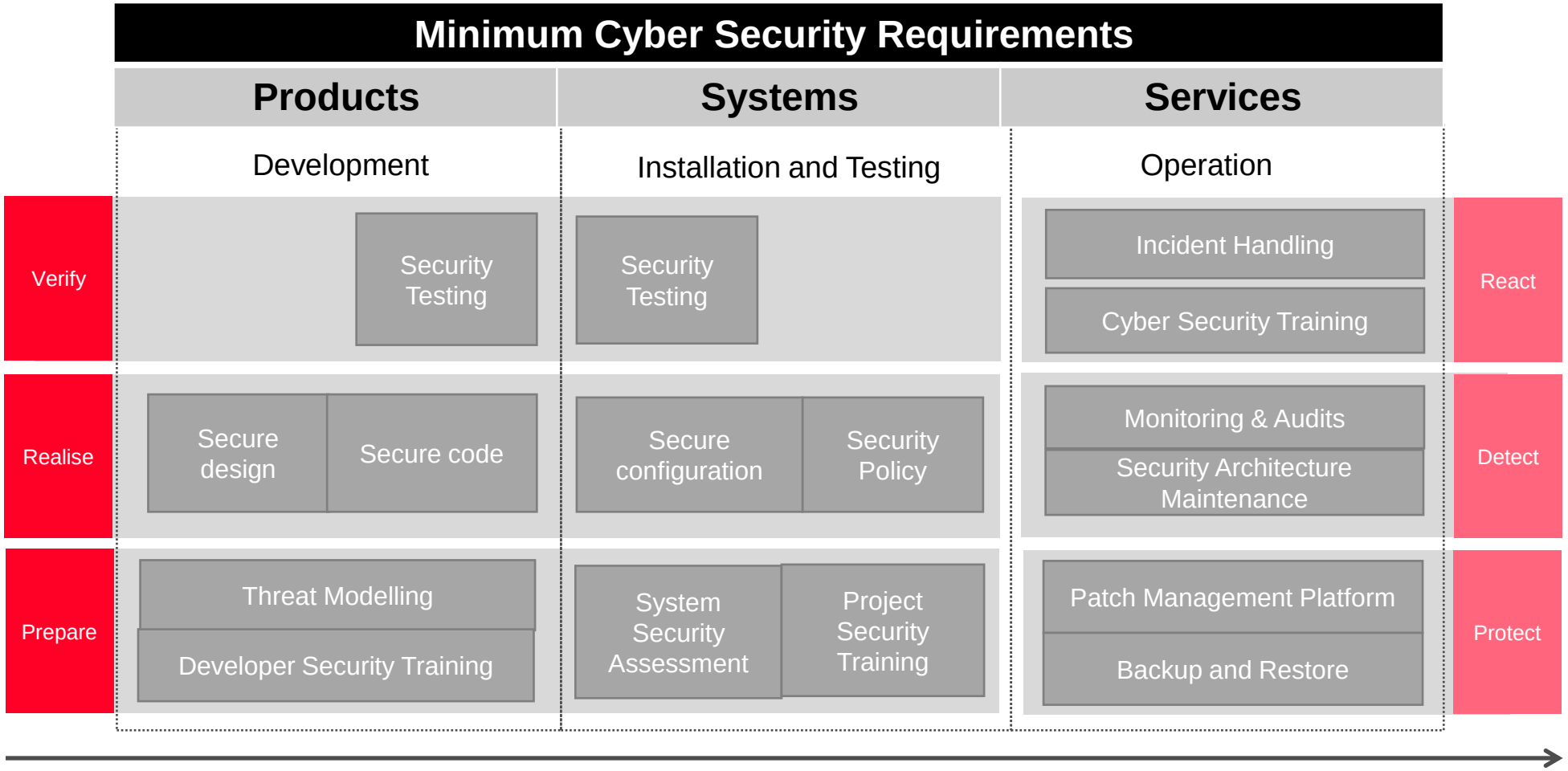
Asset performance management enabled by advanced system and equipment supervision for

HITACHI ABB POWER GRIDS

Our Processes and procedures

Ensure secure product and system delivery

Cyber security throughout the entire product and system lifecycle



We maintain a Secure Development Lifecycle & applies stringent Minimum Cyber Security Rules

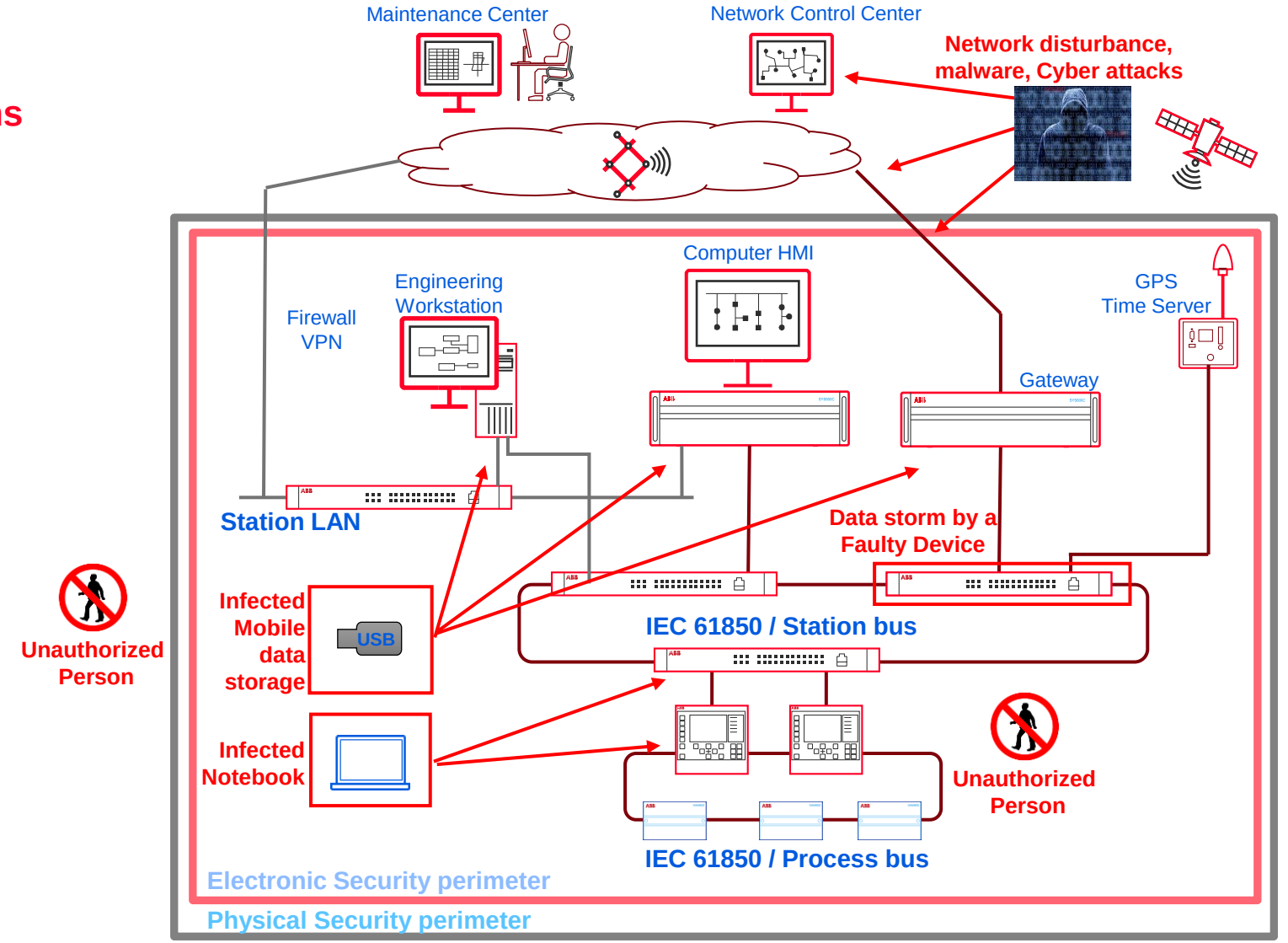
HITACHI ABB POWER GRIDS

Attack scenarios

Building secure products and systems

Understand all attack scenarios in the infrastructure is important

- From outside the substation
  - Through OT connection of WAN
  - Through IT connection of WAN
  - GPS jamming and spoofing
  - …
- From inside the substation
  - Flooding/Jamming with IEC61850 telegrams on station and process bus
  - Unauthorized device
  - Infected devices
  - Mobil storage devices
  - …



Cyber security in Hitachi-Powergrids Products

Protocol hardening

- Fuzz testing all protocols
- Security development life cycle
- Protocol conformance
- Device security testing
- Extensive service and port configuration
- Flooding protection

Account management

- Local users created in the device
- Device tool used to manage users
- Removal of default users and passwords
- Central account management – IEC 62351 with LDAP

Security event logging

- Audit trail
- Reporting on IEC 61850
- Syslog
- Offline log in every device

Role based account control

- User roles
- User rights
- IEC 62351 part 8

Certificates

- Self signed certificates
- Customer signed certificates
- Encryption of communication

Supervision and configuration

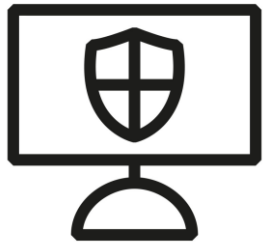
- Self supervision of hardware and software
- Denial of Service protection
- Extensive configuration possibilities
- Maintenance menu

The offering for cyber secured systems

Defense in Depth

Secure Communication

Zoning & Perimeter Protection



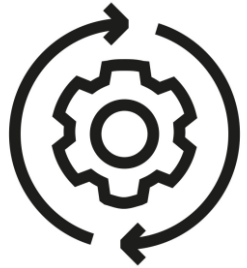
Malware Protection

Patch Management

Backup & Recovery

Account Management

Security Logging & Monitoring

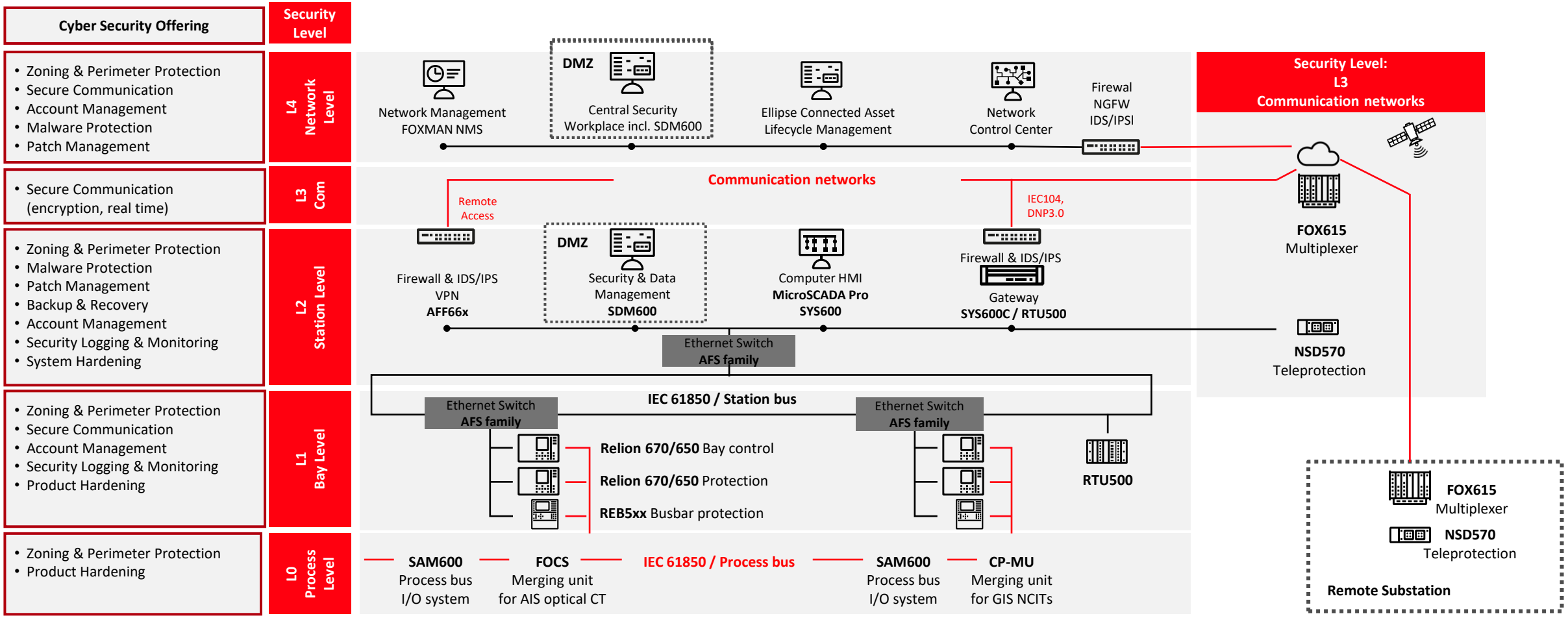


Product & System Hardening

HITACHI ABB POWER GRIDS

Secure system architecture for Grid Automation

Zones according to IEC 62443



HITACHI ABB POWER GRIDS

Ensure Cyber secured system delivery

End-to-end lifecycle solution

Hitachi-Powergrids products and systems for digital substation are thoroughly tested in our System Verification Center (SVC), ensuring they comply with industrial standards and follow the defense-in-depth approach.

All substation automation systems from Hitachi-Powergrids are designed and configured according to best practices and provide a broad range of cyber security measures, which are grouped into three main categories:

1 Monitor
Monitoring features provide real-time security and monitor the health and activity of assets across grid automation systems, including networks and applications

2 Manage
Managing features help users monitor and manage critical activity, including configurations, changes and patches across grid automation systems

3 Protect
Protecting features defend grid automation systems against unauthorized access, attacks, exploits and malware that compromise system availability, performance, security and compliance

Cyber secure systems, operations, and embracing the “new normal”

Helping you to overcome the challenges you face

HITACHI ABB POWER GRIDS

World class local customer service, globally

Hitachi-Powergrids Grid Automation Collaborative Operations Center, Switzerland

Collaboration hub for **40+** ABB Grid Automation engineering & service centers worldwide

24/7 secure remote expert service for substation automation, communication and microgrid systems

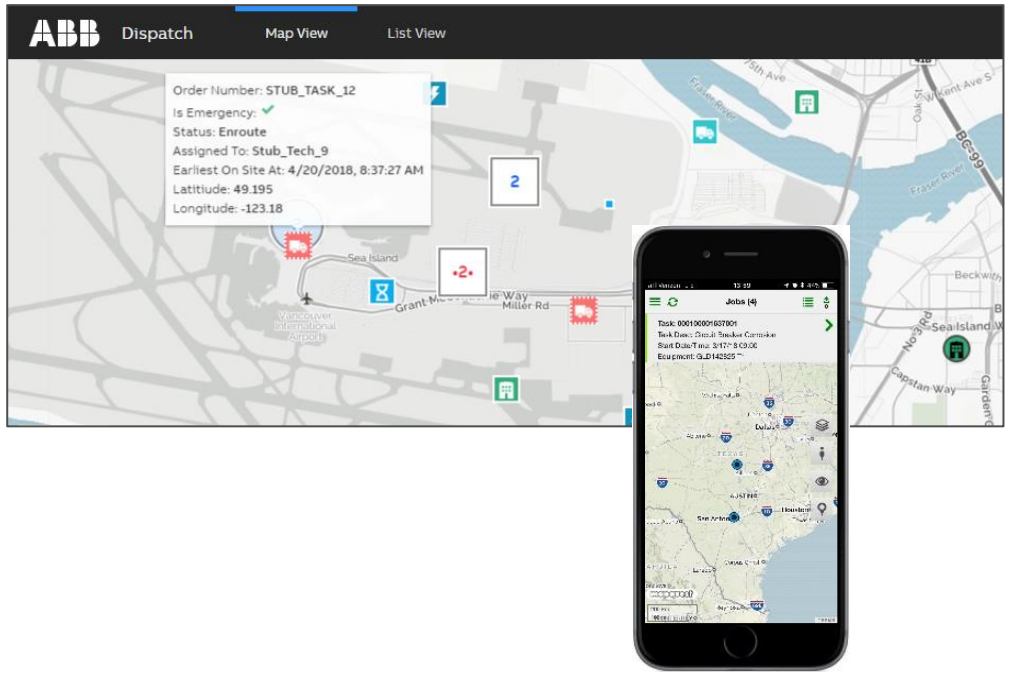
Connected Asset Lifecycle Management deployed as a service to our customers

Foundation for grid automation **Service Agreements**

Site Safety Approval Process for Onsite Activities

Field Service Engineers

Workforce Management

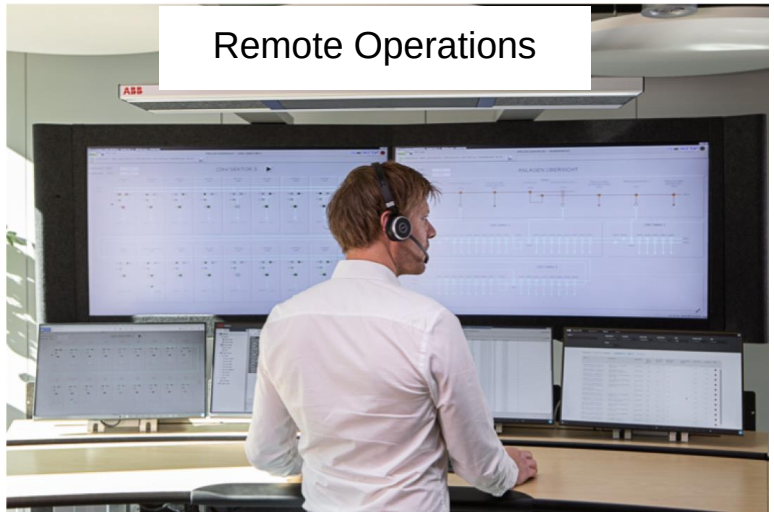


Nobody goes to site, or starts site work, without interacting with the Safety Center for approval

Grid Automation Collaborative Operations Center

Secure remote expert support for Hitachi-Powergrids Field Service Engineers worldwide

Remote Operations



Substation Automation SVC

Cyber Security Test System

Wired Communications SVC

HITACHI ABB POWER GRIDS

Use Case / Remote Factory Acceptance Test

Securely connect People

Internet based Service using secure communication between

- End Customers
- Test Engineers in Test Field area
- Experts in collaborative operation center

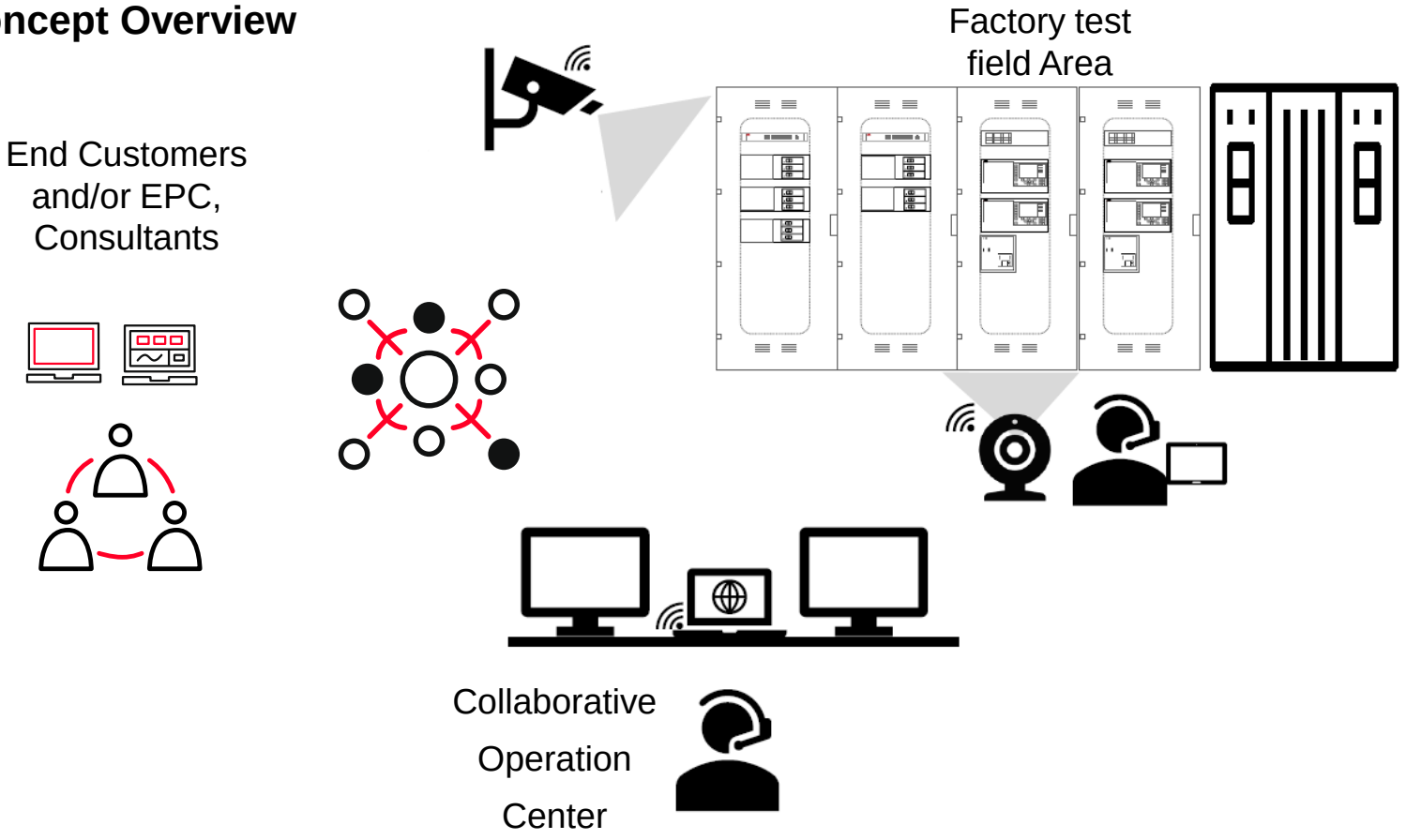
Using

Computer, phones , cameras and voice communication

To share

Documents , Displays , Views on Equipment and Test cases

Concept Overview



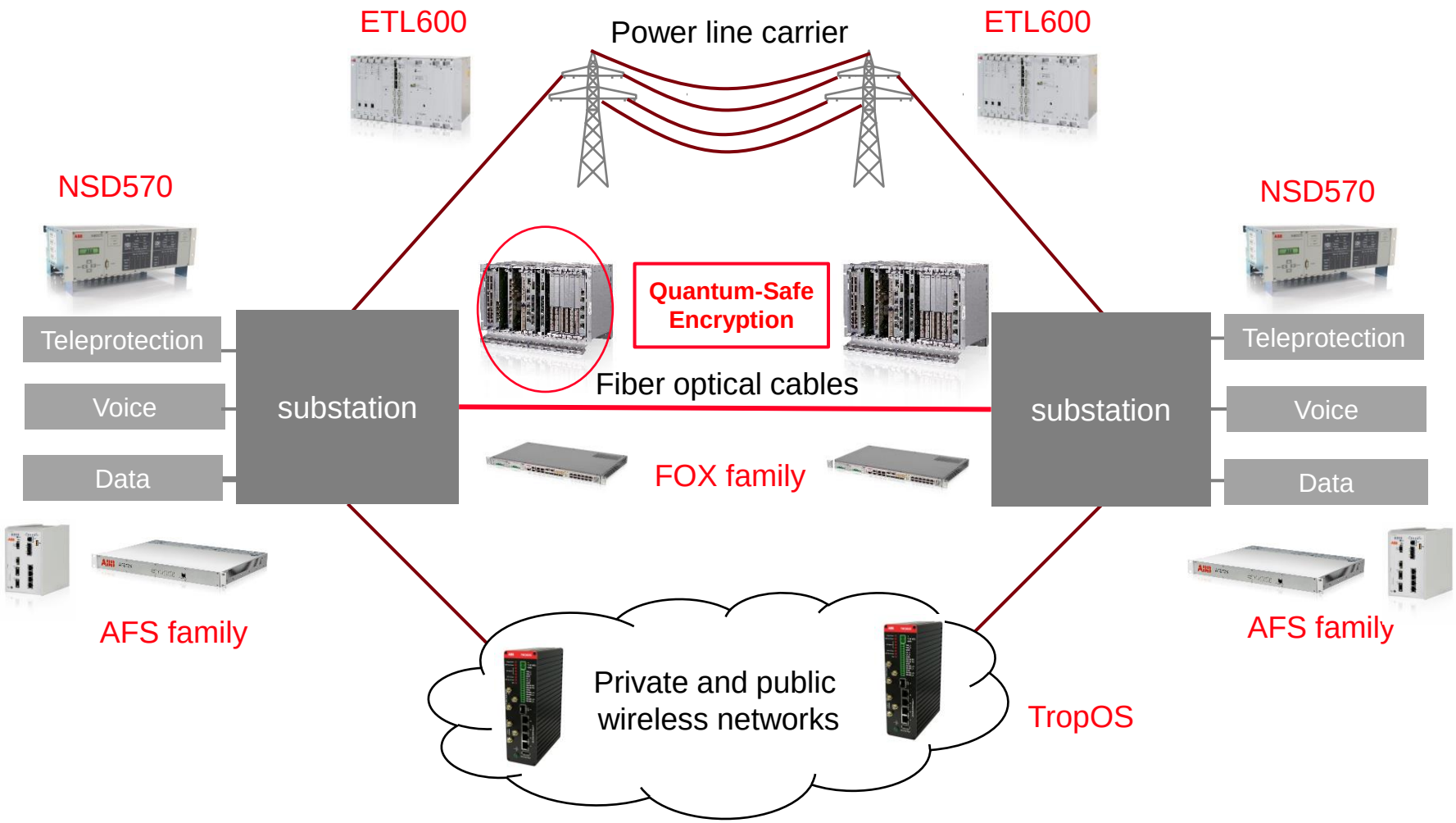
Remote Factory Acceptance Test allow Customers to safely witness test in the Factories

FORTINET
HITACHI ABB

Cyber Security Innovations Grid Automation and Communciation

HITACHI ABB POWER GRIDS

Communication Solutions Offering



Quantum-Safe Encryption Card SENC1
Next Level of Cyber Security

Requirements

- Ultra low latency
- No influence on the bandwidth and timing
- End-to-end, deterministic, deploy and forget
- High-secure and trustful
- Future-proof and long term protection
- Long lifecycle

First encryption solution for mission-critical infrastructure with quantum technology

SENC1-4
4 Port

SENC1-8
8 Port

SENC1F4
4 Port
Fanless

SENC1F8
8 Port
Fanless

Trusted Security for a secure, reliable and highly available network

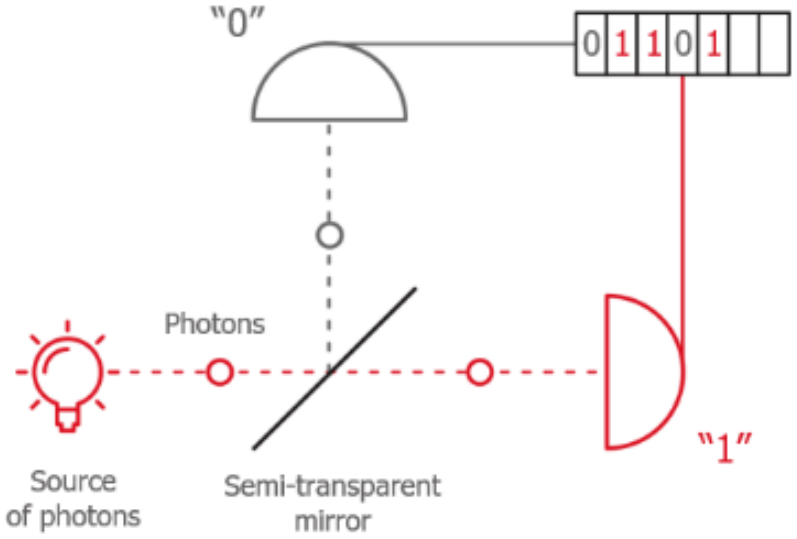
HITACHI ABB POWER GRIDS

Quantum Random Number Generator

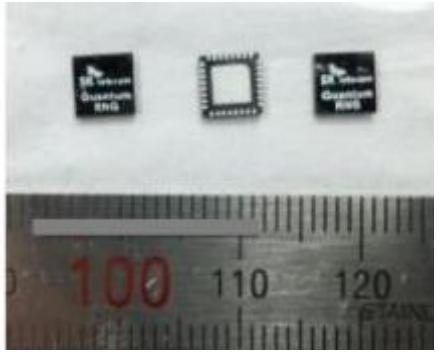
Based on quantum physics for high secure keys

Advantages

- Speed: Random bit rate up to 4 Mbps
- Truly and provably random
- Simple process
- Live monitoring of elementary components
- The most stringently tested and certified QRNG in the world
- Long-term protection
- Resistance to external environmental impacts



Quantum random number generator exploiting a phenomenon described by quantum physics – it is truly random



Certifications

National Security Government Agencies

German BSI AIS31 Standard

NEW: AEC-Q100 Grade 3 - Automotive Electronics Council

Embedded into Hitachi-Powergrids encryption card FOX615 SENC1

HITACHI ABB POWER GRIDS

Close Integration of MPLS-TP Paths and Encrypted Tunnels

MPLS and encryption endpoints paths/tunnels, jointly handled

Encryption Technologies

Data

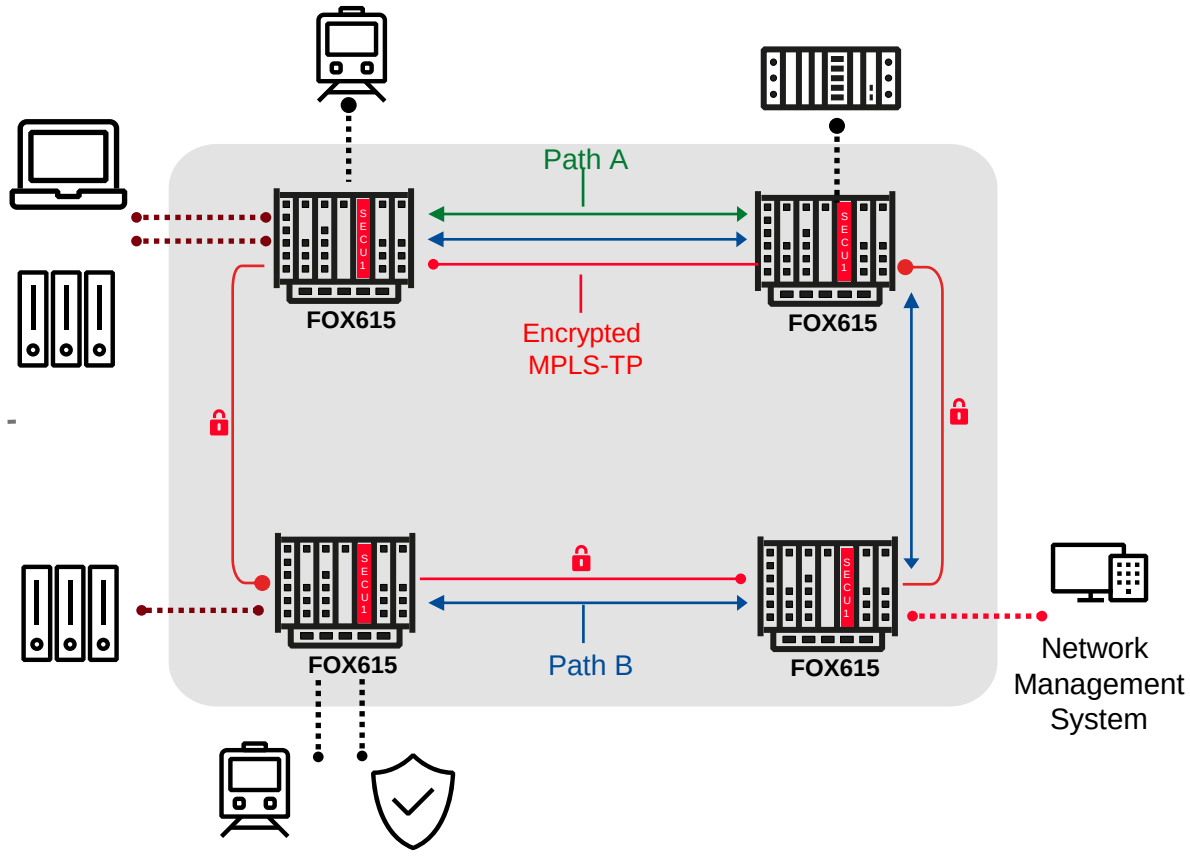
- AES-256 GCM (Encryption and authentication)

Session Key

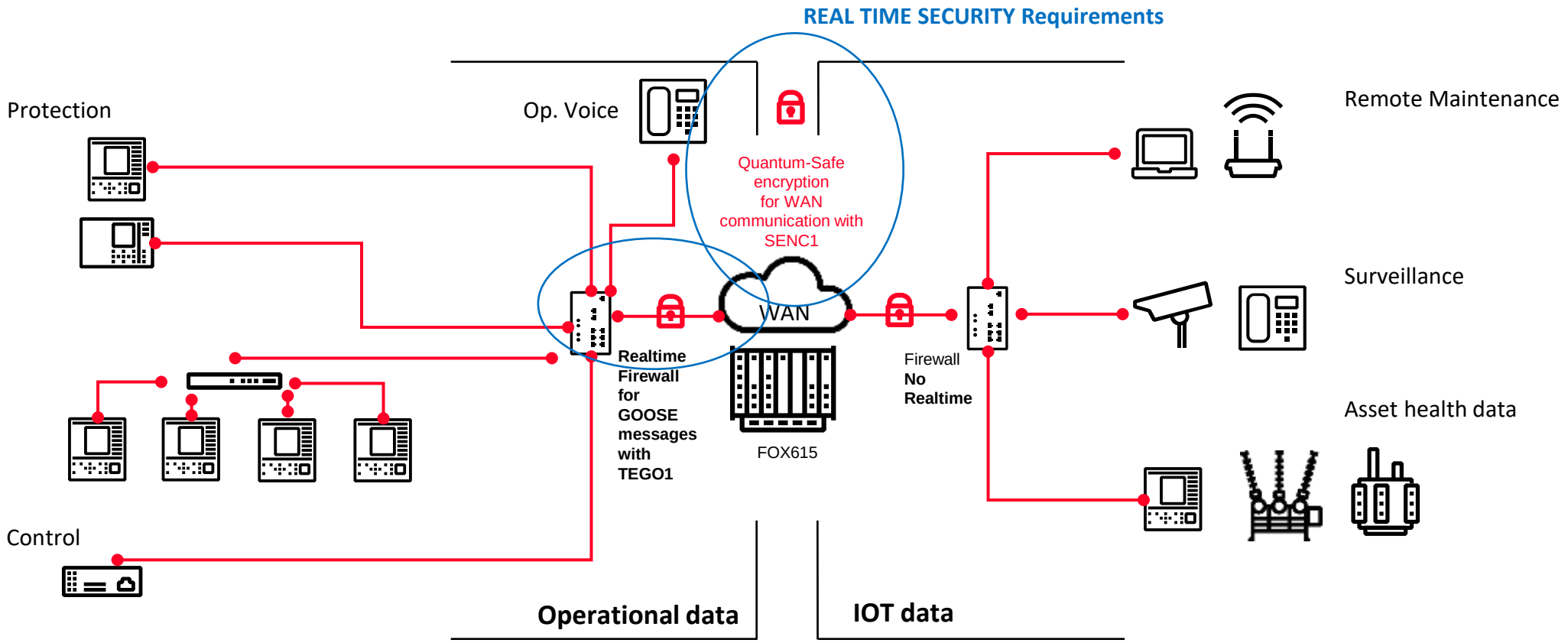
- AES-256 GCM
- Strong random numbers QRNG

Master Key

- Asymmetric Key (Hitachi-Powergrids Permanent Encryption)
- Optional: Quantum Key Distribution (QKD)



Secure real-time communication needs in substations

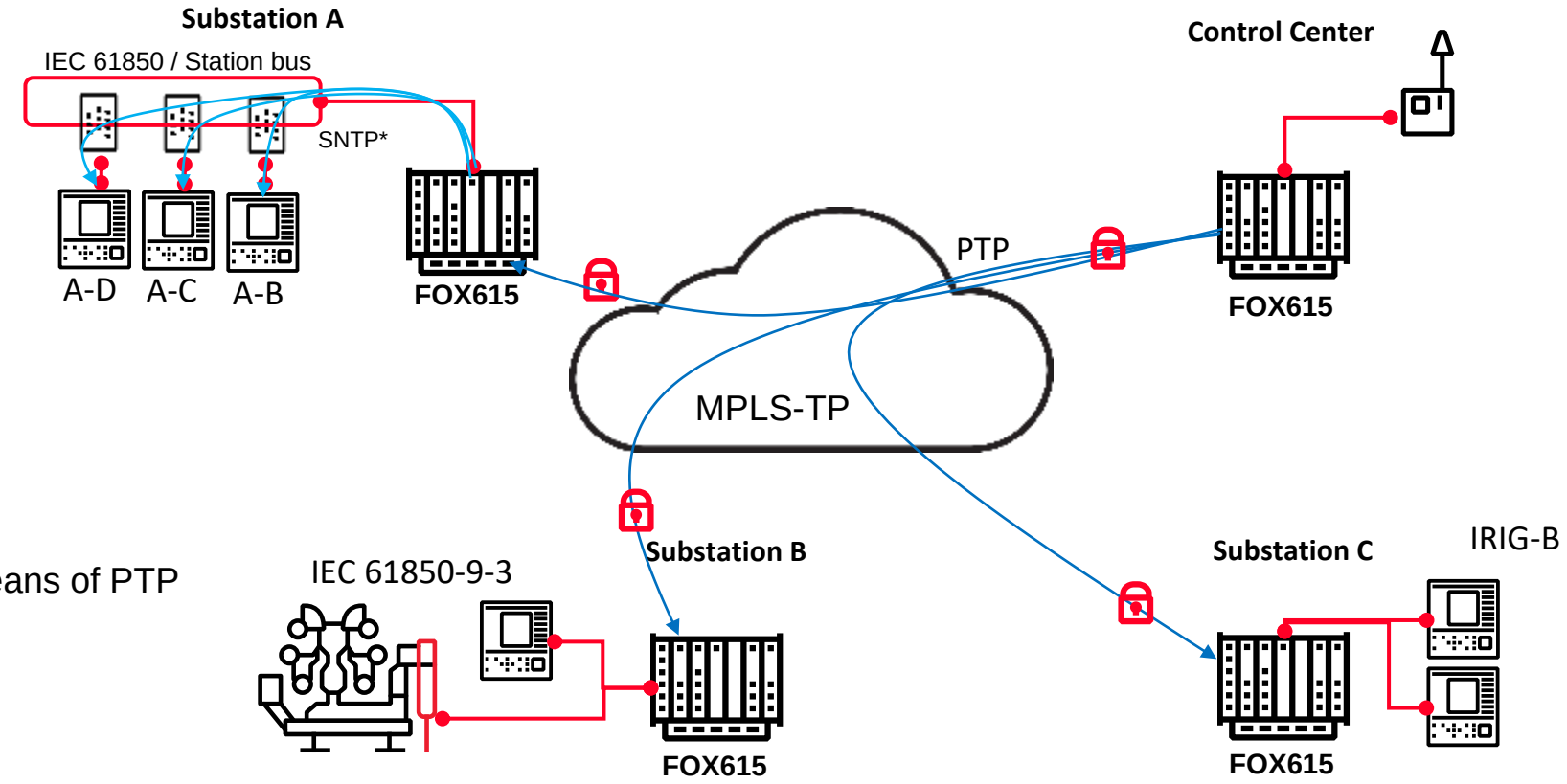


Communication for mission critical OT as well as IoT communication

Keep your network synchronized and secure

Many mission critical application are depending on time synchronization

- Substation Automation and Sequence of Events
- Line differential
- Digital substation
  - Merging unit require 1us time accuracy
- Wide Area Monitoring System
  - Phasor Measurement units require 1us
  - Time alignment of utility wide phasors



Time of day information can be distributed by means of PTP

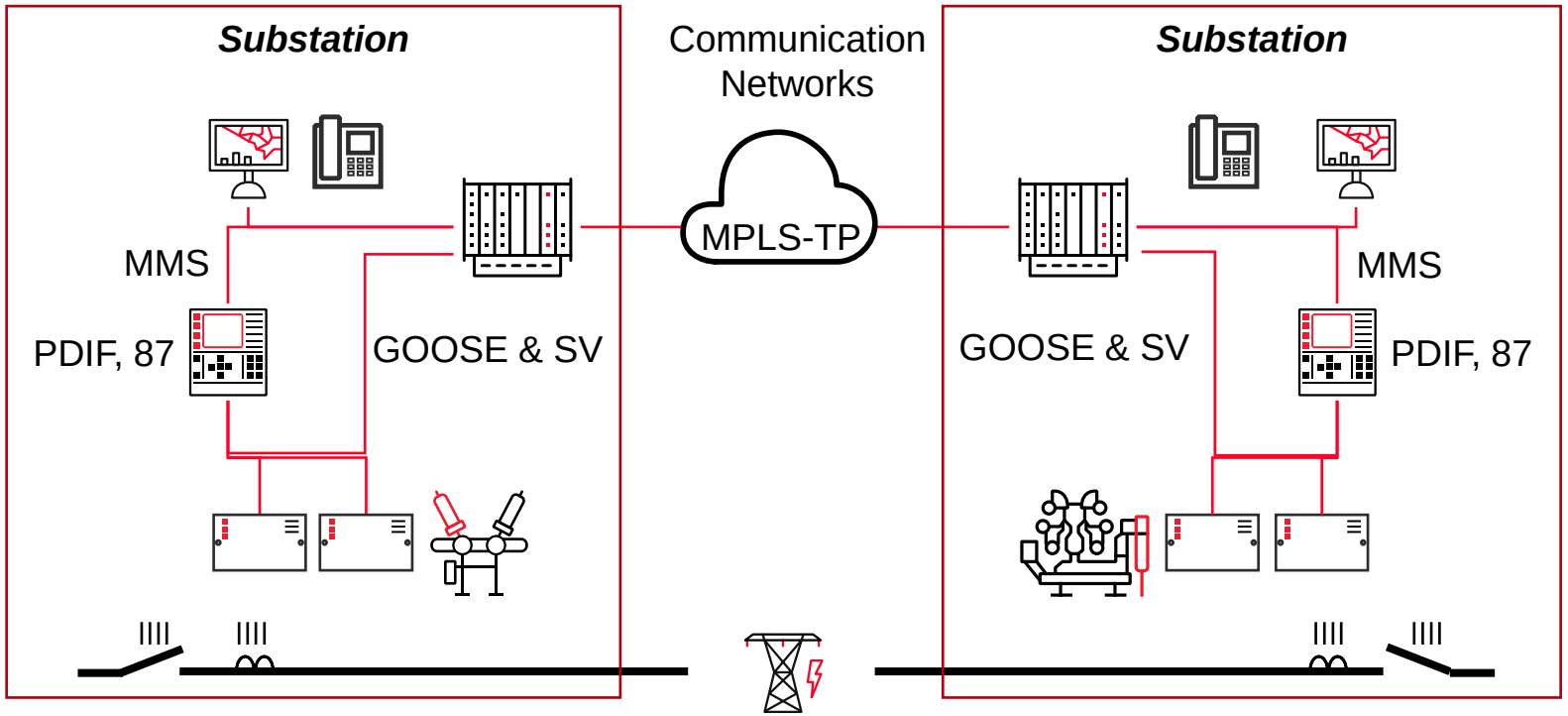
FOX615 with SENC1 allows encryption and authentication of time of day information

Distribution of time of day information

IEC 61850 based inter substation Communication, FOX 615

GOOSE, SV instead conventional Wire or C37.94

- TEGO1 card support communication redundancy (PRP) to integrate real-time data (GOOSE, SV) within Substation
- Up to 5ms performance improvement for signal transmission End to End
- Flexible and accurate configuration for point to point signaling across multiple substation



FOX multi-service platform including IEC 61850 GOOSE and Sampled

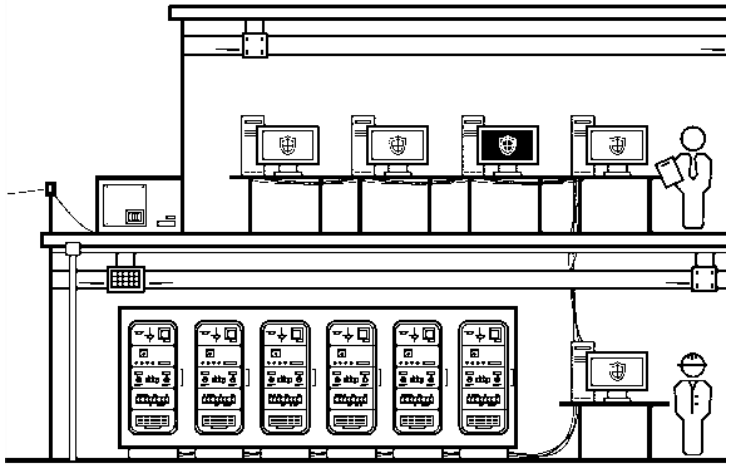
System Data Manager SDM600 – Cyber Security

Central user account management

- System wide user management
- Role based access control (RBAC) according IEC 62351-8
- Enforce password policies
- For Relion 670/650 2.1 and newer, Windows PCs, MicroSCADA Pro, RTU500 R12.4 and any RADIUS capable device.
- In accordance with IEC62443, NERC CIP and BDEW whitepaper requirements

System wide cyber security event logging

- Store user activities and other security events from IEDs or system level components
- Integration of any device using Syslog protocol (UDP and TCP)
- Integration of Windows computers (converting Windows Event Logs)
- Categorization of unknown events based on rules
- Built in visualization and reporting
- Integrate SDM600 into an existing event logging system



Vendor Independent and automatic management of users and security logs

HITACHI ABB POWER GRIDS

System Data Manager SDM600 – Fleet Management

Manage many RTU500 devices

Fleet wide management of firmware and configurations for RTU500 increases your efficiency.

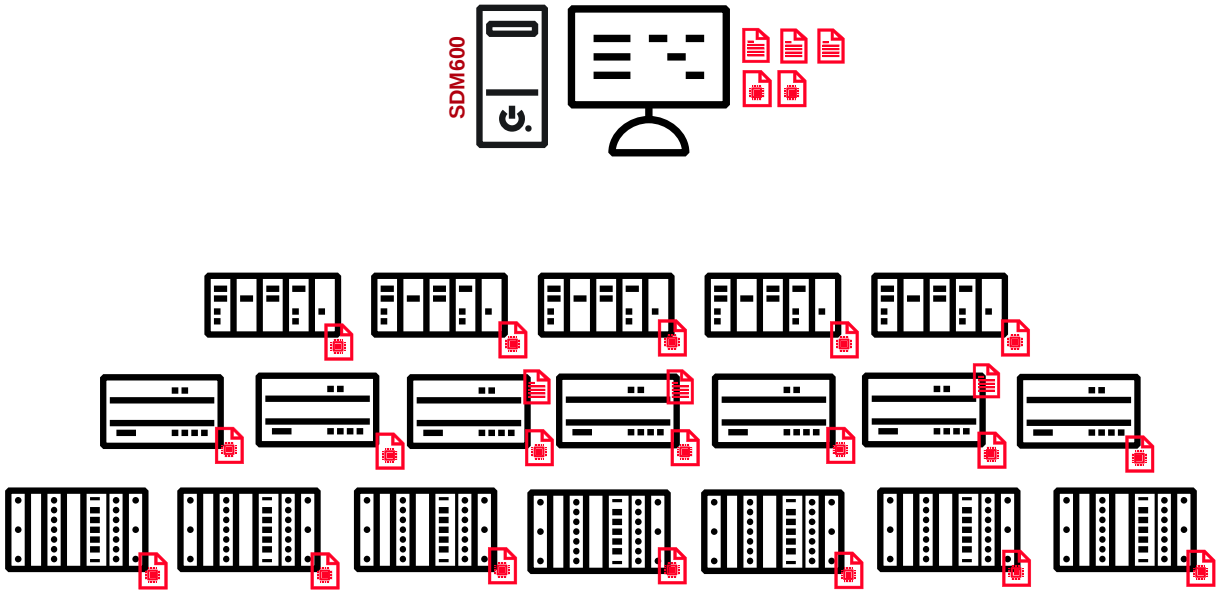
– Retrieve, maintain and write configuration files for RTU500 family devices*. Manually or cyclic.
– Keep history of last 5 configurations
– Retrieve and write firmware files to RTU500 family devices*
– Bulk operations with multiple RTUs possible

Customer Benefits

✓ Up and download of files by power shell script
✓ Support files for configuration, firmware, integrated HMI, password file, PLC logic
✓ Providing Data exchange through encrypted communication channels
✓ Reduce numbers of user interaction per RTU
✓ Automation of updates for large volumes of RTU's

New Script Interface

✓ Enable support of customer owned IT/OT management tools
✓ Use standard Power shell environment – Link to Documentation and Examples (chapter 12)



RTU500 Configuration and Firmware file management

HITACHI ABB POWER GRIDS

Substation Automation - Product & System Hardening

System Hardening

- Remove unused software and users
  - Only needed software, services, tools and users are implemented in the system, everything that that is not needed is removed or disabled
- Firewall and anti virus
  - Firewall is enabled and configured, anti virus is installed and updated through DMZ server
- Application Whitelisting is configured
- Restricted Users
  - Each user has only access to the data and tools that are needed to perform the job
- Patch update
  - WSUS Server is installed on the DMZ servers and can update all computers of the system

Cyber security in Hitachi-Powergrids Products

Protocol hardening

- Fuzz testing all protocols
- Security development life cycle
- Protocol conformance
- Device security testing
- Extensive service and port configuration
- Flooding protection

Account management

- Local users created in the device
- Device tool used to manage users
- Removal of default users and passwords
- Central account management – IEC 62351 with LDAP

Security event logging

- Audit trail
- Reporting on IEC 61850
- Syslog
- Offline log in every device

Role based account control

- User roles
- User rights
- IEC 62351 part 8

Certificates

- Self signed certificates
- Customer signed certificates
- Encryption of communication

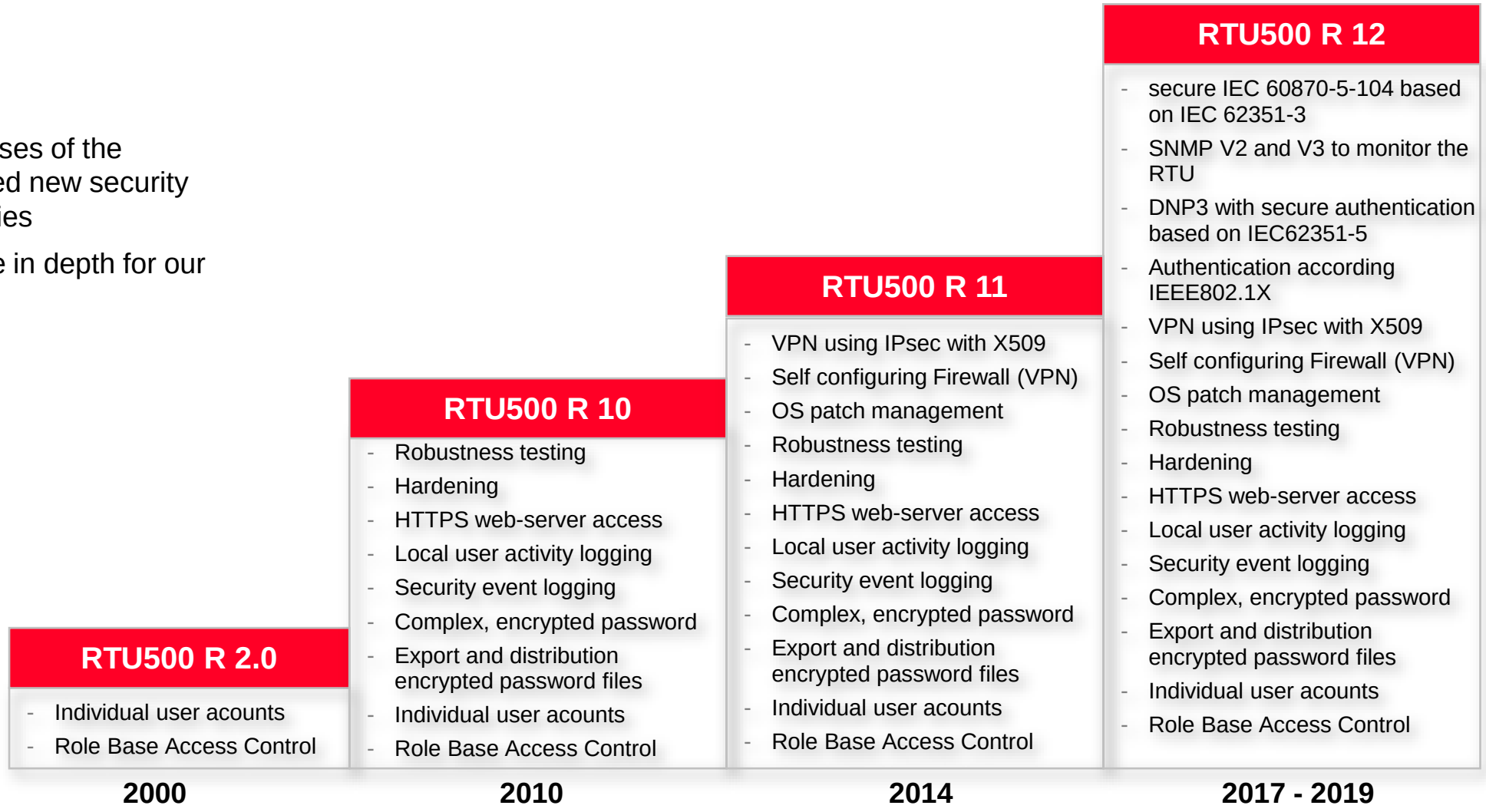
Supervision and configuration

- Self supervision of hardware and software
- Denial of Service protection
- Extensive configuration possibilities
- Maintenance menu

Cyber security in RTU500 series - Evolution

Defense in depth

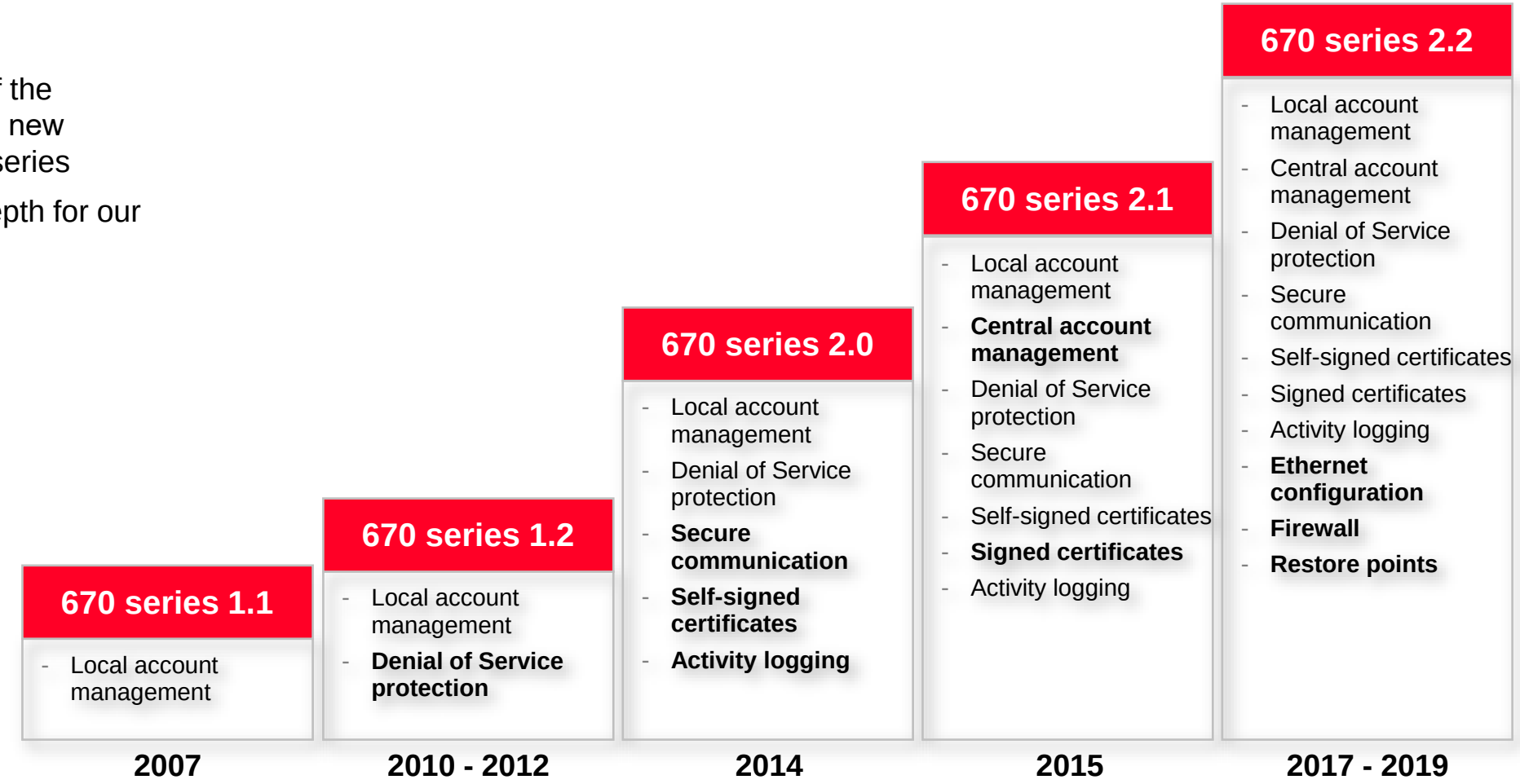
- Through the different releases of the RTU500 series we've added new security features to the product series
- This enhances the defense in depth for our users



Cyber security in Relion® 670 - Evolution

Defense in depth

- Through the different releases of the Relion® 670 series we've added new security features to the product series
- This enhances the defense in depth for our users



Cyber Security for Grid Automation

Ensuring compliance with highest requirements, from planning to maintenance

HITACHI ABB POWER GRIDS

HITACHI ABB

POWERING GOOD FOR SUSTAINABLE ENERGY

HITACHI ABB POWER GRIDS