Itay Savion – Cervello Head of Sales

June 2021

The IT and OT Cybersecurity domains

- IT: Information Technology
- OT: Operational Technology

- Telecom, Signalling and IXL networks are concerned by OT cybersecurity

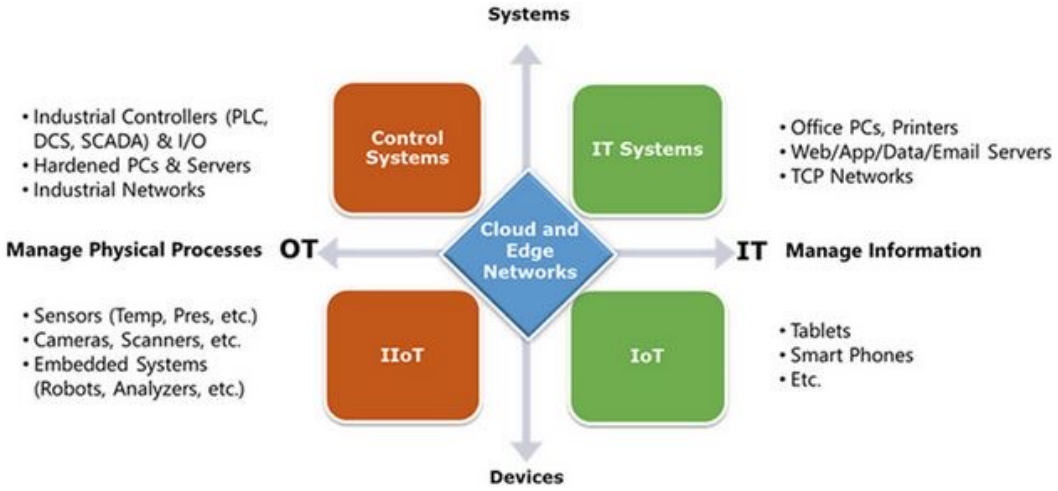
- Standards:

  IT: ISO 27.001

  OT: IEC 62443

  Future TS 50701

  dedicated for Railway



Industrial IT and OT Systems and Devices

A shortage of Cybersecurity is a Big Stop Sign

- **Lack of Visibility**
  How do you monitor railway critical assets and mission-critical activity?
- **Much Higher Complexity**
  Multi-environment, cross-generation equipment and proprietary technologies
- **Safety and Resilience Concerns**
  Challenging system credibility and business continuity
- **Moving to Digital and Autonomous Operations**
  Cloud-based, fully automated and machine-to-machine communications

Railway Cybersecurity Challenges

- **Attack can come**
  From outside of the organization
- From inside of the organization
- **Security is never ending**
  Daily new attack
- **Railway equipment**
  Old equipment
- Reluctant to upgrade industrial equipment
- **Heterogeneous and proprietary technologies**
  Telecom: from SS7 to IP
- Signalling: from legacy to ETCS
- Interlocking: from mechanical to IP

SECURITY TOPIC	INFORMATION TECHNOLOGY	OPERATIONS TECHNOLOGY
ANTIVIRUS & MOBILE CODE COUNTER-MEASURES	Common & widely used	Can be difficult to deploy
SUPPORT TECHNOLOGY LIFETIME	3 to 5 years	Up to 40+ years
OUTSOURCING	Common/widely used	Rarely used (vendor only)
APPLICATION OF PATCHES	Regular/ scheduled	Slow (vendor specific, compliance testing required)
CHANGE MANAGEMENT	Regular/ scheduled	Legacy based – unsuitable for modern security

SECURITY TOPIC	INFORMATION TECHNOLOGY	OPERATIONS TECHNOLOGY
TIME CRITICAL CONTENT	Delays are usually accepted	Critical due to safety
AVAILABILITY	Delays are usually accepted	24 x 7 x 365 x forever (Integrity also critical)
SECURITY AWARENESS	Good in both private and public sector	Generally poor inside the control zone
SECURITY TESTING/ AUDIT	Scheduled and mandated	Occasional testing for outages / audit for event recreation
PHYSICAL SECURITY	Secure	Traditionally good

iebmedia.com source

A Growing Need

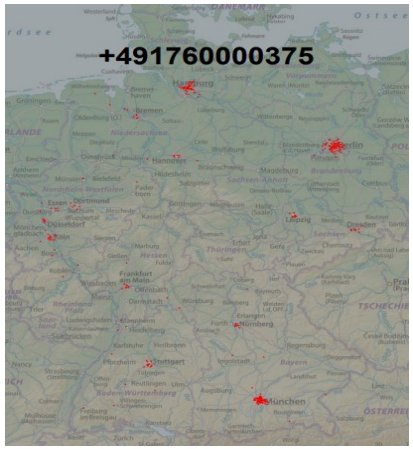
- ~$1M average loss for every one hour of service disruption
- Reputational damage
- Safety reliability is compromised
- Regulatory implications under GDPR and NIS Directive compliance
- Human lives are at risk

OT Attacks are not legends: 2G/3G

MNO example:

- SMS firewall can be bypassed if hacker knows the direct MSC global title

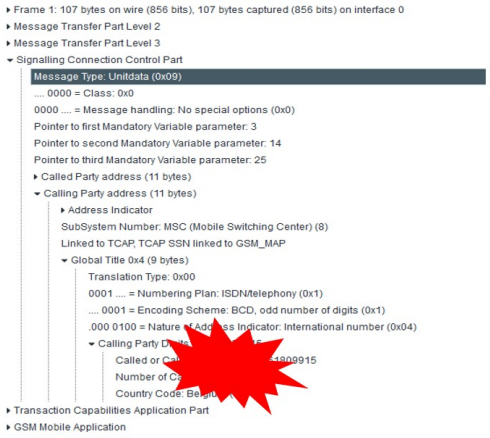
- Tobias Engel source:
  - Locates German T-Mobile and Vodafone mobiles via MSC Global Title



RAILWAY: What about your network ?

- More than 80%* of the MNO operators monitor for abnormal SMS activities. And you ?

- Here is an example of a real Railway where MSC Global Title is not crypted:



*: ENISA Source

OT Attacks are not legends: 2G/3G

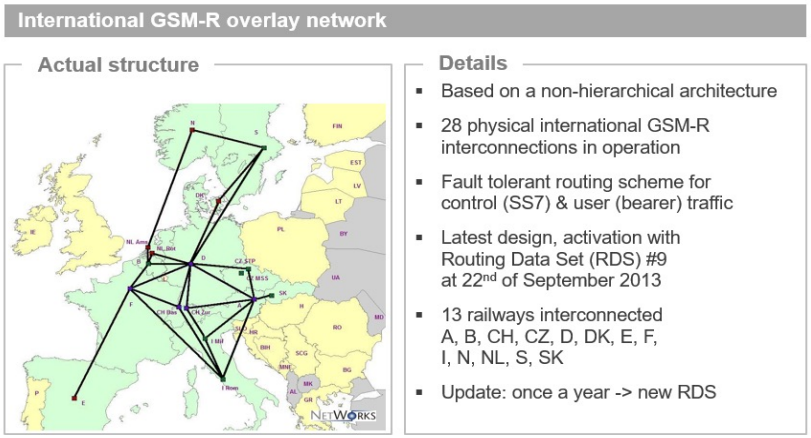
MNO:

Russia attacks the Ukrainian network by using International MTS network identity

Railway: What about your network ?

All GSM-R networks are interconnected : are your Roaming gateway safe?

Expandium/Cervello has been able to access to GSM-R international IDs.



*: UIC Source

Securing Your Operational Infrastructure

- Unparalleled threat detection accuracy using Zero-Trust framework, machine learning, and behavior-based analytics
- Fully compatible with your existing rail infrastructure, deployed physically or virtually anywhere
- Ensures compliance with industry specific regulations, security standards and safety measures
- Seamlessly integrates into your existing environment, SIEM/SOC workflows and security tools, and automatically scales to meet demand with no system changes required
- Delivering a fully agnostic service to all equipment types, generations and product lines
- Low latency architecture without requiring system downtime
- Supporting the entire signalling surface - ERTMS, CBTC, ETCS, GSM-R, FRMCS, RBC, PTC, OBU, IXL

IEC 62443 / TS 50701: we help you to operate those standards

IEC 62443: Requirements

SL1: 37 IEC requirements including:

- → Monitor access from untrusted networks ✓
- → Audit records generated by equipment ✓
- → Protect the integrity of transmitted information ✓
- → Prohibit unnecessary ports, protocols and services ✓
- → Track unsuccessful login attempts ✓

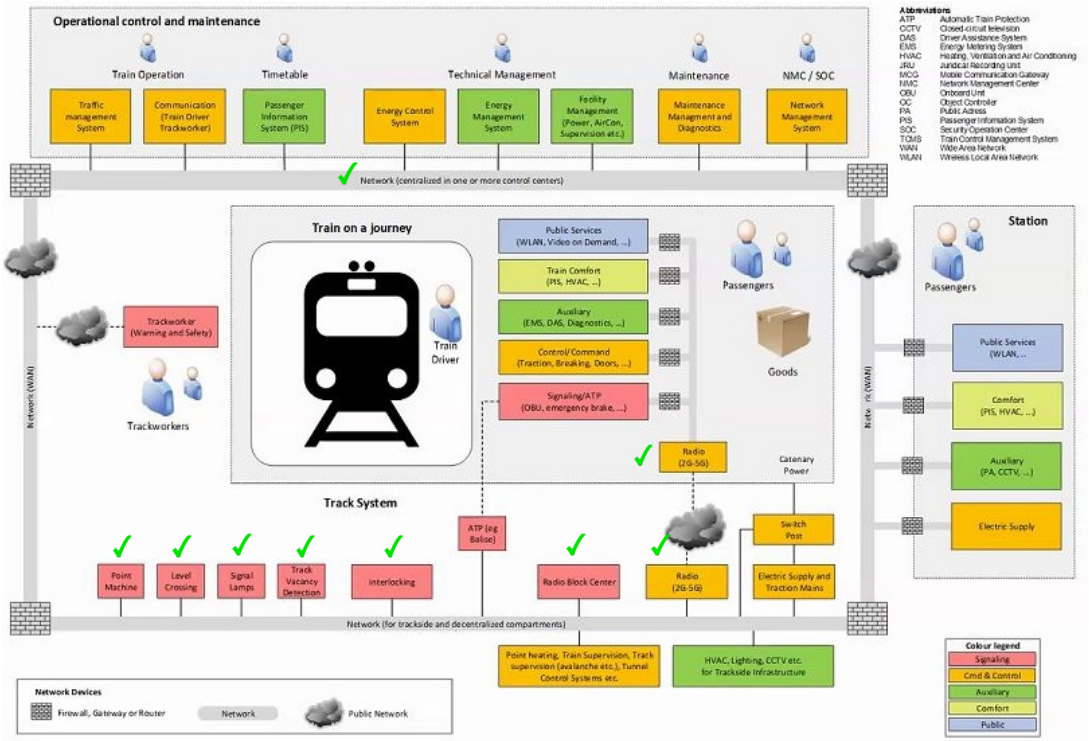
SL2: 23 IEC requirements including:

- → System shall report list of components ✓

SL3: 30 IEC requirements including:

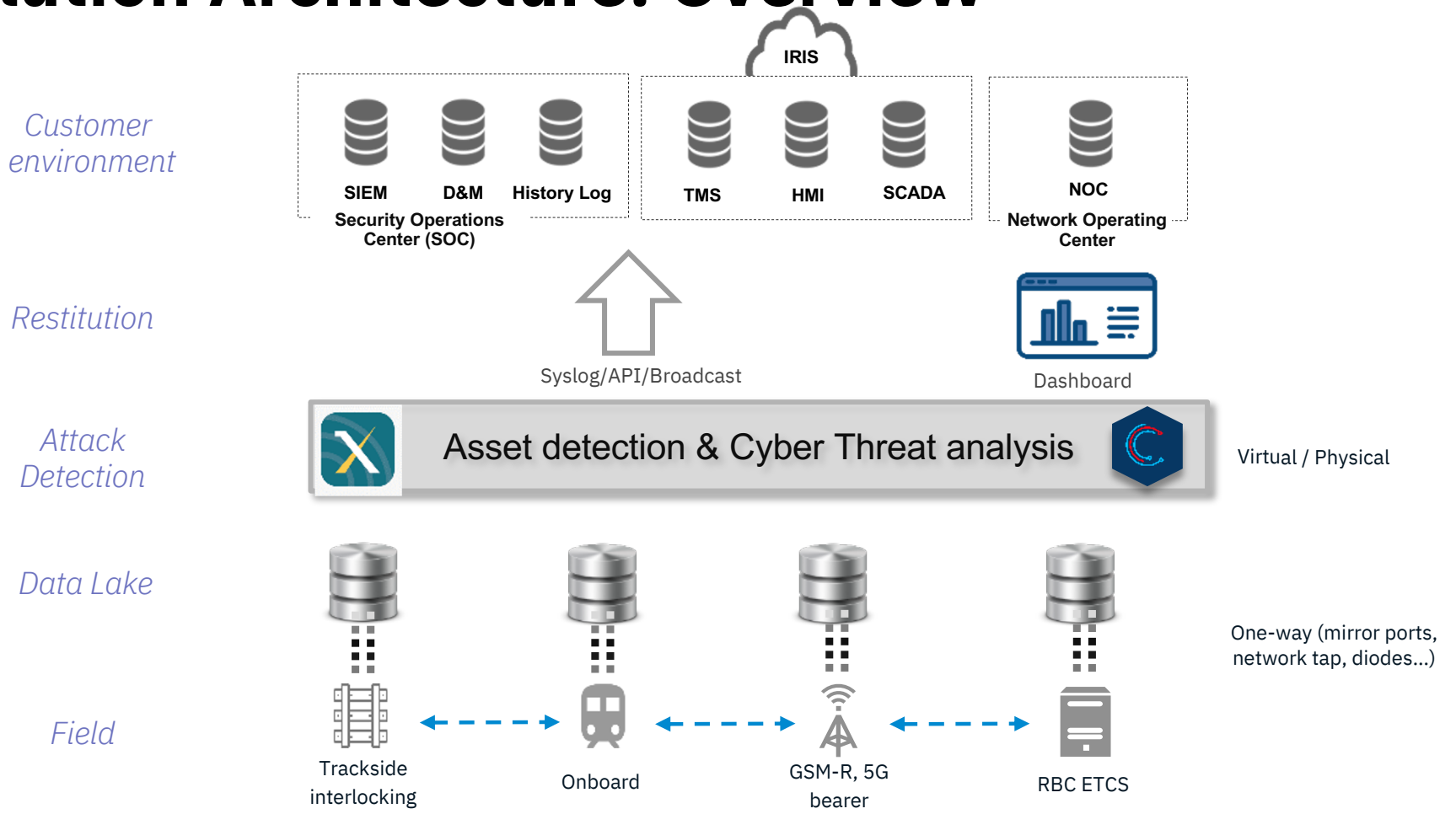
- → System shall report unauthorized wireless devices ✓
- → System shall … recognize changes to information during communication ✓

TS 50701: Railway Reference Architecture



✓ We cover it

Solution Architecture: Overview



cervellosec.com
expandium.com