



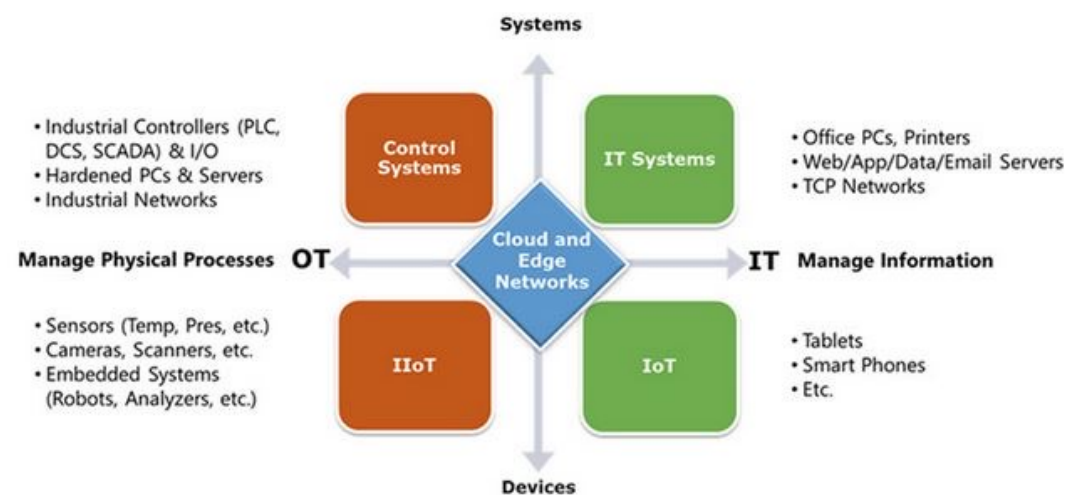
Itay Savion – Cervello Head of Sales
June 2021

CONFIDENTIALITY NOTE

This document contains confidential information. Nothing herein may be copied, reproduced or distributed or disclosed to any third party in any manner, without prior written authorization from Cervello Ltd. or Expandium

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



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

iebmmedia.com source

(9:03:42PM)
02 Jun 2019 04:03PM

Asia

14 people injured after Japan
driverless train goes wrong way



Home » Security » Dark web hacker selling admin access to a Chinese railway company

Dark web hacker selling admin access to a Chinese
railway company

MARCH 4TH, 2019

TECHNOLOGY NEWS

NOVEMBER 28, 2016 / 5:45 PM / 3 YEARS AGO

San Francisco public transit system hit in
ransomware attack

2 MIN READ



Jim Finkle

(Reuters
contain
free ser

Jaipur Metro alerted of a possible
cyber attack

Acting on the alert, the Jaipur Metro administration has started making cyber
advisory with the help of experts

IANIS • December 12, 2019, 18:19 IST



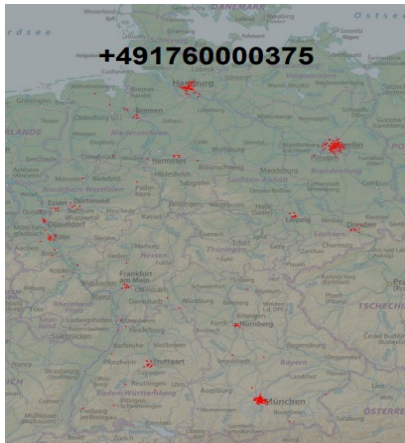
A Growing Need

- ~\$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:

```
Frame 1: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface 0
Message Transfer Part Level 2
Message Transfer Part Level 3
Signalling Connection Control Part
Message Type: Unitdata (0x00)
... 0000 = Class: 0x0
0000 ... = Message handling: No special options (0x0)
Pointer to first Mandatory Variable parameter: 3
Pointer to second Mandatory Variable parameter: 14
Pointer to third Mandatory Variable parameter: 25
Called Party address (11 bytes)
Calling Party address (11 bytes)
Address Indicator
SubSystem Number: MSC (Mobile Switching Center) (8)
Linked to TCAP, TCAP SSN linked to GSM_MAP
Global Title 0x4 (9 bytes)
Translation Type: 0x00
0001 ... = Numbering Plan: ISDN/telephony (0x1)
... 0001 = Encoding Scheme: BCD, odd number of digits (0x1)
... 0001 0100 = Nature of Address Indicator: International number (0x04)
Calling Party Details
Called or Calling Party Number
Number of Called Party
Country Code: Belgium
Transaction Capabilities Application Part
GSM Mobile Application
```

*: ENISA Source

OT Attacks are not legends: 2G/3G

MNO:

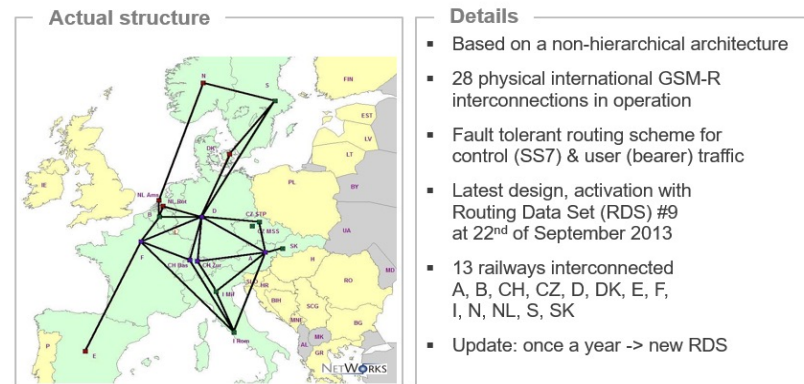
Russia attacks the Ukrainian network by using International MTS network identity

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.

International GSM-R overlay network



*: 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:

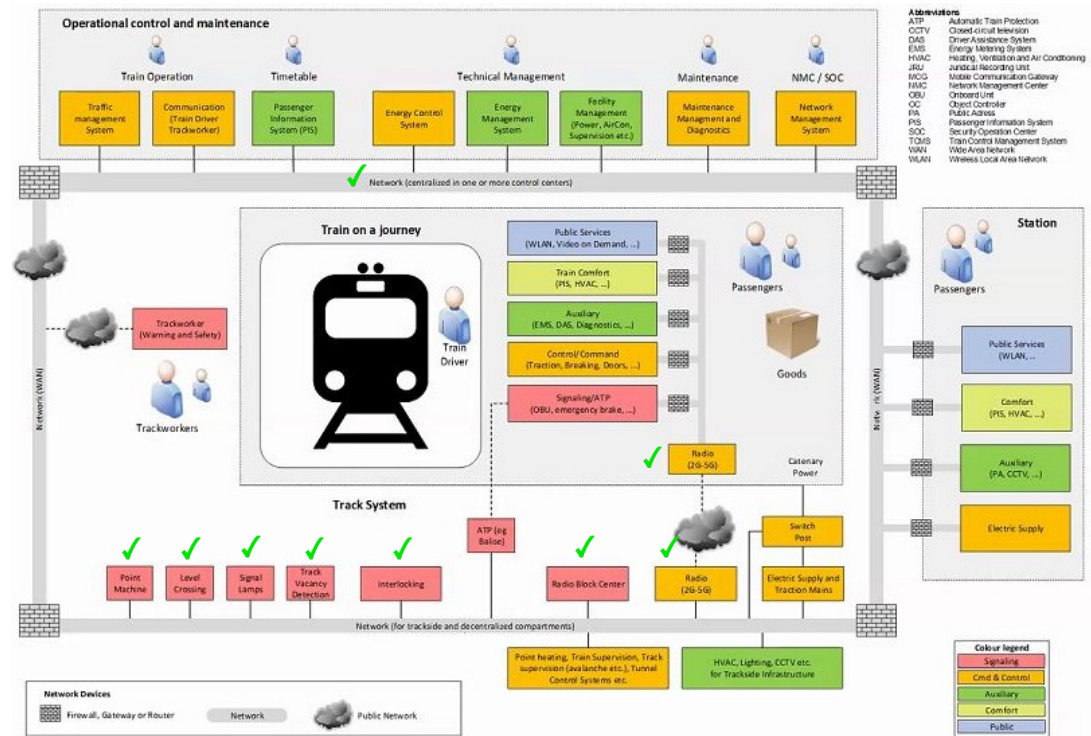
- System shall report list of components ✓

SL3: 30 IEC requirements including:

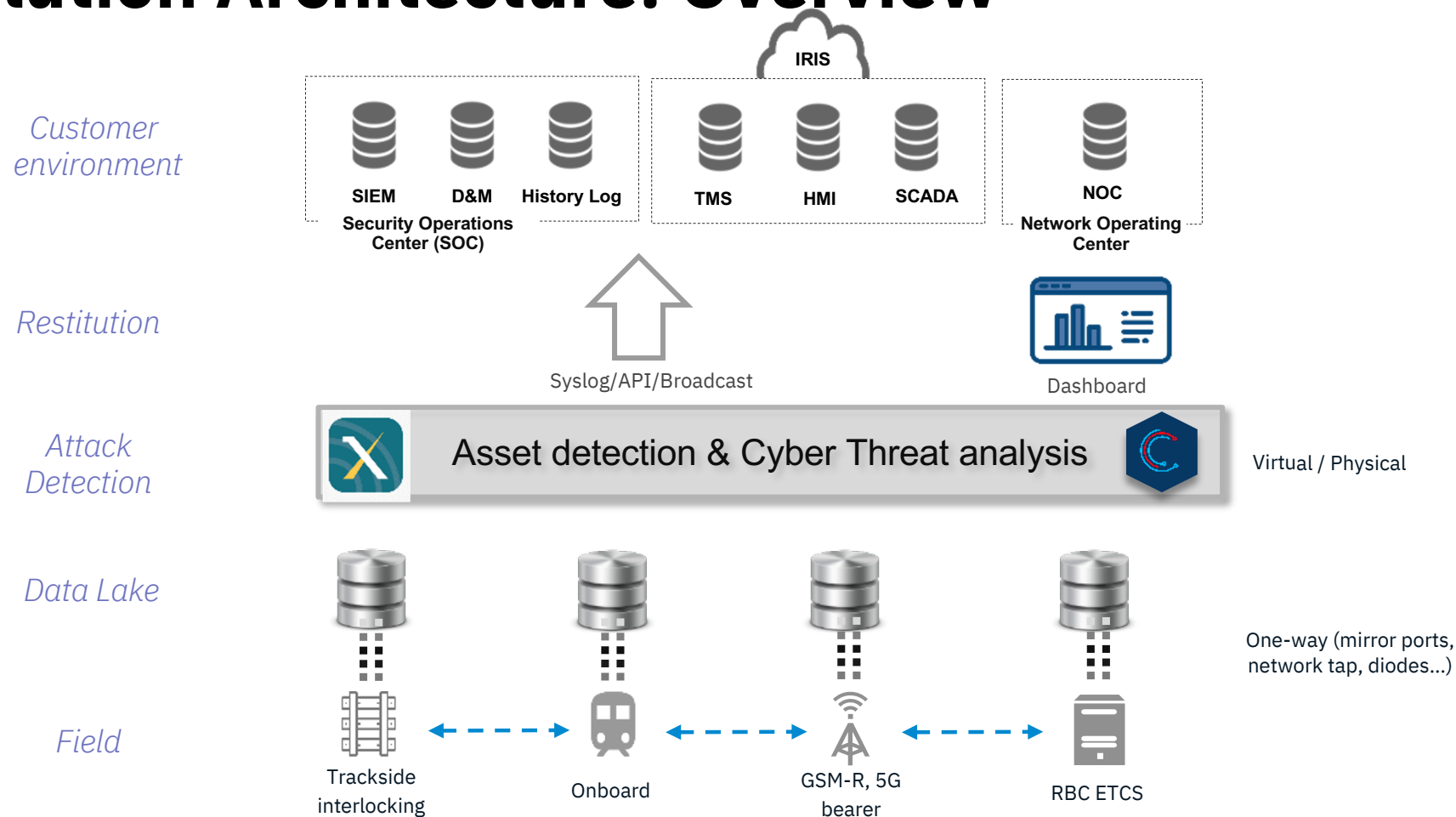
- System shall report unauthorized wireless devices ✓
- System shall ... recognize changes to information during communication ✓

✓ We cover it

TS 50701: Railway Reference Architecture



Solution Architecture: Overview





cervellosec.com

expandium.com

CONFIDENTIALITY NOTE

This document contains confidential information. Nothing herein may be copied, reproduced or distributed or disclosed to any third party in any manner, without prior written authorization from Cervello Ltd. or Expandium