THALES

ÖSTERREICHISCHE VERKEHRS-WISSENSCHAFTLICHE GESELLSCHAFT
www.oevg.at

Cybersecurity for Rail Systems

WOLFGANG WERNHART, THALES AUSTRIA GMBH

ÖVG / RRTM / AG2
1. December 2016

Safety & Cybersecurity

Safety: « The state of being free of risk or danger and the means/actions to obtain this state ».

Cybersecurity: « The protection of information systems from theft or damage, as well as from disruption or misdirection of the services they provide ».

The « digital transformation » of Rail Systems requires increased attention on Cybersecurity, to avoid operational disruption, access to user confidential data, and ensure safety is not impaired.

Reasons to be Attacked

Blackmail

To cause Chaos

Damage of reputation

Industrial Spying

For „fun“ or „competition“

Infiltration Rate & Source

Rate of Infiltration (sans.org, 2015)

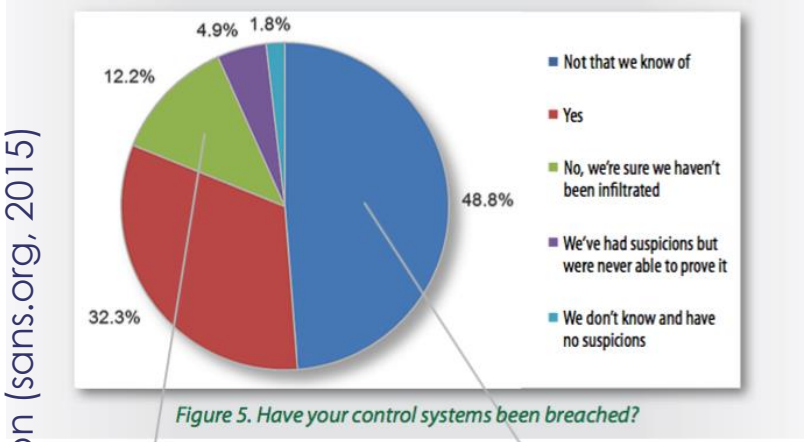
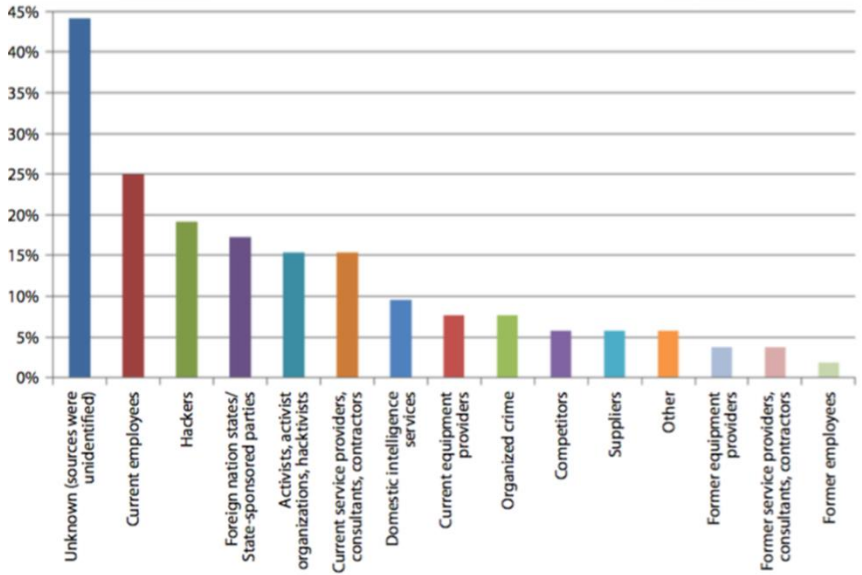


Figure 5. Have your control systems been breached?

Percentage of respondents sure their systems have not been breached

Percentage of respondents not aware of any infiltration or infection of their control systems

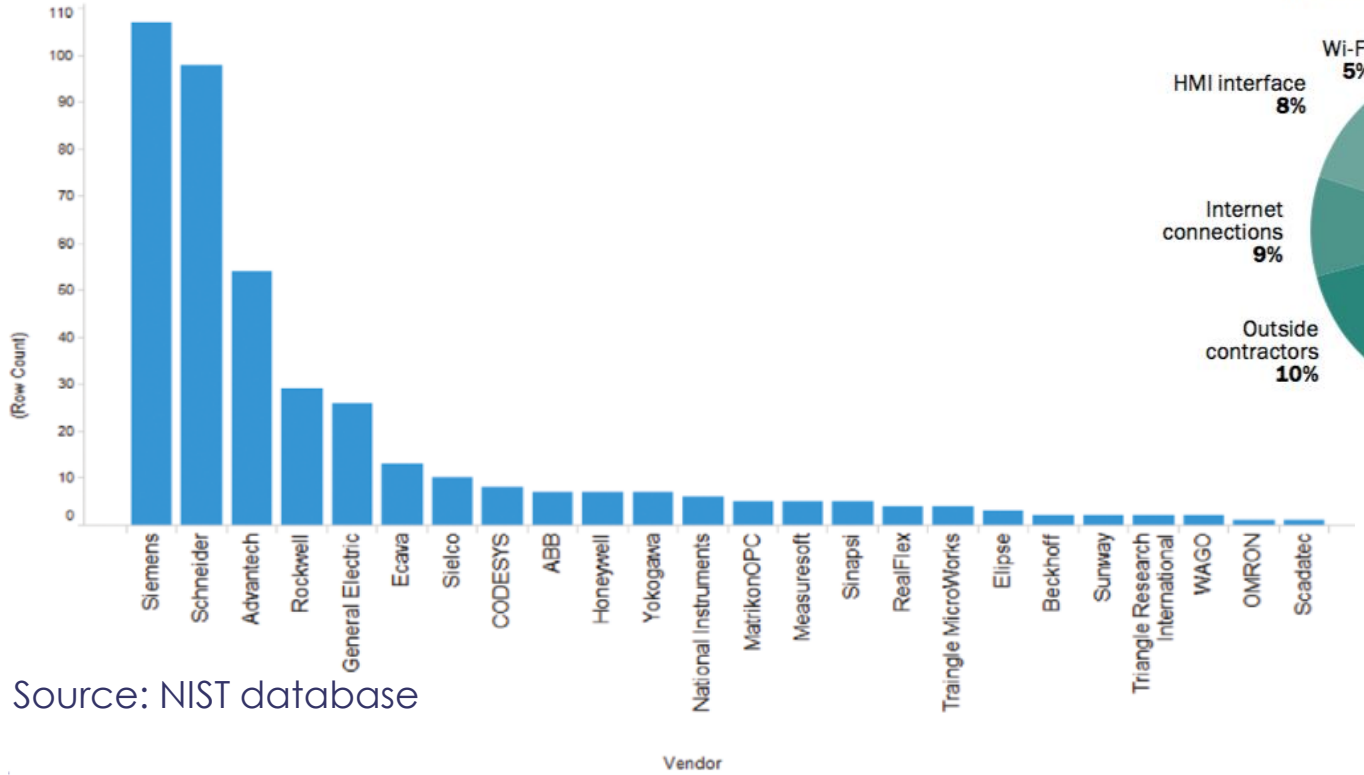
Source of Infiltration (sans.org, 2015)



THALES

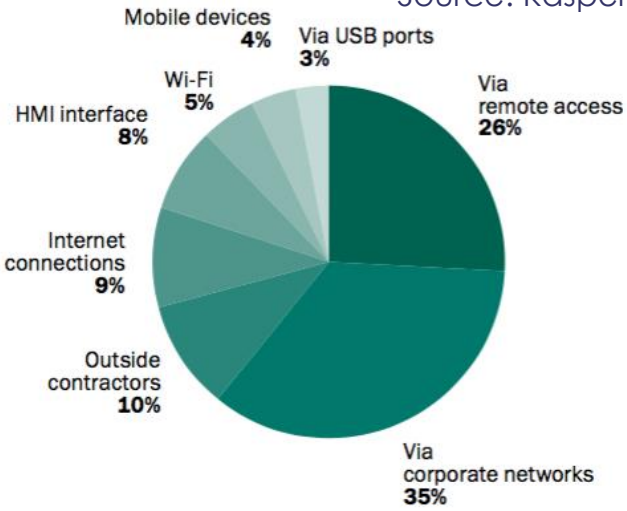
ÖSTERREICHISCHE VERKEHRS-WISSENSCHAFTLICHE GESELLSCHAFT
www.oevg.at

Vulnerabilities



Source: NIST database

Source: Kaspersky

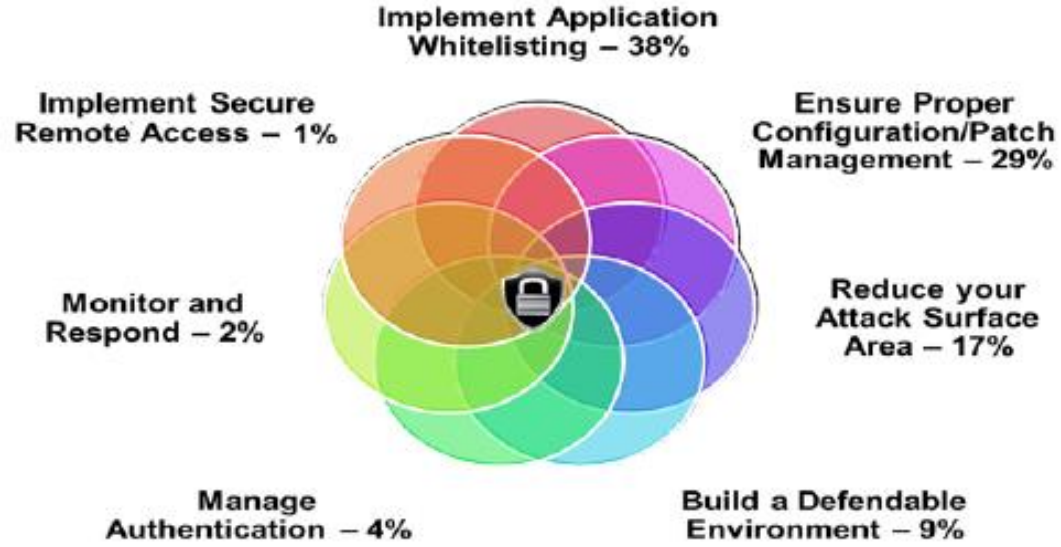


THALES

ÖSTERREICHISCHE VERKEHRS-WISSENSCHAFTLICHE GESELLSCHAFT
www.oevg.at

Strategies

7 strategies and their percentage of incidents potentially mitigated by each strategy



Source: US dept of Homeland Security

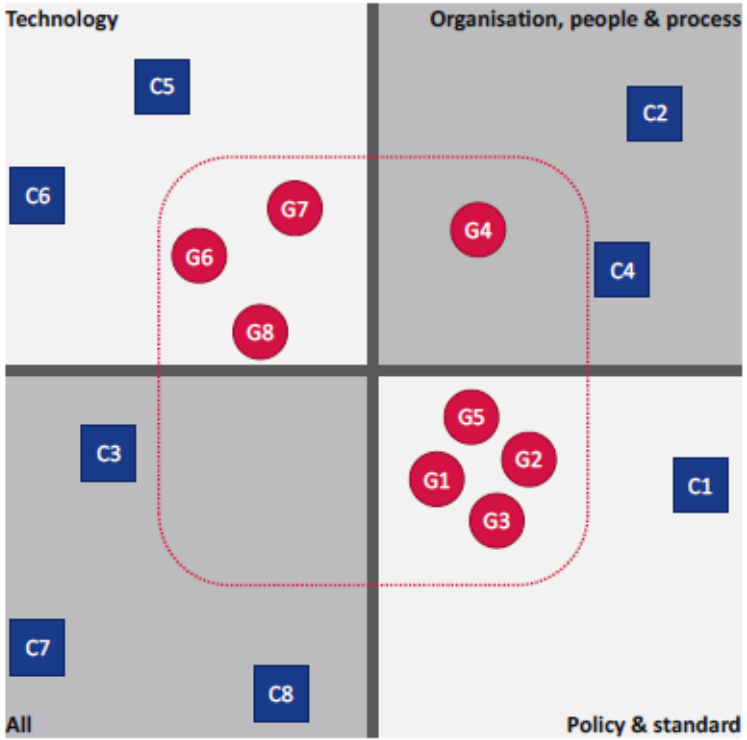
Cybersecurity in Intelligent Public Transport (IPT)

Challenges

C1 Difficulties to integrate security for safety
C2 Inadequate importance and spending for Cybersecurity
C3 Inadequate checking for countermeasusers
C4 Unwillingness to collaborate and exchange information
C5 Slow phasing out of legacy systems
C6 Inadequate data exchange between IPT and CS operators
C7 Weak situational awareness of cyber threats
C8 Resistance to security adoption

Gaps

G1 Lack of a common EU approach to IPT
G2 No integration of security in current guidelines/strategies
G3 Lack of common definitions and formalised policies
G4 Lack of corporate governance for IPT security
G5 No specific security standards for IPT
G6 Lack of advanced interdependet analysis tools
G7 Lack of advanced risk assessment tools
G8 Lack of advanced real-time security technologies



Source: enisa

THALES

ÖSTERREICHISCHE VERKEHRS-WISSENSCHAFTLICHE GESELLSCHAFT
www.oevg.at

Standards

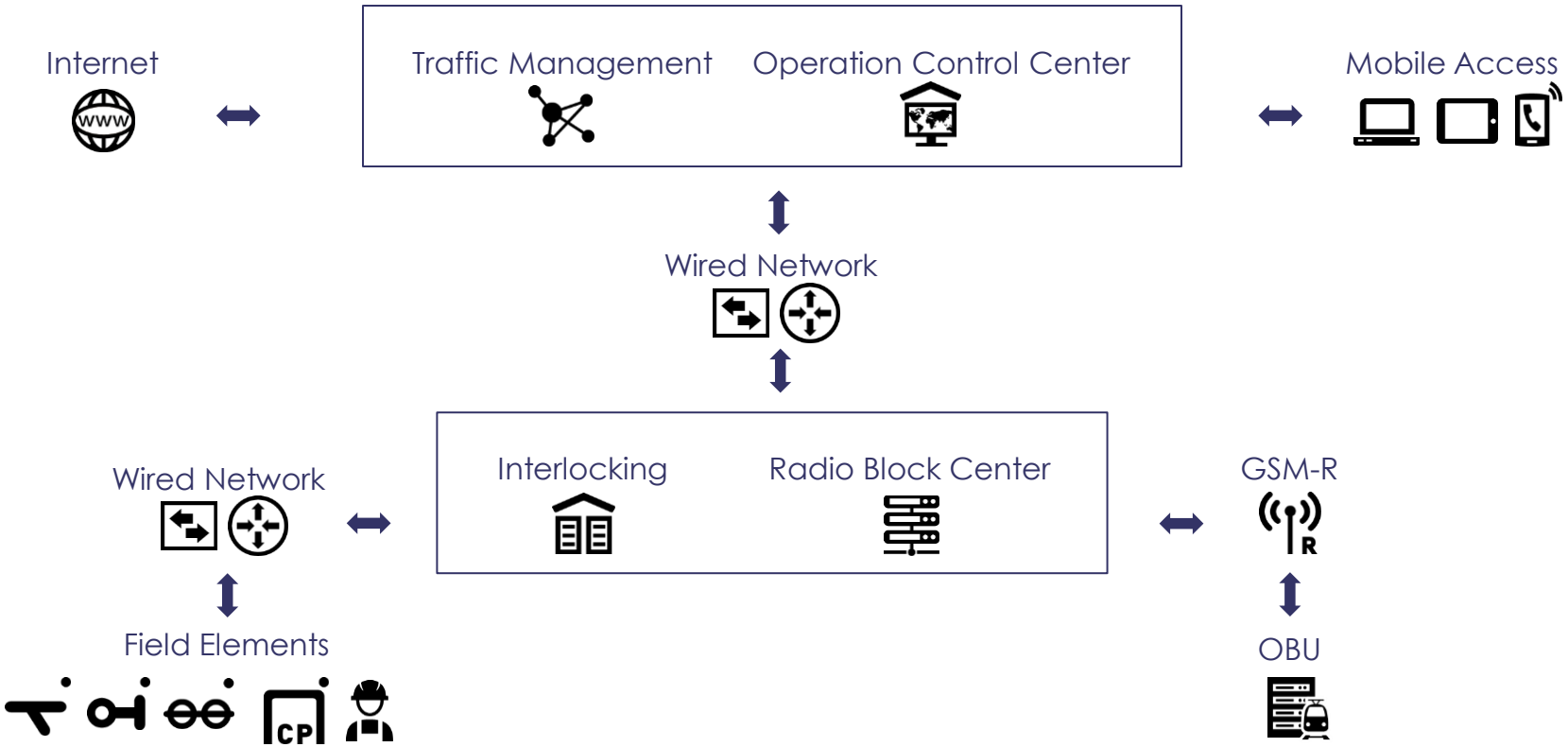
Requirements for critical infrastructures firmed up by Public Authorities

- European commission: ENISA, Europe 2020 NIS
- Most National NSAs introducing guidelines

Active standards and working groups

- Generic ICT: NIST SP800-53; ISO/IEC2700x
- Industrial Control Systems: NIST SP800-82 (US), ISA(IEC) 62443
- Rail specific: APTA, CENELEC SC9XA-SG16 WG, UITP WG, UNIFE WG

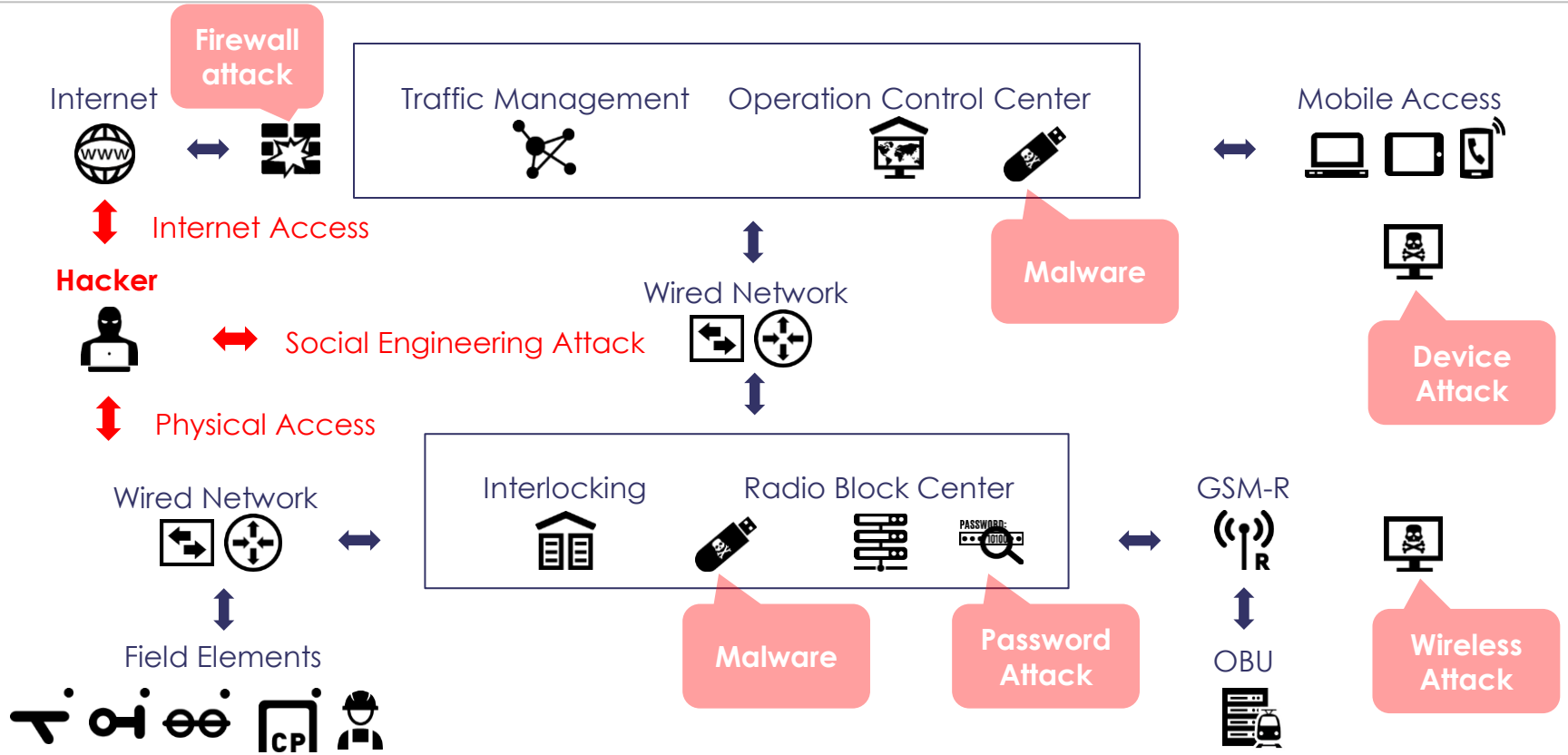
Areas of possible vulnerabilities in Rail Systems…



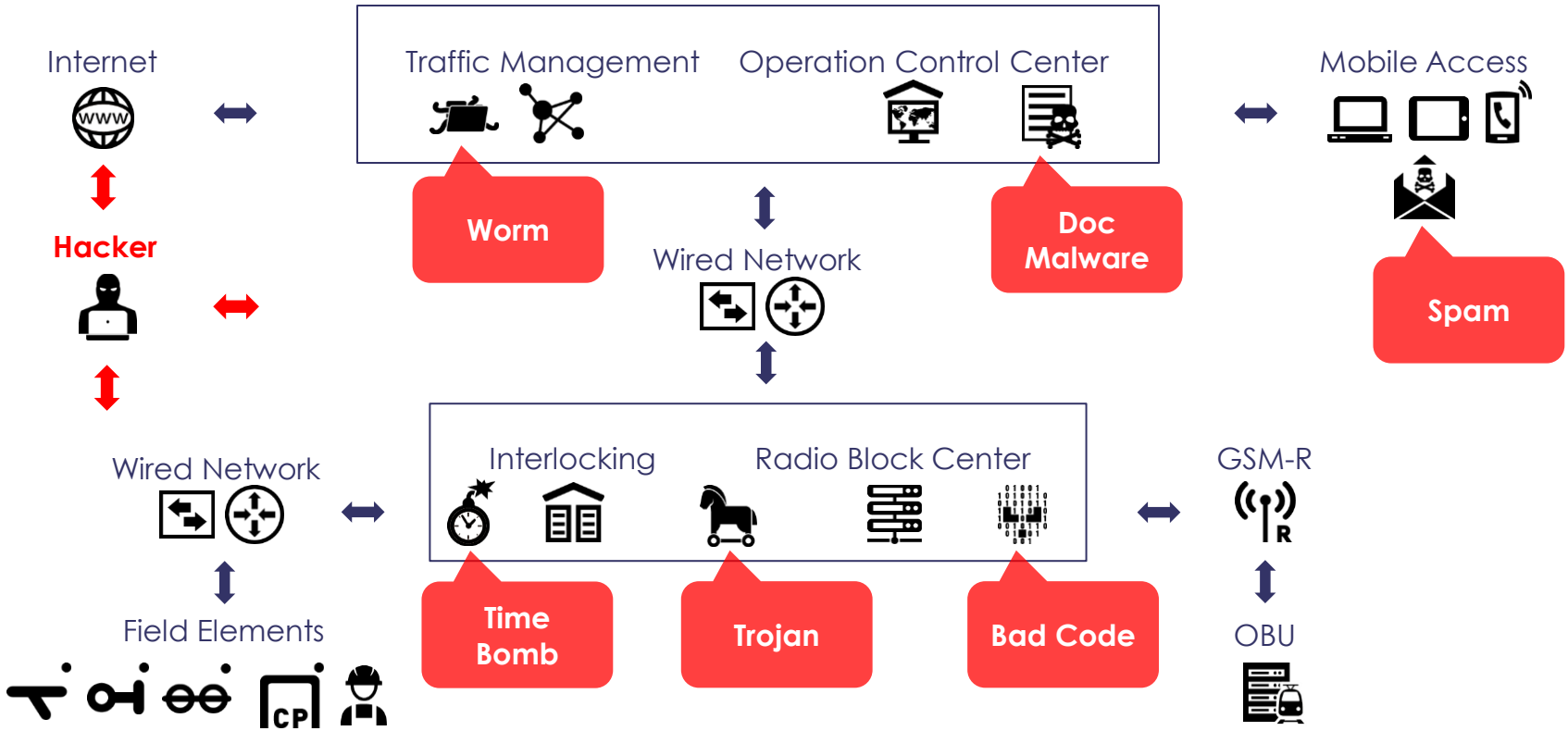
THALES

ÖSTERREICHISCHE VERKEHRS-WISSENSCHAFTLICHE GESELLSCHAFT
www.oevg.at

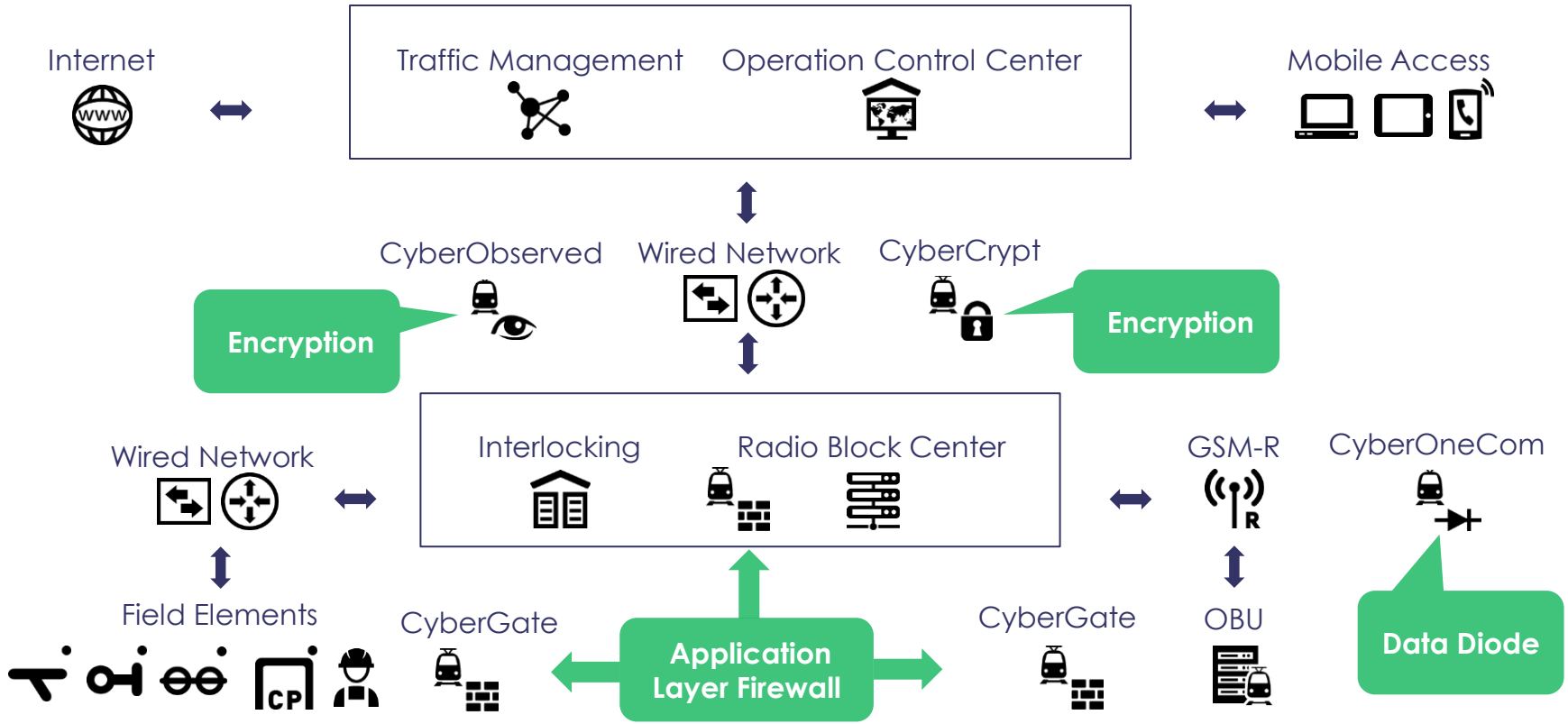
Areas of possible attacks in Rail Systems…



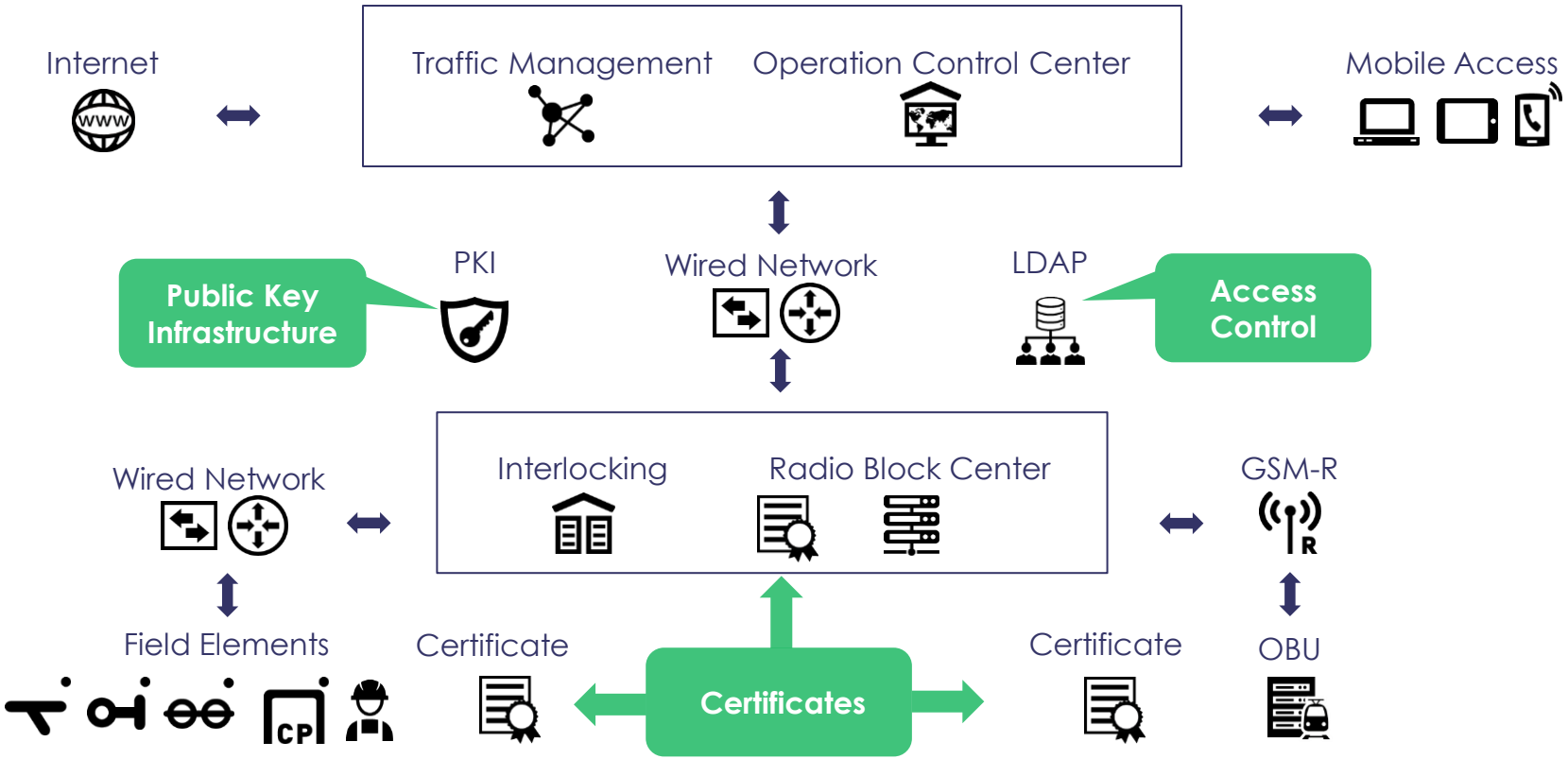
Areas of possible impacts in Rail Systems…



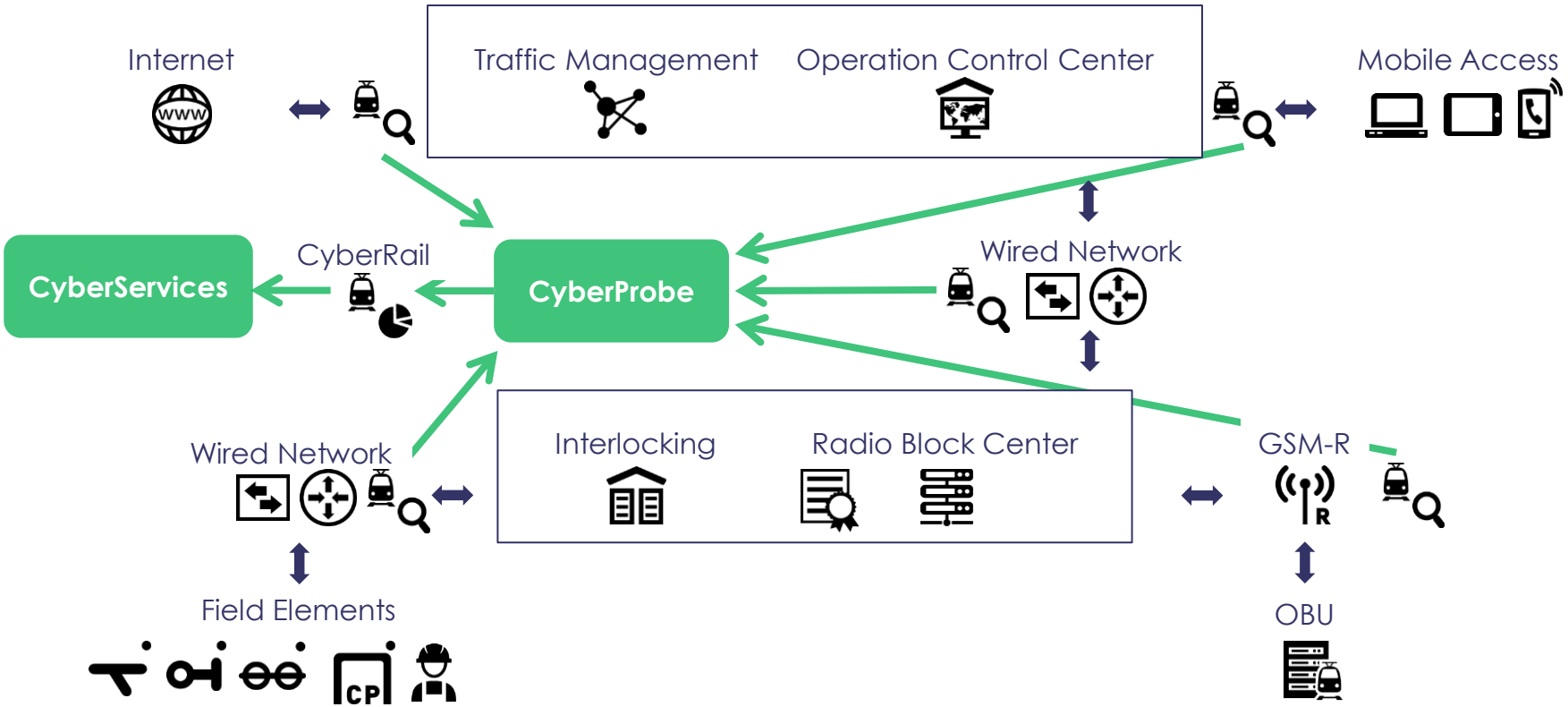
Areas to protect Rail Systems



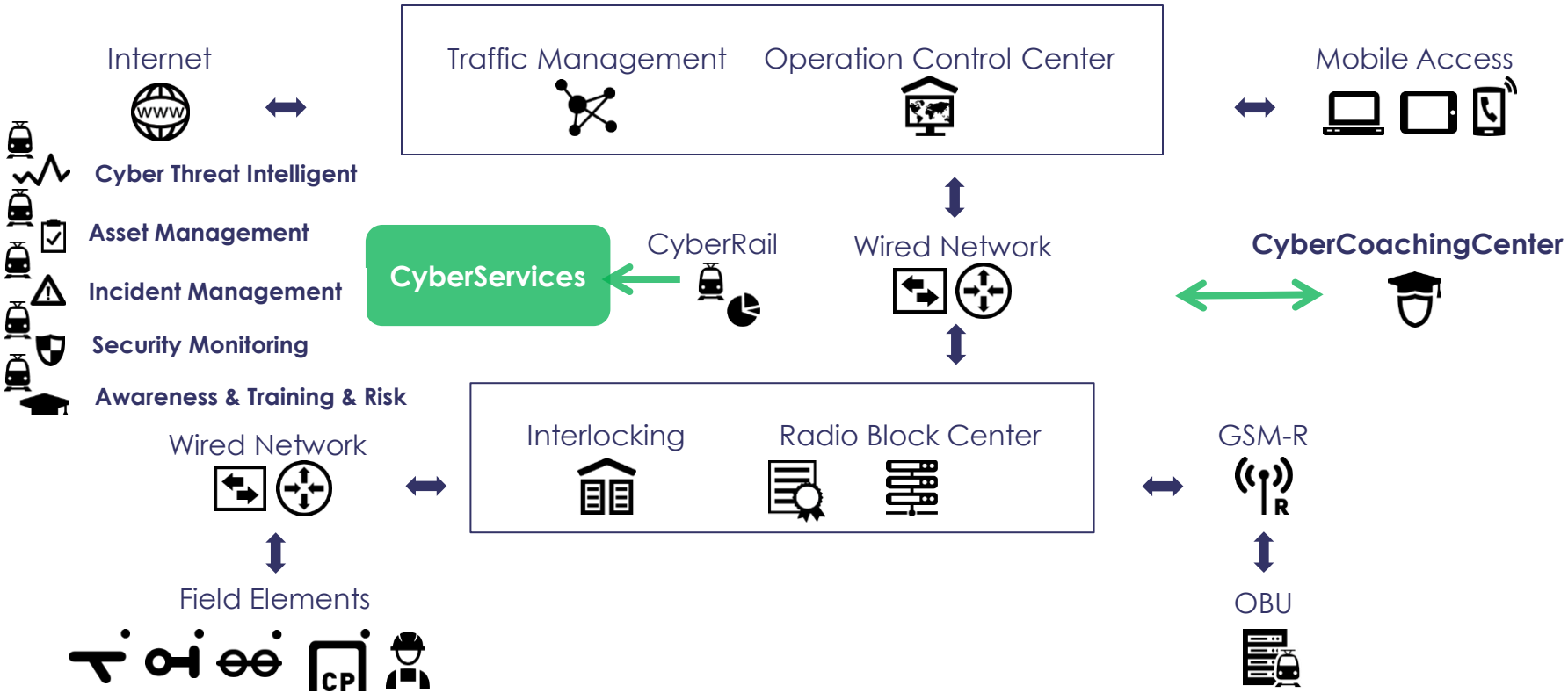
Areas to protect access in Rail Systems



Areas to monitor security in Rail Systems



Areas for security services in Rail Systems



THALES