INTERNATIONAL UNION OF RAILWAYS

unity, solidarity, universality

Security of Critical Rail Infrastructures: UIC contributions

Grigore M. Havârneanu, PhD

Research Advisor
Fundamental Values Department – Security Division

UNECE Workshop on Critical Transport Infrastructure and Cyber Security
Geneva, 6 September 2016

Overview

- **Security – a fundamental value of the railways**
- **Security at UIC**
  - working groups
  - publications
  - projects
  - future events
- **The way forward**

Why security?
Because the time of carefree attitude has finished!

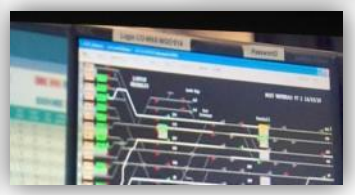
Conventional rails
High-Speed rails
Commuter lines
Stations & hubs
Services
Operations

Wagons
Dangerous goods
Global corridors

Rolling stock
Assets
Signalling
Telecommunications

Security threats and risks for railways...

Pickpocketing
Begging
Pandemic
Extreme Weather
Harassment
Property Damage
Freight Theft
Derailment
Power Blackout
Cyber Attacks
Terrorism
Media Reports
Graffiti
Migration
Metal Theft
Trespassing
Labor Dispute
Sabotage
Accidents
Mass Events
Violence
Ticket Fraud
Suicide



… may lead to unwelcome effects

Operational impact

- Operational performance, delay minutes and cancellations / significantly delayed services
- Availability of equipment and resources
- ...

Financial impact

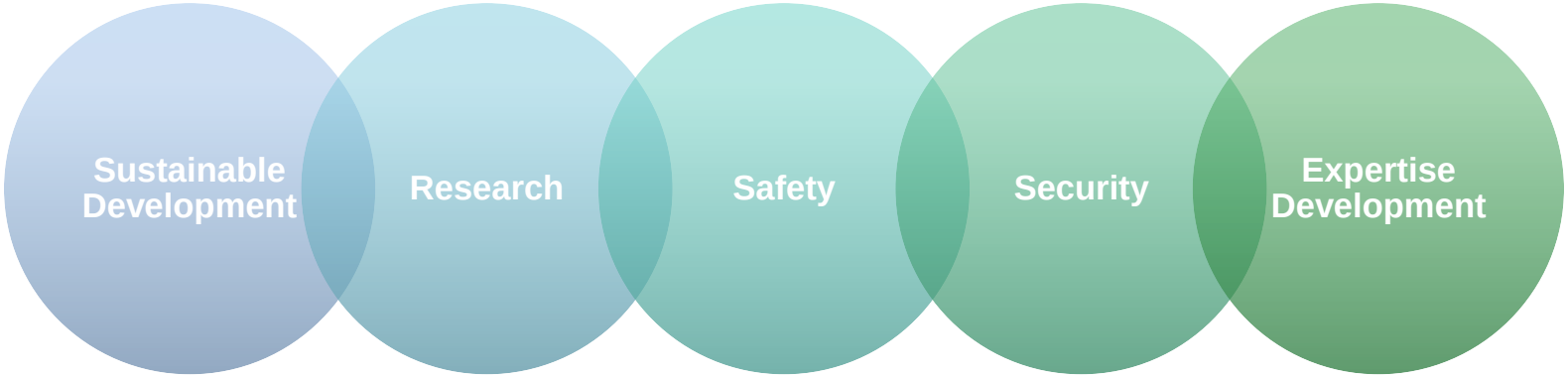
- Direct cost from loss of infrastructure and rolling stock components
- Compensations paid to train / freight operating companies
- Revenue loss due to loss of customers etc.
- ...

Reputation impact

- Media and public will look for errors, misjudgement
- Customers and business partners' confidence in how the railway is run and what is being done to secure the railways
- ...

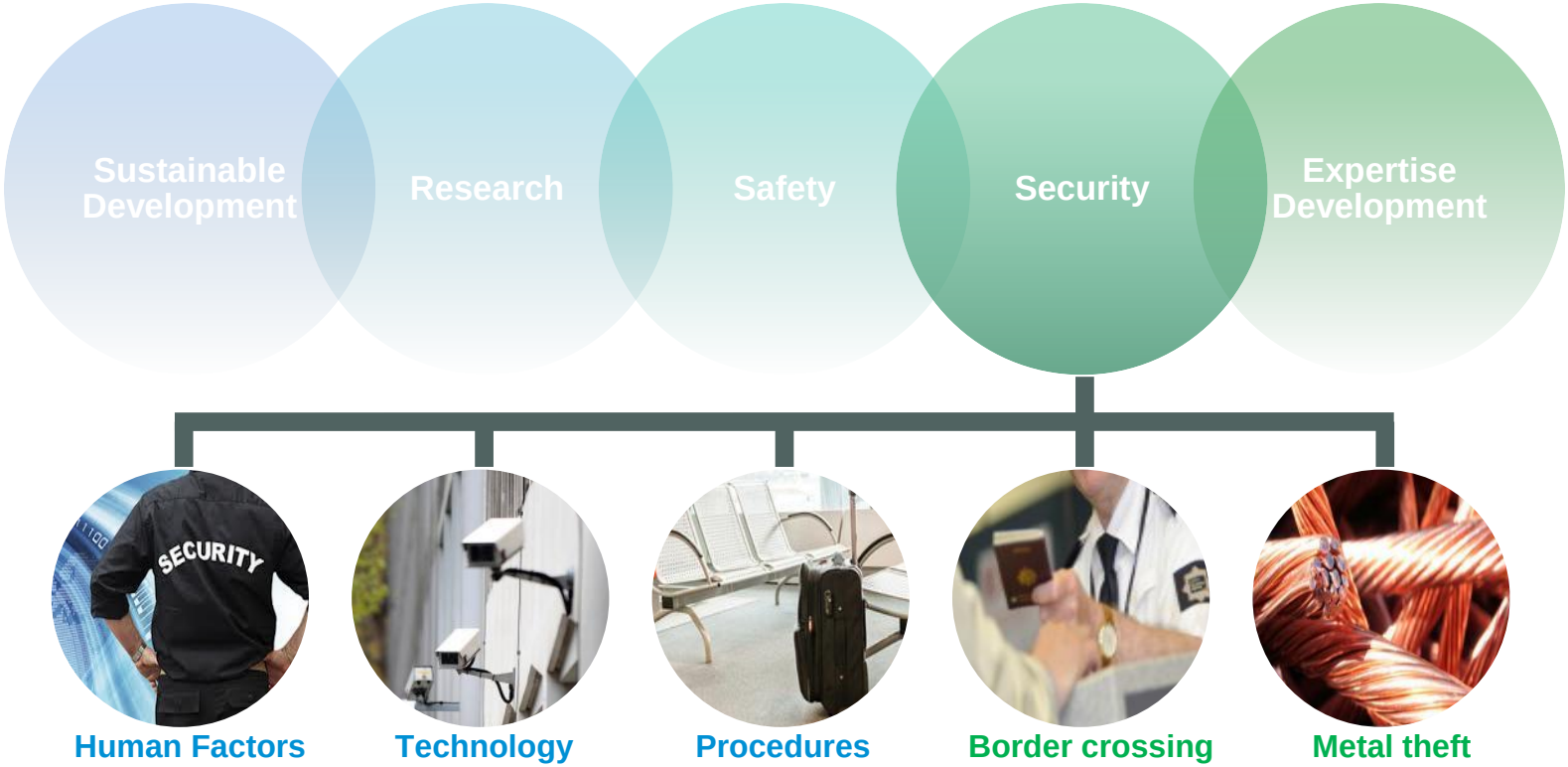
Security at UIC

- **Fundamental Values Department**



Security at UIC

> Global Security Platform and Steering Committee

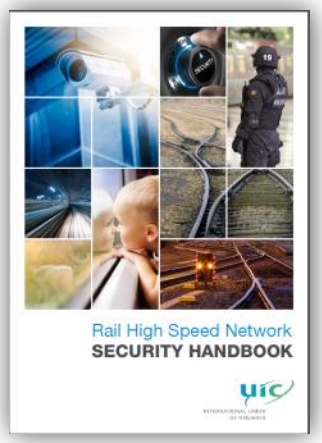


UIC Security Division Publications

Leaflets, brochures, practical guides & handbooks

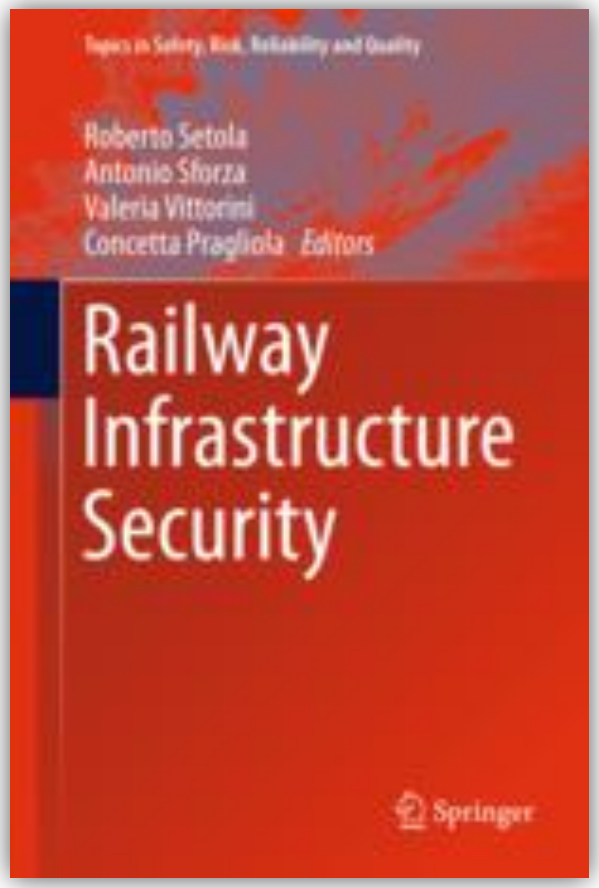
- **from the WGs**

- **on particular topics**



UIC Security Division Publications

Scientific publications



Past EU research projects

SECRET PROJECT
SECURITY OF RAILWAYS AGAINST ELECTROMAGNETIC ATTACKS

Protection of railway infrastructure against electromagnetic attacks - www.secret-project.eu

Starting date : 01 August 2012 for 36 Months
Budget : 4,268 M€ (including 3,059 M€ funding by EU)
Coordinator: IFSTTAR (France)
Partners: 10 Partners from 5 countries

IFSTTAR · UIC International Union of Railways · SNCF · UPV EHU · Politecnico di Torino · Zanasi & Partners · ALSTOM · Université de Liège

Past EU research projects

Protection of railway infrastructure against electromagnetic attacks - www.secret-project.eu

- **Added value:** Provision of recommendations to better protect rail communication and signalling system against electromagnetic attacks
- **White paper:** Key lessons learned

Ongoing EU research projects

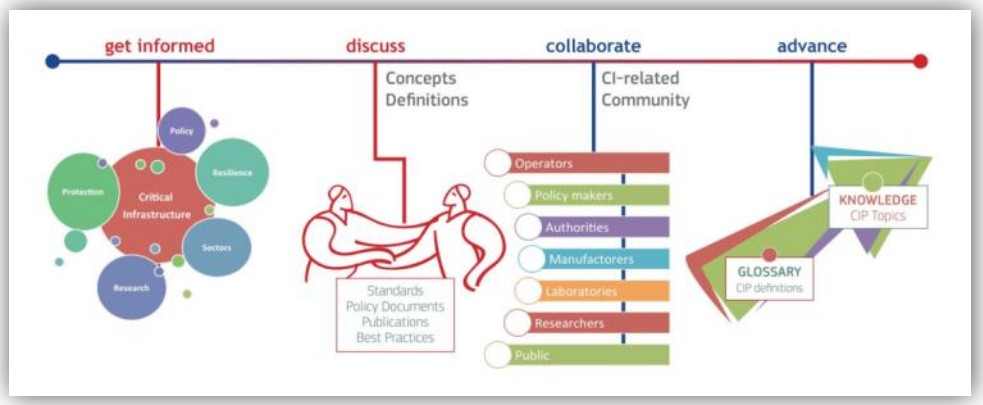
Critical Infrastructure Preparedness and Resilience Research Network - www.ciprnet.eu

Starting date: 01 March 2013 for 48 months
Coordinator: Fraunhofer IAIS
Partners: 11 partners from 8 countries: 10 R&D partners and UIC as end-user representative

Ongoing EU research projects

Critical Infrastructure Preparedness and Resilience Research Network - www.ciprnet.eu

- **Added value: common security culture among CI operators and authorities**
- **CIPedia©: A "Wikipedia" of CIP & CIR www.cipedia.eu**
- **Capability forming services**



Starting EU research projects

Horizon 2020 Programme

Cybersecurity in the RAILway sector

Topic: SR2-OC-IP2-01-2015 – Threat detection and profile protection definition for cyber-security assessment

- **Estimated starting date: 01/10/2016 for 2 years**
- **Consortium led by Evoleo with EUSKOIKER, FORTISS, UIC, Cassidian Cybersecurity, ATSEC**

Starting EU research projects

Horizon 2020 Programme

Cybersecurity in the RAILway sector

Objectives :

- deliver tailored specifications and recommendations for secure modern rail systems design and operation,
- create innovation by bringing existing intelligent and secure techniques from other domains into the railway context,
- research improved detection techniques in different operational scenarios

Project within UIC rail system department: ARGUS

Strategic aim:
How to avoid at the “railway level” the consequences coming from threats (cyber attacks…) on operational signaling networks?

- Availability (network fall down)
- Security (intrusion) and Safety (malware)
- Security management during all the life of the network

Results :
UIC will publish in 2016 a specific IRS (International Railway Standard) with requirements for:

- Functional level: data coherence, detection system...
- System organisation and architecture: Security and safety management system, skill, education, authorizations…

UIC Security Division Events

Workshops and Seminars

World Congress on Railway Security (every year since 2000)

Next events

Main topic: Security of stations

Organized by: Security Division + Station Managers Global Group (SMGG)

With local support from the Finnish Transport Agency (FTA)

Save the date and **call for papers** launched on 5 September.

Expected topics:
- Legal aspects
- Technologies (e.g. detection of weapons and explosives)
- Human Factors (e.g. management of crowds)

Next events

Early bird registrations until: 10 September 2016

Keynote speeches on hot topics of the moment

30 papers to be published by Springer

Topics:

- Innovative responses for the protection of cyber-physical systems
- Policies, best practices and lessons learned
- Advances in Human Factors, decision support, and cross-sector CI(I)P approaches
- Young CRITIS and CIPRNet Young CRITIS Award (CYCA)
- **http://critis2016.org**

The way forward

PAST: Never again

- Learn from past experiences
- Feedback loop

PRESENT: Crisis management

- Coherent policy for system resilience
- Mitigation of consequences (especially for CI)

FUTURE: Anticipate

- Think ahead
- New threats

Thank you for your kind attention!

UIC website (Security activity):	http://www.uic.org/security
Security private workspace: *(Around 1000 documents available)*	http://extranet.uic.org
Contact:	havarneanu@uic.org