INTERNATIONAL UNION
OF RAILWAYS

unity, solidarity, universality

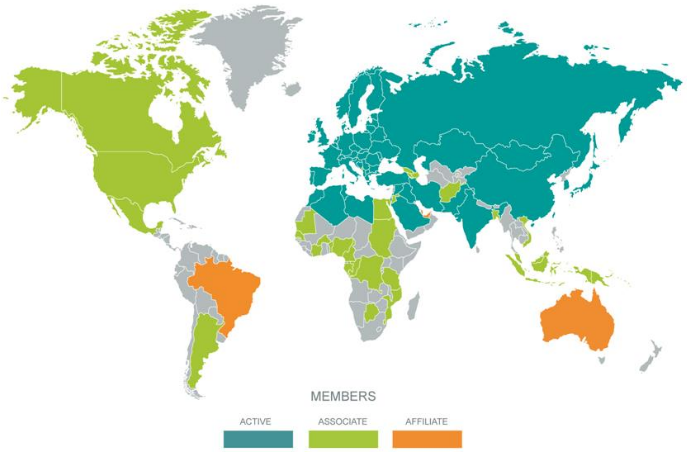
Lessons learned from EU funded projects SECRET and CYRAIL

CYBERSECURITY4RAIL,
Brussels, 04 October 2017

Marie-Hélène Bonneau, UIC Security Division

UIC today

- 200 Members in 100 countries
- Cooperation with over 100 institutions
- 700 UIC Leaflets, new International Raiway Solutions (IRS)
- 85 congresses, conferences, workshops



Security at UIC

UIC
DB
13th UIC World Security Congress
Potsdam 2017
© Deutsche Bahn AG Max Lautenschläger
29 Nov – 1 Dec Potsdam, Germany

- Security platform : global level

  Current chair : DB AG

  Current vice chair : VIA RAIL CANADA

- 5 Working groups

  Human factors, Technologies, Strategy and regulation, Border crossing and international corridors, Sabotage-Intrusions-Attacks

- An annual worldwide congress et an annual security week

  2017 security congress in Potsdam, Germany on “Rail freight secutiy door to door”

  2018 security congress will focus on “crisis management & resilience

- Research projects

  Provide rail companies with recommendations/toolbox

  Develop cooperation with other sectors at international level

Cyber security on rail : the challenges

- Rail Network is a critical infrastructure
- Rail Systems are more and more connected and open
- Rail Technologies are becoming more and more interoperable and harmonized
- Threats (human and technology based) - are adapting quicker that traditional security detection methods

SECRET PROJECT

SECURITY OF RAILWAYS AGAINST ELECTROMAGNETIC ATTACKS

EU SECRET project

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement n° 285136

- Protection of railway infrastructure against EM attacks

  Duration: 01 August 2012 for 36 Months

  Budget : 4,268 M€ (3,059 M€ funding by EU)

  Coordinator : IFSTTAR (France)

  Partners : 10 Partners from 5 countries

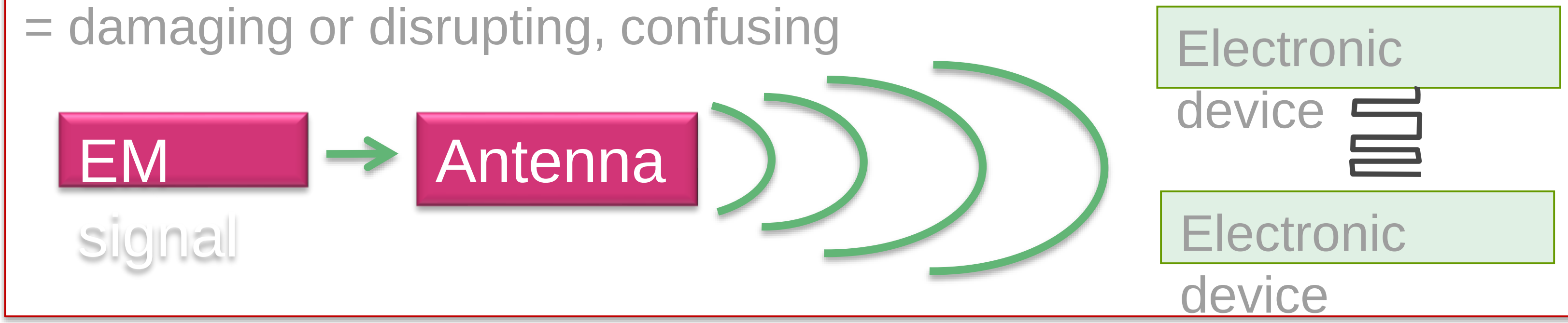
IFSTTAR SNCF UIC INTERNATIONAL UNION OF RAILWAYS ALSTOM POLITECNICO DI TORINO 1859 1906

Université de Liège ULg eman ta zabal zazu UPV EHU TRIALOG Fraunhofer IAIS Zanasi & Partners

EM attacks: definition

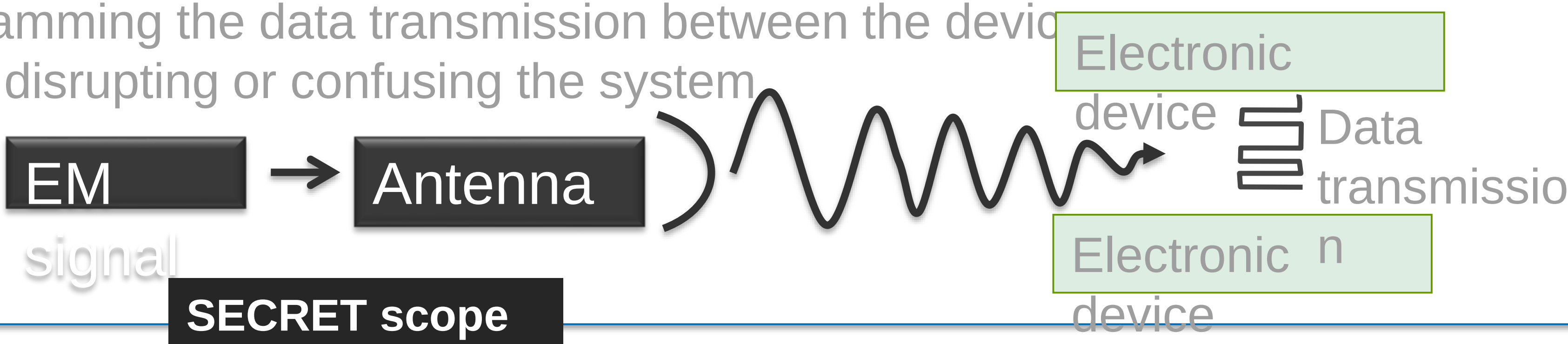
Case 1: The target is an electronic device

Permanent or Temporary Default on electronic devices
= damaging or disrupting, confusing



Case 2: The target is to avoid the data transmission

Jamming the data transmission between the devic
= disrupting or confusing the system



SECRET scope

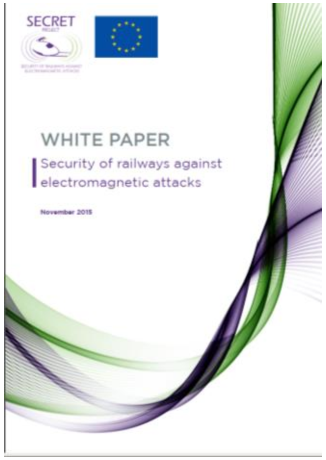
SECRET PROJECT
SECURITY OF RAILWAYS AGAINST ELECTROMAGNETIC ATTACKS

Objectives

- To assess the risks and consequences of EM attacks on the rail infrastructure
- to identify preventive and recovery measures
- To develop protection solution for EM attacks
- To produce technical recommendations to reinforce the railway infrastructure

Public Results : WHITE PAPER

- About 40 recommendations
  - Organisation
  - Standardization
  - Technical



SECRET

WHITE PAPER

Security of railways against electromagnetic attacks

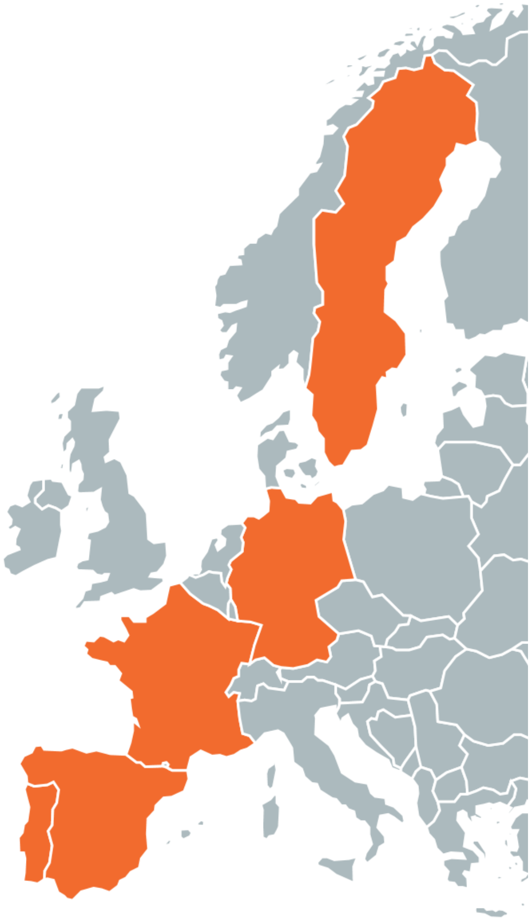
November 2015

- 3 categories of recommendations
  - Prevention from EM jamming effects
  - EM attack detection solution
  - Mitigation of EM jamming effect

Available at http://www.secret-project.eu

Cybersecurity in the RAILway sector

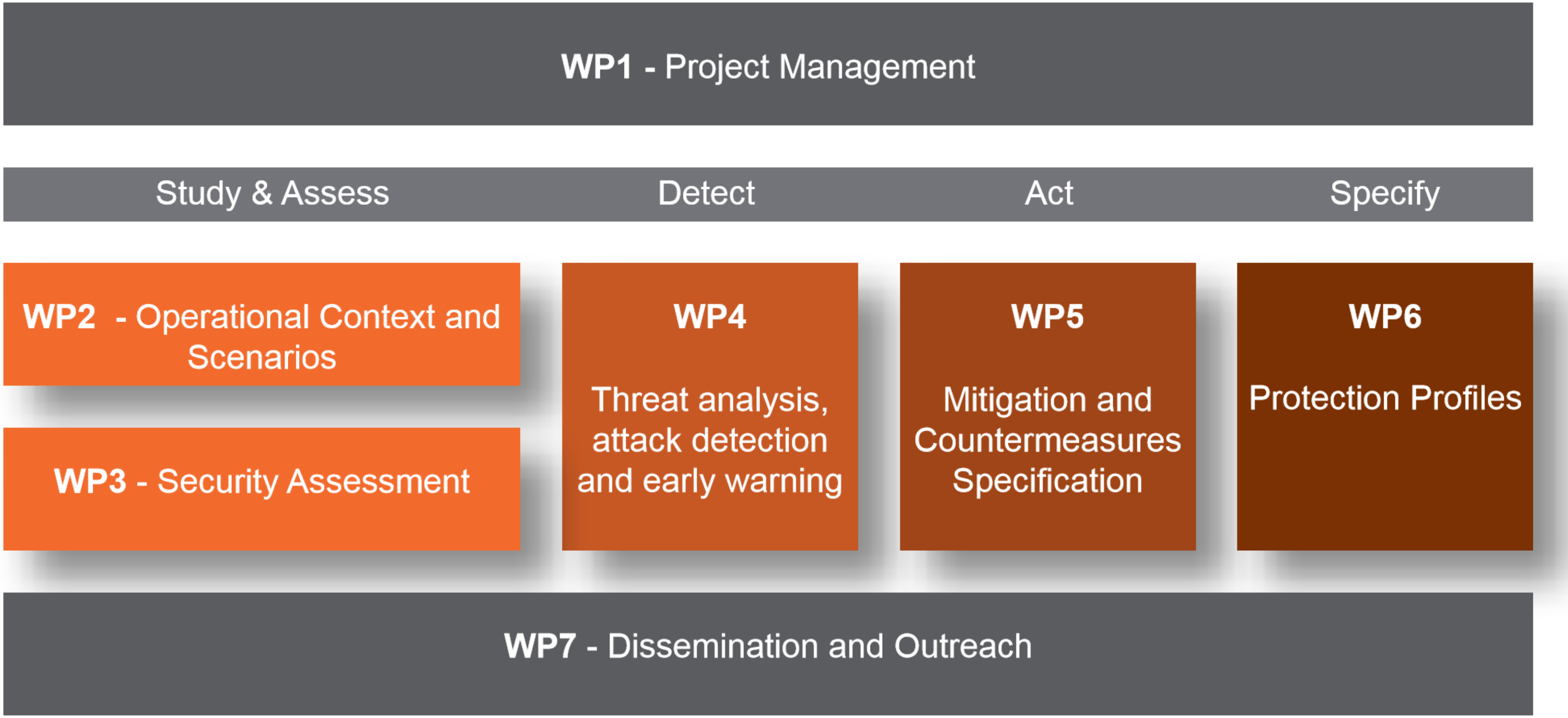
- Duration: 1 Oct. 2016 - 30 Sept. 2018
- Estimated Budget : 1,500 000
- Coordinator : Evoleo
- Consortium : 6 partners from 5 countries



Goal

- Perform a cyber security assessment of the Railway systems
  - » *What are the most critical railway services, zones and communications?*
- Deliver a taxonomy of threats targeting rail management and control systems
  - » *What are the threats?*
- Assess and select innovative rail management systems attack detection techniques
  - » *How to detect attacks targeting rail management systems?*
- Specify Countermeasures and Mitigation strategies for improved quality levels;
  - » *How to prevent , how to make the system resilient*
- Achieve Security by Design, by selecting a development framework and specifying Protection Profiles with Evaluation of Assurance Levels.

CYRAIL Structure



WP1 - Project Management

Study & Assess

Detect

Act

Specify

WP2 - Operational Context and Scenarios

WP3 - Security Assessment

WP4

Threat analysis, attack detection and early warning

WP5

Mitigation and Countermeasures Specification

WP6

Protection Profiles

WP7 - Dissemination and Outreach

On-going work : operational scenario

- Work led by UIC Rail System Department

INTERNATIONAL UNION
OF RAILWAYS

- Definition of the operational scenario based on
  - » different communication systems
  - » smart rail transport technologies such as automatic train Location, train movement management, train data management, smart ticketing, ..
- Focus on signaling and communication system

Security Assessment Methodology for the railway domain

- Work led by the university of the Basque country : euskoiker

- No common European standard to define a security assessment methodology for rail

- Analysis of existing Cyber Security Assessment Methodologies

- Definition of a Security Risk Assessment Methodology based on ISO 62443 standard and ETSI TVRA

Added value

- Preventing cyber-attacks
- improving the operational security level of the different rail segments
- enhancing the robustness of the railway information, control and signalling sub-systems

Further information

- Secret project : **www.secret-project.eu**
- Cyrail project : **www.cyrail.eu**
- UIC Security division : **www.uic.org/security**

- Contact point : **security@uic.org**