SECRET PROJECT

SECURITY OF RAILWAYS AGAINST ELECTROMAGNETIC ATTACKS

SEVENTH FRAMEWORK PROGRAMME

Project co-funded by the European Commission

SECurity of Railways against Electromagnetic aTtacks

Virginie Deniau, Scientific coordination
virginie.deniau@ifsttar.fr

IFSTTAR SNCF UIC INTERNATIONAL UNION OF RAILWAYS TRIALOG UPV EHU ALSTOM Université de Liège Zanasi & Partners Fraunhofer IAIS

SECRET *SECurity of Railways against Electromagnetic aTtacks*

- **Collaborative project 01/08/2012 to 31/07/2015 - 36 months**
- **website address: http://www.secret-project.eu**
- **Name of the coordinating persons**
  - Virginie DENIAU - IFSTTAR (scientific coordinator) and
  - Erik BESSMANN- IFSTTAR (project manager)

- **10 partners**

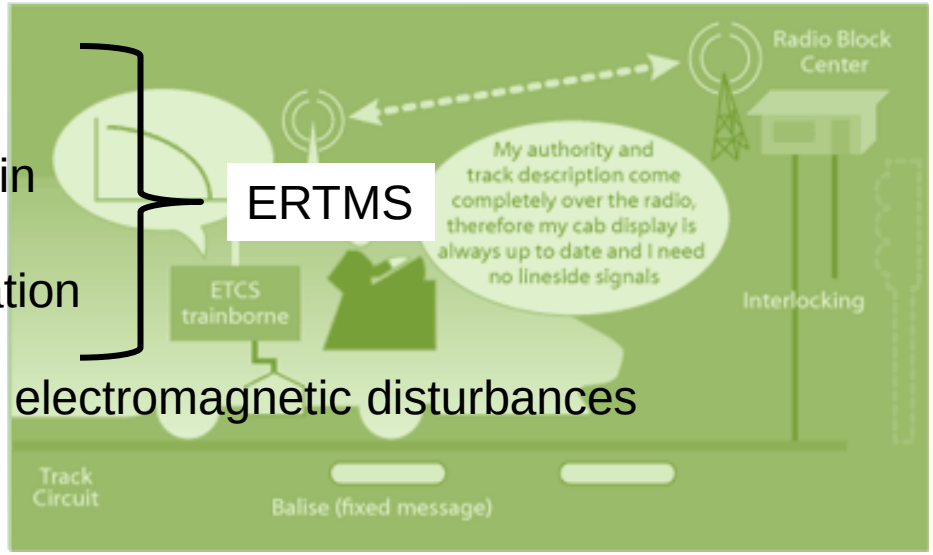
IFSTTAR, Politecnico di Torino, SNCF, UIC International Union of Railways, Zanasi & Partners, ALSTOM, TRIALOG, Fraunhofer IAIS, UPV EHU, Université de Liège

Context of SECRET

Railway network

- ↗ Speed, ↗ capacity
- Centralized management
- Automatic action on board train
- Sensors (balise), antennas
- Spot or continous communication systems

⇒ More and more vulnerable to electromagnetic disturbances



+

- Multiplication emission devices, antennas and amplifiers accessible to the general public
- ⇒ Easy to design emission devices able to disrupt rail technologies

Context

Railway network : an attractive target for attacks

- Mass transport system
- Ease of access, openess
- High economic and security impacts

ERTMS homogenizes the technologies in Europe and so the **EM** vulnerabilities

⇒ Facilitates the implementation of organized and simultaneous attacks

SECRET Project objectives

To Protect railway communications and signaling against potential electromagnetic Attacks by solutions compatible with ERTMS

- **To assess the real risks concerning EM attacks on the rail networks**
- **To identify areas for strengthening the railway network against EM attacks**
- **To develop detection solution for EM attacks**
- **To design management system for EM attacks integrated into the rail communication architecture, making it resilient**

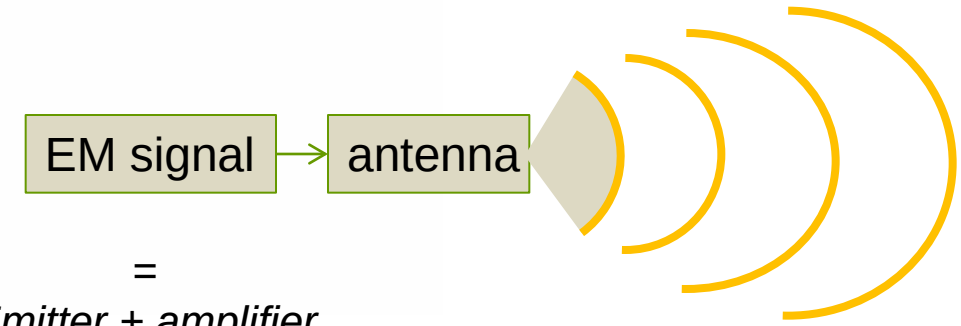
IEMI: Intentional EM Interferences

- **The International Electrotechnical Commission (IEC) defines IEMI as the**

"intentional malicious generation of electromagnetic energy introducing noise or signals into electric and electronic systems thus disrupting, confusing, or damaging these systems for terrorist or criminal purposes."

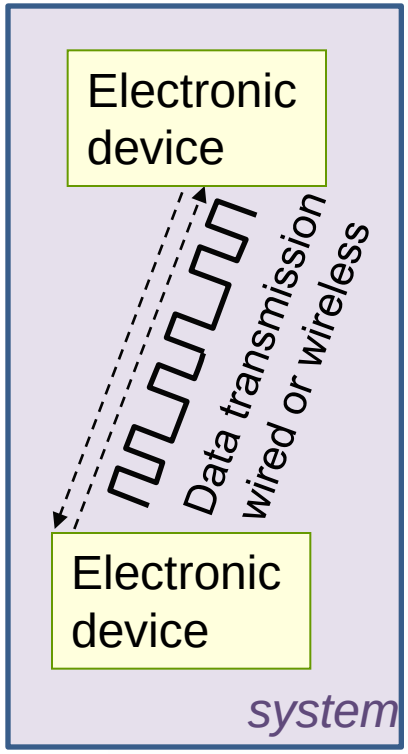
EM attacks…which methods?

Illustration with radiated interferences



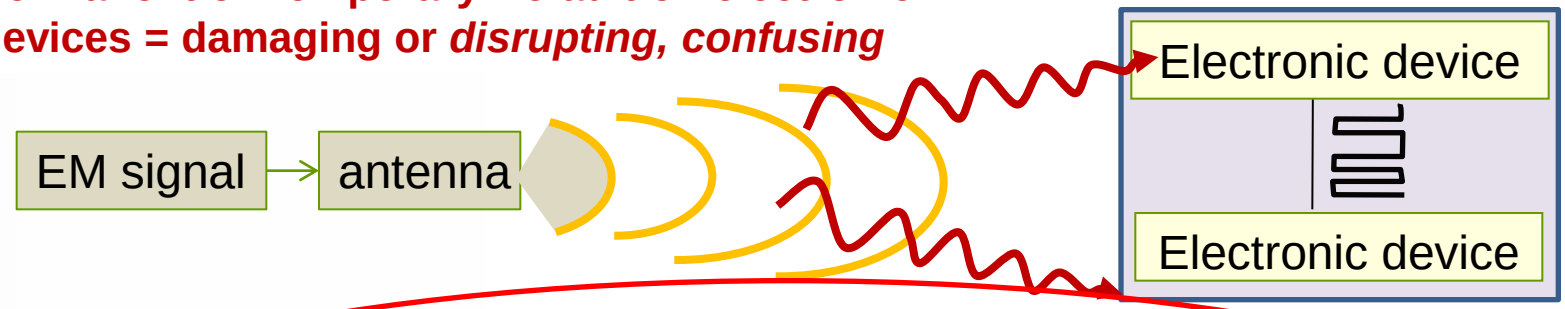
=

Emitter + amplifier



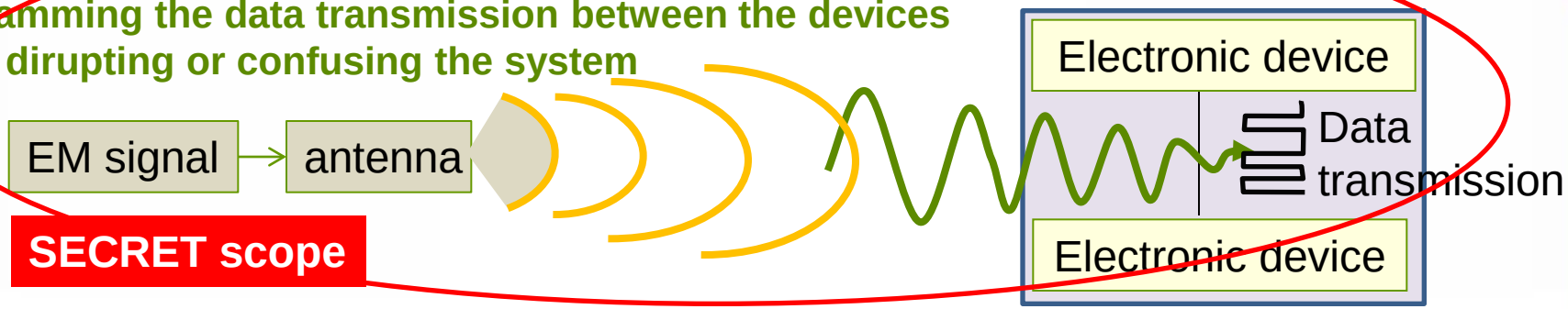
Case 1: the target is an electronic device

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



Case 2: The target is to avoid the data transmission

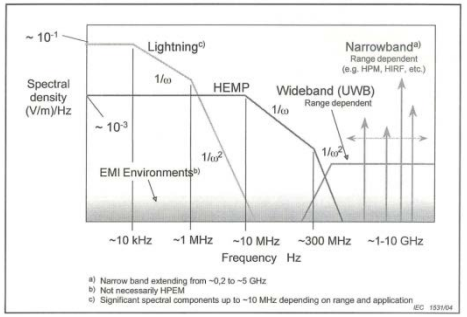
Jamming the data transmission between the devices = dirupting or confusing the system



Case 3: The target is to intervene in the system and to modify his behavior = modyfing the transmitted data

EM attack devices

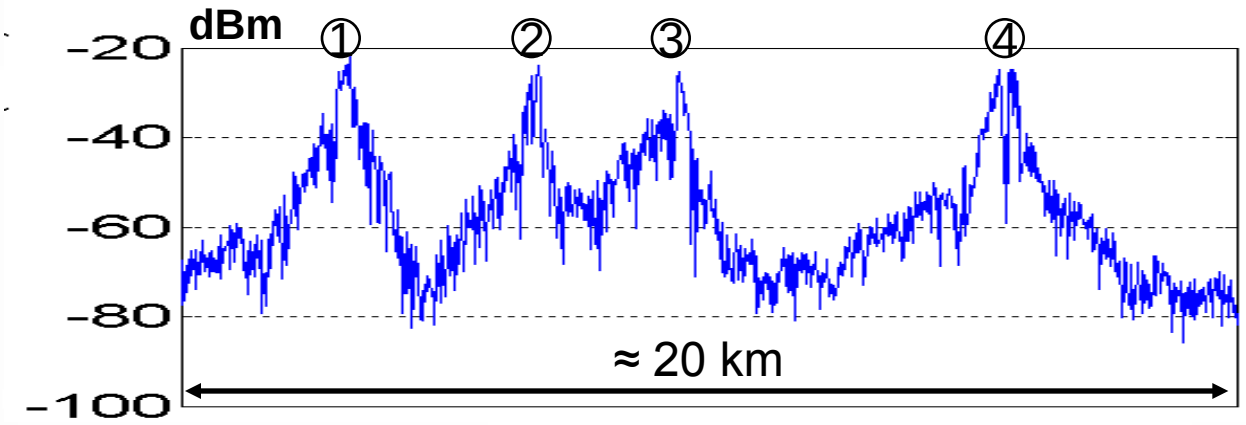
- **IEMI: Intentional EM Interferences**
  - HPEM sources: High Power EM sources
  - HEMP: High-altitude ElectroMagnetic Pulse



  - Any system of emission unauthorized or not, available on public domain: Jammer, remote control, emission and amplifier components, EMP Guns…..

Scope of the SECRET project

SECRET
PROJECT



Power of the GSM-R signal received by the train

Jammers can generate similar power levels over the GSM-R frequency band

Project Structure

- **WP1 Threat analysis and risks assessment of EM attack scenarios for Railway**
  Leader : SNCF
- **WP2 Static protection: Topologic solutions to strengthen the railway infrastructure**
  leader: Polito
- **WP3 Monitoring the EM environment and detection of EM attacks**
  leader: IFSTTAR
- **WP4 Dynamic protection: detection system for resilient architecture**
  leader: Trialog

- **WP5 Recommendations for a resilient railway infrastructure to EM attacks**
  leader: Alstom

- **WP6 Exploitation and Dissemination** — **leader : UIC**
- **WP7 Technical management** — **leader: IFSTTAR**
- **WP8 Administrative and financial management** — **leader: IFSTTAR**

Presentations in link with the WPs

- **WP1 Threat analysis and risks assessment of EM attack scenarios for Railway**
  - EM attacks and risks analysis for railways – by SNCF
  - EM attacks and threats for railways – by Zanasi &Partners
- **WP2 Static protection: Topologic solutions to strengthen the railway infrastructure**
  - IEMI and immunity tests in SECRET - by Polito
- **WP3 Monitoring the EM environment and detection of EM attacks**
  - IEMI: signature and detection in railways – by IFSTTAR and EHU
- **WP4 Dynamic protection: detection system for resilient architecture**
  - Detection and resilient architecture- by IFSTTAR and TRIALOG
  - Implementing the Multipath Communication System (Work in Pogress) - by EHU
- **WP5 Recommendations for a resilient railway infrastructure to EM attacks**
  - Recommendations and strategy – by ALSTOM

SECRET
PROJECT

Thank you and have a nice workshop!