SECRET project: Motivations, context and objectives
Virginie Deniau (IFSTTAR)

SECRET was motivated by the awareness of the threat of intentional electromagnetic interferences linked to the evolution of our critical infrastructures. Indeed, in not taking into account the electromagnetic vulnerability of new integrated technologies, upon which a greatly increasing proportion of railway network management is based, we multiply the risk of threat becoming reality.

Through this project, we wanted to illustrate the risk by implementing certain electromagnetic attacks and analyzing their effects, thereby inciting the different railway actors to work together to strengthen the resilience of a system that must remain effective and safe for the serenity of our society.

The second objective was to open ways to resilience solutions regarding this type of attack. Preferring to avoid unconstructive and alarming rhetoric, which is unjustified as the European railway system is above all a very safe means of transport, we wanted to identify and propose strategies in which each actor would be able to inspire itself in order to act towards resilience.

These strategies mainly concern:

- *The tests that can be performed to assess the susceptibility of individual network components dealing with intentional interferences and allowing each designer, integrator or operator to build, evaluate and compare the susceptibility of these products,*
- *The methods of detection of electromagnetic attacks that are essential for several reasons: Detecting is to be able to demonstrate that we have been a victim of an electromagnetic attack, detecting avoids confusing an electromagnetic attack with a technical failure which could unduly jeopardize the operator, who could initiate unnecessary diagnostic inquiries. And, finally a reliable detection can instigate a fast and appropriate reaction to the threat.*
- *The resilient architecture which is a compulsory issue when we consider a critical infrastructure which is a network. The resilient architecture has to ensure the maintenance of communication for the transmission of critical information, thus maintaining the control of the network. We worked on an adapted architecture permitting us to assess the impact of certain technological solutions on reliability and responsiveness.*

Finally, knowing all the importance of community work performed by the various standardization organizations, and so that every stakeholder (manufacturers, operators, infrastructure managers) is able to work at their own level for a safer railway system, and that all the advances fit together harmoniously, we have sought to extract exploitable recommendations at different levels (organization, standardization, technical recommendations).

So, for today, we've established a program of presentations and demonstrations that we hope will allow each of you to go away with ideas and concrete ways, to confidently and effectively deal with this new threat.

11H00-11H15 H. Philippe (SNCF): Intentional ElectroMagnetic Interferences (IEMI) and railway: What are the risks?

Abstract: This presentation is focused on the results of the evaluation of electromagnetic attack to railway system as critical infrastructure. The means to perform an electromagnetic attack and technical characterisation of the potential attack devices were considered. An analysis and a classification of the devices that could be found on market, has led to a selection of devices to consider in SECRET project. Then, different methodologies for risk assessment were considered in order to answer the question: "Must we be afraid about EM attacks to railway infrastructure?". This presentation will detail the risk assessment approach which was developed on the base of the **Failure mode and effects analysis** (FMEA) in order to classify the technical risks which can be produced by EM attack and to identify the case of critical situations.

11H15-11H30 Alessandro Zanasi (ZANASI & partners): “Risk Assessment: human factor and cyber threat analysis”

Abstract: Risk assessment is a way of evaluating risks from quantitative and/or qualitative points of view which has a longstanding tradition in high tech industries such as the nuclear, aerospace, oil, military, and, of course, rail industries are. Methods for the assessment of risk, in which the evaluation of the recognized threats is the first necessary step, may differ between industries and whether the focus is on general safety engineering or public security. In this presentation it will be shown how the risk assessment activities performed in SECRET have taken into account the human factor (important element for the terrorism threat) when related to cyber technologies (as EM technology is).

About 5-10 mm questions

11H40-12H10 Veronique Beauvois (ULG): Standardisation and immunity tests regarding IEMI

Abstract: Considering the vulnerabilities to IEMI put in evidence in this project, there is a gap in the present standardization. Tests were carried out in SECRET on GSM-R, TETRA and Eurobalise to assess the resistance of railway communication systems facing the signals generated by telecom jammers. After a short background about the present standardisation in the domain of Electromagnetic immunity, this presentation will develop how these tests could influence the development of new railway equipment and standards.

Flavio Canavero (POLITO): Railway Vulnerability to EM attacks

Abstract: Intentional malicious generation of electromagnetic energy, introducing noise or signals into electric and electronic systems, may disrupt, confuse or damage railways equipment and infrastructure for terrorist or criminal purposes. Disabling electromagnetic pulses can be generated with improvised weapons, which can be easily acquired or manufactured by moderately technologically-skilled terrorist groups with limited financial resources. Although the potential impact is less critical than in the case of nuclear electromagnetic impulses, such devices could still inflict major damages. The current situation of the European railway network in terms of vulnerable technologies in case of EM attacks will be illustrated.

About 5-10 mm questions

12h10-12H30 Demonstrations

WP2 GSM-R test bench (vulnerability of GSM-R against EM attacks)	WP3 EM Attack detection : Focus on the implementation solutions

12H30-13H50 Lunch

13H50 -14H10 Marc Heddebaut (IFSTTAR): Intentional ElectroMagnetic Interference in Railway: why and how to sense them?

Abstract: This presentation considers IEMIs generated by low power electromagnetic jammers operated in railway environments. Jammers can be used to disturb or even interrupt the radio communications of railway operators. This presentation will detail methods which were developed and evaluated to detect jamming signals appearing in a radio channel while a radio communication is running. Several supervised detection methods were tested and will be presented. The performances of the different methods will be discussed.

14H10 -14H25 Marina Aguado (UPV): Impact of EM attack signatures on ETCS Quality of Service Indicators

Abstract: We present how electromagnetic interferences in the communication architecture may disrupt the railway communication architectures resulting in the introduction of a potential risk into the railway operation. The main goal of our research is to establish the link between these interferences and the Quality of Service or Key Performance Indicators (KPIs) of a Railway Control Signalling System (RCSS), i.e. ETCS communication between the train and the RBC. We assess the impact of the jammers on the application level and not only on the physical layer. We will present the internals of our integrated RCSS simulation framework and the simulation results obtained for the two different jammers. Our simulation results show that information provided by network devices (packet loss, delay) could be used as an additional sensor to detect abnormal behaviour or attacks.

About 5-10 mm questions

14H35-14H45 Antonio Kung or Michel Sall (TRIALOG): Architecture for resilience in presence of IEMI

Abstract: This presentation will present the SECRET architecture for resilient communication under EM attacks. It will highlight the important features of such an architecture consisting of an attack detection component at train and trackside level, a health attack manager at train, trackside and central level and a redundant communication capability. It will show how such architecture is designed and evaluated. It will also elaborate on how such architecture can be integrated in railways systems.

14H45-14H55 Eduardo Jacob (UPV/EHU): Multipath Communication System (MCS): Using Multipath-Transmission Control Protocol (MPTCP) for resiliency

Abstract: The Multipath Communication System (MCS) is the system of the Resilient Communication Architecture (RCA) of the SECRET Project responsible for managing multiple communication interfaces with the objective of improving the resiliency of the wireless communications between the train and the command centre. The presentation will cover the initial considerations for the design of the system, the components it consists of, the configurable traffic policies and the interaction with the rest of components of the RCA.

14h55-15H15 Demonstrations

14H55- 15H15 Proof of concept of resilient architecture for dynamic protection system to IEMI, for railway applications
Presented and commented by Christian Pinedo and Eduardo Jacob (UPV/EHU)

15H15-15H25 questions discussions

15H25- 15H40 coffee break

15H40- 16H10 Pierre Lambert (Alstom): Recommendations to railway domain issued from SECRET project

Abstract: Throughout the SECRET project activities, we reviewed on regular basis all subjects that can form the basis of technical recommendations able to improve the railway resiliency to EM attacks. The recommendations were analyzed and, for some of them, evaluated for their technical feasibility. Originally foreseen as inputs to UIC/UNIFE TECREC standardization, the SECRET technical recommendations were classified in three categories: standardization, engineering guidelines and operational. The presentation aims to provide an overview of the recommendations on preventive and recovery measures as well as the suitable methodology to evaluate and mitigate EM attacks in the railway context. Finally, the recommendations consider the possible evolutions of the system architecture following the introduction of next generation technologies.

About 5-10 mm questions

16H20-16h50 Point of views
IEC, EPSF (French Rail NSA), ANSSI, ERA, PO

16H50-17H00 Exploitation plan by Marie-Hélène Bonneau (UIC)
Conclusion by IFSTTAR