PRESS RELEASE Nr. 32/2015

UIC, in charge of the dissemination, participated in the Final Conference of “SECRET” on Security of Railways against Electromagnetic Attacks

(*Lille, France, 30 October 2015*) The SECRET consortium, IFSTTAR, coordinator of the project, and the International Union of Railways (UIC), in charge of the dissemination of the results among its Members, held the SECRET Final Conference at the IFSTTAR office in Lille, France, on 29 October 2015.

The consortium includes 10 members: research centres – IFSTTAR – Institut français des sciences et technologies des transports, de l'aménagement et des réseaux (the French institute for science and technology for transport, development and networks); Fraunhofer Institut für IAIS (Fraunhofer Institute for Intelligent Analysis and Information Systems); Politecnico di Torino (Polytechnic University of Turin); University of Liege – Institut Montefiore; University of the Basque Country; ZANASI Alessandro Srl), manufacturers (ALSTOM TRANSPORT S.A., TRIALOG) and railway representatives (SNCF, UIC).

SECRET (SECurity of Railways against Electromagnetic aTtacks) is a three-year research project co-funded by the European Commission as part of the 4th call for proposals under the 7th Framework Programme. The project was officially launched on 1 August 2012 for a duration of 40 months.

The project SECRET aims to assess the risks and consequences of EM (Electromagnetic) attacks on the rail infrastructure, to identify preventive and recovery measures and to develop protection solutions to ensure the security of the rail network, subject to intentional EM interferences, which can disturb a large number of command-control, communication or signalling systems.

Around 85 participants came from 12 different countries at the international level from 55 companies including external experts of the advisory group; decision-makers from rail companies; infrastructure managers and rail operators; the scientific community; policy makers; standardisation bodies; related EU projects and the general public.

Mr Marc Antoni, Director of the UIC Rail System Department, delivered the opening speech of the SECRET final conference and gave a few words about the role of UIC and highlighted the importance of the SECRET project for the railways as cyber attacks may have consequences on transport availability with huge losses.

He said "*SECRET is a good example of a project that is supporting the interoperability of the European railway network and working towards improving the security of the rail system by ensuring its critical signalling system is robust and resilient in the face of EM attacks."*

He added: *"SECRET is an important project for UIC: its involvement in such projects can benefit all its members by disseminating the relevant information and editing professional standards called IRS (International Railway Standards): The work and results of SECRET which lead to a set of technical recommendations will be disseminated to our members and submitted to standardisation bodies for "industry standards" and transcribed by UIC for "professional standards", as practical guidelines for the railways (infrastructure managers and railway undertakings) responsible for the safety and security of the system. This standard will complete the IRS describing "how to manage critical computerised signalling systems using IP networks"... the work is ongoing.*

The SECRET project has enabled players from very different backgrounds: researchers, universities, providers and railways from five different countries to work together – thanks to EU financing, without which nothing like this would have been possible."

He then thanked all the organisers and the partners and staff involved: and gave special thanks to IFSSTAR as coordinator of the project.

Mr Pierre Brodin, from the French Ministry of Sustainable Development (DGITM), added that intentional electromagnetic interferences are a growing threat and need to be addressed. Rail security is an important issue and security cannot be achieved by the government alone, but all stakeholders have to be involved, all playing their part.

The following issues were presented:

- SECRET project: Context and objectives by Virginie Deniau (IFSTTAR)
- Intentional ElectroMagnetic Interferences (IEMI) and railway: what are the risks?, by Henry Philippe (SNCF)
- Risk Assessment: human factor and cyber threat analysis, by Alessandro Zanasi (Zanasi & Partners)
- Standardisation and immunity tests regarding Intentional Electromagnetic Interferences (IEMI), by Véronique Beauvois (ULG)
- Railway Vulnerability to EM attacks, by Flavio Canavero (POLITO)
- Intentional ElectroMagnetic Interference in Railway: why and how to sense them?, by Marc Heddebaut (IFSTTAR)
- Impact of EM attack signatures on ETCS Quality of Service Indicators, by Marina Aguado (UPV/EHU)
- Architecture for resilience in presence of IEMI by Antonio Kung and Michel Sall (TRIALOG)
- Multipath Communication System (MCS): Using Multipath- Transmission Control Protocol (MPTCP) for resiliency by Eduardo Jacob (UPV/EHU)

Real-time demonstrations were held in front of the participants, includes tests for GSM-R susceptibility to EM attacks. The possible implementations were also presented and how to cope with the effect of the jammer. In the afternoon, participants were shown an example of resilient architecture for a dynamic protection system to EM interferences for railway applications.

Mr Pierre Lambert from Alstom focused on railway recommendations issued for the SECRET project. The SECRET technical recommendations were classified into three categories: standardisation, engineering (design, techniques) guidelines and operational (process, methodology, railway application). 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.

Several points of view from the EPSF (French Rail National Safety Authority), the IEC (International Electrotechnical commission), the ANSSI (French Network and Information Security), the ERA (European Railway Agency) and the European Commission were delivered.

Mr Bruno Chenard, the Project Officer from the European Commission, emphasised the good results of the projects and said that the results must be disseminated at the international and European level and to the standardisation bodies. It is important to have feedback from the stakeholders.

Mrs Marie-Hélène Bonneau, Senior Adviser at the UIC Security Division, gave an overview of the project's exploitation plan to maintain the viability of the project results and to distribute appropriate information to each type of identified target.

Mrs Virginie Deniau, scientific coordinator of the project from IFSTTAR, delivered the final conclusion. She highlighted some perspectives and for example the need to monitor the EM environment and to detect the intentional jamming situation and develop resilient architecture since more and more critical domains use wireless communication.

CONTACTS:

UIC Security Division: Marie-Hélène Bonneau, bonneau@uic.org

UIC Communications Department: Florence Albert, albert@uic.org; com@uic.org