European Commission

SECRET Report Summary

Project reference: 285136
Funded under: FP7-SECURITY

Periodic Report Summary 1 - SECRET (SECurity of Railways against Electromagnetic aTtacks)

Project Context and Objectives:
SECRET project aims to study the impact of EM attacks on the European rail network and provide solutions to strengthen the resilience of the rail system against such attacks.
This project is directly related to the context of the deployment of ERTMS (European Railway Traffic Management System) over the European railway network. Indeed, the ERTMS is notably based on the deployments of the GSM-R communication system and ETCS (European Train Control System) in order to homogenize the communication, signaling and train control solutions inside the European territory. However, this homogeneity of the technologies employed in Europe also conducts to the homogenization of the vulnerability points to the EM interferences.

Thus, when a malicious person has a intentional EM emissions device capable of disrupting the rail network in Berlin, for instance, the same device will have the same attack capacity in all European cities. This will cause at least immediate economic consequences and possibly more.... Harmonization thus facilitates the implementation of organized and simultaneous EM attacks. Our project notably aims to complete the harmonization solution to ensure its resilience and robustness against EM attacks.

Meanwhile, the technologies and frequencies employed in the railway field are similar to technologies and frequencies used for applications available to the general public. Indeed, the railway no longer develops technology "owners" but adapts general public technologies. That increases the vulnerability of the railway because it is easy to obtain emission devices capable of disrupting rail technologies. With relatively basic electronics knowledge and the performance of electronic components and antennas available on the open market, these emission devices can be combined with amplifiers to increase the capacity of EM attacks.

Knowing that today the state of deployment of ERTMS is not the same in the different European country and the European rail system is still very diverse in terms of supporting technologies and knowing that its EM vulnerability is directly depending on the technologies involved, the consortium decided to prioritize the work on the technologies expected within ERTMS level 2 and SECRET consortium aims to provide recommendations for strengthening the ERTMS security aspects.
The methodology followed in the project to extract available recommendations is composed of 4 main activities.

The threat assessment and risk analysis: the project's first objective is to conduct a systemic analysis of the management of a railway network to identify the different scenarios, which may occur in the case of an EM attack and evaluate its consequences. In parallel, a list of potential EM attacks equipment available in the public domain is established. A lot of effort are also involved in the implementation of demonstration EM attacks and produce a clear and quantified vision of the threats and risks in the case of an EM attack on the railway network. Preventive and recovery measures at a systemic level have to be identified.
Technical protection: the issue of protection of railway wireless systems is addressed in order to ensure the resilience of the railway infrastructure regarding EM attacks. The project then aims at a global EM protection solution consisting of monitoring the EM environment to detect and characterize EM attacks, adopting redundancy and complementarity in information transmission links and finally a dynamic protection permitting the selection of robust transmission links relative to the characteristics of the EM attack, thus providing resiliency quality to the whole infrastructure
Recommendations for a resilient railway infrastructure: Finally, in order to optimize the contribution of this project to a secure and harmonized European railway network, a WP is focused on recommendations and guidelines for policy makers, operators and the rail industry and will contribute to improving European standardization.

Project Results:
Knowing that the EM possible attack scenarios are endless, during this first year is was necessary to define the limits of the scenarios considered in SECRET. To establish these limits, we proceeded on the assumption that there are three main classes of EM attacks EM:

• the EM attacks which aims to permanently disrupt electronic equipment,

• the EM attacks which aims to modify the transmitted information in order to send false information to the components of the railway systems and
• the EM attacks which aims to jam the transmitted information between the railway components in order to confuse the system and to affect its capability.
The first type of EM attack requires a relatively high power level and wide band EM attacks signals. This means that criminals must obtain and use bulky equipment.
The second case of EM attacks requires a high level of knowledge of the railway components and specific railway equipment which are difficult to obtain.
Nevertheless, the last type of EM attacks is relatively easy to implement with devices available to general public and the consortium decided to focus its work on this last type of EM attacks. In consequences, the potential victim systems considered are the wireless systems employed in the railway domains and with can be seriously confused or disrupted in case of jamming of transmissions.

From the established limits, the WP1 partners have conducted research on the definition of scenarios to consider and how to jointly conduct a risk analysis on the technological characteristics of the railway system and an assessment of the threat that would permit to classify the EM attack among all threats to the rail system.

Indeed, the partners came to the conclusion that the risk analysis (bow-tie approach) was essential to identify the multiple consequences that could emerge in case of attack EM and identify technological solutions to make but it was also essential to conduct an assessment of the threat (Generic Threat Matrix methodology) in order to qualify the EM attacks for policy makers.

On the other hand, given the sensitivity of some information in some attack scenarios, a scenario "use case" containing no sensitive information has also been defined to test the various technological solutions envisaged in the project and to make presentations the work to the whole consortium and outside the consortium meetings.

Another important facet of SECRET is the driving of tests in laboratory, station or train. Various tests were carried out during the first year with different purposes. Laboratory tests were designed to characterize the signals produced by some jamming devices or to quantify the vulnerability of some receivers used in the middle rail (WP1). Measurement were also performed in train station, in train (inside IRIS 320) and along the track in order to collect a large number of railway EM environment characterisation and to extract model of normal operating conditions (WP3). These models will then permits to detect attack situation.

Figure 1 Electric field measurement using the conical dipole in Paris, gare de l'Est and along LGV Est

Measurements were also performed on train in order to measure the potential coupling between the potential victim equipment on board train and an attack device inside the train of on the track side (WP2). Finally, a preliminary dynamic protection solution combining resilient communication architecture with a resilient health and attack management subsystem was proposed (WP4).
Currently discussions are in progress in order to test specific and relevant EM attack scenarios on railway communication components (GSM-R and TETRA).

Potential Impact:
Today, many actors in the railway world are facing technical difficulties accompanying the deployment of ERTMS and many specifications should be regularly established or strengthened to ensure the safety of the rail network. SECRET project aims to support all the works underway to also introduce enhanced solutions from a security point of view. In this objective we must first fully assess the risks and communicating them adequate. The project has already identified specific risks and we must now find a way to communicate in a secure manner with the players in the railway. In this context, the Security platform of the UIC will organize relationships with some of its members in order to control the process of diffusion of this potentially sensitive information.

Today, thanks to the different experimentations which was performed on the trains, on some attack devices and on the railway network, we have all the required information to assess how an attack device can reach certain potential victim railway equipment. We now have to perform vulnerability test in laboratory on these equipment in order to conclude the level of disturbing that the attack devices can involve on the victims equipment and to identify the solutions to strengthen these equipment.

The project also aims to provide practical technological solutions to support ERTMS towards resilience vis-à-vis the electromagnetic attacks. In this context, various studies conducted to propose solutions and detection of attacks to strengthen communication links will be sheets of "recommendations" that will be communicated to the UIC, ERA and UNISIG. Preliminary versions of these sheets will probably be published in October 2013 to engage exchange with key stakeholders.

List of Websites:
www.secret-project.eu

Related information

Result In Brief	Improving railway security

Contact

LAPORTE, Stéphane (In charge of contract)
Tel.: +33 1 81 66 86 71
Fax: +33 1 81 66 80 01
E-mail

Subjects

Information and communication technology applications - Security

Information source: SESAM

Last updated on 2014-11-13
Retrieved on 2016-07-07

Permalink: http://cordis.europa.eu/result/rcn/149411_en.html