SECRET : SECurity of the Railway network against Electromagnetic ATtacks

Virginie Deniau, Philippe Massy, Antonio Kung, Renaud Comte, Marie-Hélène Bonneau

European Railway Review Volume 21, Issue 1, February 2015

SECRET : SECurity of the Railway network against Electromagnetic ATtacks

Virginie Deniau, Philippe Massy, Antonio Kung, Renaud Comte, Marie-Hélène Bonneau

The European railway network is in significant evolution with the deployment of ERTMS. In particular, the level 2 of ERTMS which is based on the transmission of the signaling information through the GSMR network mobilizes all the railway stakeholders to maintain an optimal security level.

Due to the increasing terrorism threat, various aspects and in particular electromagnetic attacks need to be taken into account. The harmonisation of the European railway network results in a harmonized electromagnetic vulnerability which need to be addressed at European level and especially the resilience of ERTMS against potential malicious actions which could be implemented in order to disturb the railway network. Knowing that some information will be transmitted via wireless solutions, the issue of the Intentional ElectroMagnetic Interferences (IEMI) naturally occurs.

The European project SECRET co-funded by the European Commission within the FP7 program was then initiated in order to study the potential impact of such interferences and to implement solutions to avoid any disruption.
SECRET consortium involves 10 partners from 5 European countries. The project is coordinated by IFSTTAR which is the French institute of science and technology for transport, development and network.

Figure 1 ï The SECRET Consortium

The project SECRET assesses the risks and consequences of EM attacks on the rail infrastructure, works on preventive and recovery measures and develops protection solutions to reinforce the security of the rail network, subject to intentional electromagnetic (EM) interferences, which can disturb command-control, communication or signalling systems.

During this project, several scenarios were studied in order to identify the potential vulnerable situations. Regarding the interferences considered in this project, we did not identify direct potential dangerous situations for the persons. However, such interferences can impact seriously the good operation of the rail and the capacity of the network.

The project is then oriented in four major contributions.

The first contribution is oriented on the definition and realization of susceptibility tests performed on specific railway components in presence of interferences corresponding to specific intentional interferences. This work is linked with an issue larger than the railway domain. Indeed, the International Electrotechnical Commission (IEC) Subcommittee (SB) 77C works on the standards to protect civil systems against man-made high power electromagnetic threats. Initially, this subcommittee considered mainly very high power electromagnetic threats and progressively the definition of the considered intentional interferences evolved. Indeed, with the proliferation of the emission devices accessible to general public and with the deployment of the application ensured by wireless communication technologies, the threat is in permanent evolution. The test methodologies developed in SECRET and the definition of the EM attack signal were then discussed with members of IEC SC77C in order to contribute to the evolution of the international standardisation concerning the civil infrastructure.

The second contribution is focused on the research of solutions to detect the presence of IEMI. Indeed, in the case that IEMI would be generated in the space dedicated to the railway network, the priority is to diagnosis the situation. The detection can permit us to involve an adequate countermeasure and to not confuse an attack with a technical failing. Different detection methods were studied in order to identify what can be the more efficient solutions according to the context (on board train, along the track or in railway station).

A first detection approach is based on the analysis of the spectrum occupation to distinguish ñnormalò distributions, corresponding to the absence of attack signal, from ñabnormalò distributions corresponding to the presence of attack signal in the spectrum. For this spectrum distribution approach, two different methodologies were studied: the supervised detection or the attack signal classification. The supervised detection consists in learning and modelling the ñnormalò environment. In that case, the detection application consists in recognizing an environment which does not belong to the ñnormalityò
The attack signal classification method consists in learning the environment in presence of different attack devices and to extract distribution models for each device. In that case, the detection consists in comparing the environment with the different models and to recognize the presence of one of the models. In SECRET, measurements were performed in different situations (on board train, along track and in train stations) in order to define the laws corresponding to all these ñnormalò situations. In parallel, different attack devices were characterized and modelled, optimizing the model definition in order to facilitate the detection without being affected by over fitting. The spectrum approach can allow monitoring several communication systems in adapting the frequency bands monitored and in using adequate antennas.

Another detection approach is based on the in phase and quadratic (IQ) data received by the GSM-R terminal and consists in analysing the GMSK IQ constellation with and without attack signal. The Error Vector Magnitude (EVM) which corresponds to the sum of the errors on the sample positions is calculated for each GSM-R time slot. The values reached by the EVM and the evolution of these values over the time permits to efficiently detect the presence of IEMI. We noticed that the variation of the EVM is really significant in presence of attack signal even if the power of the attack signal is 20 dB lower than the GSM-R signal. Then, the jamming signal could be detected even if the communication is not affected and the reaction to have could be anticipated.

The third contribution of the project consists in designing an ICT communication architecture resilient to EM attacks. It integrates a detection system (DS), a redundant multipath communication system (MCS), and a management capability in charge of acting upon attack. The DS detects in real-time EM attacks and to be able to take over manual or automatic actions to overcome them. The MCS can harden for instance an ETCS (European Train

Control System) communication between the RBC (Radio Block Centre) and the train using multiple paths simultaneously. The management system consists of distributed components called health attack managers (HAMs): a central HAM located at the command center level, HAMs at the track level and HAMs at the train level.

The architecture is specified to take into account configuration flexibility requirements and interoperability requirements. Different configurations are possible: DS only, MCS only, DS and MCS together. Interoperability interfaces are defined, e.g. between a central HAM and a HAM, between a HAM and an MCS. Examples of configurations could be the following: an ETCS solution over a non IP based communication, with a DS at the track level; an ETCS solution over an IP based communication (e.g. GPRS-R, WiMAX, LTE, Tetra) with one of the three options (DS only, MCS only, DS and MCS together).

The architecture was evaluated with a modelling and simulation tool with different scenarios of attacks. Examples of parameters were attack position, train position, strength and duration of attack. Simulation showed that under different conditions and scenarios the railway communication is resilient against EM attacks. For practical reasons the architecture will be demonstrated through a different use case: a railways worker will have an alert equipment on himself (inside his coat) which is connected through Bluetooth to his GSM mobile. Upon attack detection, an alert is sent from the detecting equipment to the mobile. The mobile connects to the control centre to inform that there is an attack.

During the architecture specification work, it was realised that the use of different risk analysis methods and tools created a terminology problem. For instance the concept of threat was different in each method. Consequently an unification work is being carried out. It is based on ontologies and can lead in the future to automatic generation of rules to be used by health attack managers.

The fourth action is about the dissemination of the project results to key players and contributing to the improvement of standardisation. Because the project wants to make the whole railway community hoarding on its outcomes, contributions to Technical Recommendations (TecRec) will be proposed in link with the UNISIG/UNIFE normalization process. Meanwhile, fearing the TecRec process duration, a parallel activity consists in porting those outcomes to more specialized normalization commitees, as well at hardware level with committes like CENELEC (European Committee for Electrotechnical Standardization), CEN (European Committee for Standardization, except electrotechnical and telecom) or ETSI (European Telecommunications Standards Institute) with providing some EMC recommendations but also at system level like UNISIG with discussing more resilient architectures.

Cyber threats are an increasing concern for every business. Barely a week goes by without new reports of sophisticated IT systems ï even of the largest organisations or intelligence services ï falling victim to cyber attacks. It was therefore important to check what further precautions could be taken within the railway sector should the need arise. The SECRET project addresses this issue for electro-magnetic attacks targeting infrastructure and will then contribute to reinforce the signalling systems.