SECRET
SECurity of Railways against Electromagnetic aTtacks

Grant Agreement number: 285136
Funding Scheme: Collaborative project
Start date of the contract: 01/08/2012
Project website address: http://www.secret-project.eu

Deliverable D 5.3

Proposal for TecRec on static hardening rules

Submission date: October 2015

Document details:

Title	Proposal for TecRec on static hardening rules
Work package	WP5
Date	25/10/2015
Author(s)	
Responsible Partner	POLITO
Document Code	SEC- ? 20130227 - ?
Version	A2
Status	Draft

Dissemination level:

Project co-funded by the European Commission within the Seventh Framework Programme

PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission) Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Document history:

Revision	Date	Authors	Description
A1	12/10/2015	POLITO	Draft
A2	25/10/2015	POLITO	Draft
A3	21/12/2015	POLITO	Draft

Table of content

1. Executive summary

A largest part of WP5 involves carrying out Technical Recommendations (TecRec) based on the results of the different WPs. Developed on WP1 and WP2, these analyses were used for the establishment of TecRec on preventive and recovery measures and on static hardening rules.

This deliverable represents the task 5.3 of the project. Based on the results of WP2, and based on the analysis of standards, this TecRec will specify the rules to be applied in the design (including the test phase), certification and deployment, up to the intervention during the maintenance and modification phases of critical equipment.

An annex file is added to this document, this annex represents the template of the recommendation in excel file.

2. Introduction

2.1. Purpose of the document

The purpose of this document is to provide technical recommendations from the susceptibility analysis of the railways infrastructure devices to a potential attack. These recommendations will define hardening rules aimed at increasing the network immunity.

Related to the results of WP2 and the consortium discussions we can investigate some rules to prevent from the effect of electromagnetic waves coupling to the infrastructure and rolling stock devices.

We propose in this deliverable recommendations to minimize the interference effects and identify disturbances.

2.2. Definitions and acronyms

Acronym	Meaning
BTS	Base station
dB	Logarithmic unit used to express the ratio between two values of a physical quantity
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSM GSM-T	Global System for Mobile Communications
H	High
IEMI	Intentional ElectroMagnetic Interference
Jammer	High impact IEMI attacker device
L	Low
M	Medium
Mfg Mfgs	Manufacturer (s)
MS	Mobile station
Rf	Radio frequency
S/N	Signal to Noise
Tbd	To be defined
Tlc	Telecommunication
Uplink	The MS to BTS channels
WiFi, Wi-Fi	Wireless local area network

3. Summary of potential victim systems

In the context of the railway domain, the EM attacks to consider can be classified in 3 types:

- the EM attacks which aims to affect and 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 potential victim systems considered are the wireless systems employed in the railway domains, that can be seriously confused or disrupted in case of jamming of transmissions. The potential “victim systems” considered are the GSM-R system, the TETRA system, the Eurobalise and the GPS.

Deliverable D1.1 (CO) contains the details of the analysis carried out; the following is a short summary of the characteristics of all potential victims, to be used as a reference for the recommendations of Sect. 4.

3.1. The GSM-R system

GSM-R is part of the ERTMS/ETCS standard associated with Eurobalise and Euroloop. GSM-R carries part of the signalling information directly to the train on board signalling unit. It constitutes a continuous communication system between trains and infrastructure, thanks to the existence of a set of base stations deployed along the railway tracks.

The system operates on frequency bands close to the public GSM system which are the frequency bands 876-880 MHz for the uplink (from trains to base stations) and 921-925 MHz for the downlink (from base stations to trains). Frequency spacing between each physical channel is 200 kHz.

The power receiving signal on–board train depends on the distance between the train and the base station. Measurements performed along a train displacement have shown that the power of the reception signal has a large dynamics (generally on the order of 70 dBm).

The coverage level to verify is defined as the field strength at the antenna on the roof of a train (nominally a height of 4m above the track). The reference values are given for an isotropic antenna with a gain of 0dBi.

3.2. Eurobalise

Eurobalise is a spot communication system, taking part in the ERTMS/ETCS system. It is a beacon fixed on the floor between the tracks and it transmits to the trains route data at fixed points.

The beacon is tele-powered by a 27.115 MHz radio frequency signal generated by

trains. The trains are equipped with a loop antenna and generate continuously a RF signal at 27.115 MHz. When the train passes above the balise, the balise is activated thanks to the inductive coupling and sends back to the train its position or specific signalling information. The modulation of the Up-link signal, from the balise to the train is a frequency shift keying (FSK) with a 4.234 MHz center frequency.

The time duration of communication between the track side Eurobalise and the on board BTM is relatively short but should permit to transmit telegrams for both Up-link and Down-link at a maximum vehicle speed of 500 km/h. The end of transmission between the on track balise and the train is located at 1.3 m from the center of the balise.

3.3. TETRA

TETRA (Trans European Trunked Radio) is an ETSI standard of a second generation digital cellular network developed for professional mobile radio solution. It is not limited to railway domain but it was designed for use by government agencies, emergency services (police, fire departments, ambulance) for public safety networks, public transportation services and the military. TETRA offers a High security level of the transmissions thanks to an end to end encryption and is developed in accordance with the current requirements for Interoperability and multi-provider situations.

In terms of services, TETRA permits to establish point-to-point or point-to-multipoint communications and to transmit emergency signals to the dispatcher, overriding any other activity taking place at the same time. TETRA allows the transmission of voice exchanges and data, but with a relatively low data rate up to 7.2 kbps. The frequency bands allocated to TETRA are in the 400 MHz band.

3.4. GPS

Some railways use GPS (Global Positioning System) mainly to non-safety applications. The applications can be information to passengers or to fleet supervision by monitoring in real time the movement of locomotives, wagons, maintenance of railway vehicles and track equipment. Sometimes combined with other sensors, computers and communication systems, GPS can improve the operational efficiency of rail. However, in the future, GPS could be used for the next generation of European Rail Traffic Management System (ERTMS) by enhancing odometry.

All satellites broadcast at the same two frequencies, 1.57542 GHz (L1 signal) and 1.2276 GHz (L2 signal). The satellite network uses a CDMA spread-spectrum technique.

4. Topologic solutions to strengthen the radio links

4.1. GSM-R

The following table shows a list of actions aimed at the improvement of GSM-R communications, their supposed cost, effect and applicability

N	Action	Cost	Effect	Applicability	Gain	Involved Bodies
1	Increase the antenna ground plane	L	L	Easy	3-6 dB	Mfgs
2	Lower the antenna profile	L	L	Easy	3-6 dB	Mfgs
3	Use double shielded cabling	L	L	Easy	3 dB	Mfgs
4	Cure fringings and refractive bodies	L	L	Easy	3 dB	Mfgs
5	Rf absorbers below the cab roof	L	L	Easy	3-6 dB	Mfgs
6	Seam welding / roof tight riveting	M	M	Easy	Up to 10 dB	Mfgs
7	Vent holes wrongly sized (if case)	L	M	Easy	Up to 10 dB	Mfgs
8	Place long-range antennas (BTS)	M	M	Medium	TBD	Mfgs / Tlc op.

4.2. TETRA

The following table shows a list of actions aimed at the improvement of TETRA communications, their supposed cost, effect and applicability

N	Action	Cost	Effect	Applicab	Gain	Involved Bodies
1	Increase Tx power (Bts and/or MS)	M	L	Medium	3-6 dB	Mfgs / User
2	Increase the number of BTS	H	H	Difficult	Up to 20dB	Tlc operators
3	Narrow beam antennas on BTS	M	M	Medium	TBD	Mfgs / Tlc op.

4.3. GPS

The following table shows a list of actions aimed at the improvement of GPS communications, their supposed cost, effect and applicability

N	Action	Cost	Effect	Applicab	Gain	Involved Bodies
1	Enlarge antenna' s ground plane	L	L	Easy	3-6 dB	Mfgs
2	Lower the antenna profile	L	L	Easy	3-6 dB	Mfgs
3	Use double shielded cabling	L	L	Easy	3 dB	Mfgs
4	Seam welding / roof tight riveting	M	M	Easy	Up to 10 dB	Mfgs
5	Rf absorbers below the cab roof	L	L	Easy	3-6 dB	Mfgs
6	Place steerable antennas	L	H	Easy	Up to 20 dB	Mfgs / User
7	One antenna on each train ends	L	M	Easy	Up to 10 dB	Mfgs / User
8	Vent holes wrongly sized (if case)	L	M	Easy	Up to 10 dB	Mfgs

4.4. EUROBALISE

The following table shows a list of actions aimed at the improvement of Balise communications, their supposed cost, effect and applicability

N	Action	Cost	Effect	Applicability	Involved Bodies
1	Add an RF sensor of alien signals	L	H	Easy	Mfgs
2	Add a capacitive detector to sense bodies that could de-tune the antenna	L	M	Easy	Mfgs

4.5. Additional susceptibility tests on communication equipment

We concluded in D2.2 and D2.3 that up to now standardization is not taking into account those IEMI interferences in the product standards, even if the basic standards developed by IEC TC 77C are beginning to consider jamming.
Nevertheless, we encourage manufacturers to add additional susceptibility tests on their communications subsystems (GSM-R, Tetra, Eurobalise, but also LTE and new technologies).
Even if those tests are not taken into account in the standardization, it could be really helpful to compare the performances of these electronic communication subsystems regarding those attacks. The susceptibility tests (conducted and radiated) we have performed during this project, e.g. on GSM-R show that a performance criterion based on RXQual could be a good choice as in ETSI standard EN 301 489-7 for GSM.

5. Technical recommendations for WP2

5.1. Secret_WP3_TecRec_017

5.1.1. Definition

This technical recommendation implies the introduction of TecRec to minimize/avoid the effect of jamming coming from lower direction with respect to the horizontal line. GSM-R antennas are generally located on the roof of train for communication with BTS that are located at higher levels; this means that the communication takes place in the half space above a theoretical horizontal plane defined from the train roof. On the other hand, possible jamming signals come from inside the train or from an attacker on ground; this means that the propagation between the jammer and the train antenna is confined between the ground and the theoretical horizontal plane above the train roof. If part of this theoretical plane around the antenna base is made conductive, the unwanted jamming signal will be shielded by the plane itself.

Topic	Enlarge the ground plane below the train' s antenna and/or reduce the antenna profile
Description	The antenna should reject all signals coming from the bottom.
Type	Engineering rules
Involved bodies	Railway industry and operators

5.1.2. Technical requirements

The larger is the reflector plane of the antenna, the more efficient is the antenna reception from the half space above the plane. In fact, a larger plane improves the image effect of the half dipole constituting the antenna. Technically speaking, the dimension of the reflector plane must have a minimum size to start to be effective: an edge length equal to the wavelength corresponding to the functional frequency of the antenna is the minimum theoretical size. As an example, for a GSM band around 900 MHz, the propagation wavelength in air is around 35 cm.

To be effective, the enlargement of the reflector plane should reach between the double and triple of the critical wavelength. For the above example, is therefore advisable to adopt reflector planes with a dimension of approx. 1 sq. meter.

The suggested provision is also indicated for the protection of transmission systems like TETRA and GPS, although the practical realization may be more difficult than for the protection of GSM communication. Finally, the suggested provision is not applicable for the Eurobalises protection, due to the different operation principles, frequency and location of such devices.

5.2. Secret_WP3_TecRec_018

5.2.1. Definition

This technical recommendation implies the introduction of TecRec to minimize/avoid the effect of jamming on sensitive reception devices. GSM-R receivers are generally located inside the train body, in particular inside the locomotor below the roof antenna. Since jamming signals may directly interfere with the receiver, one should take care that the interfering power is attenuated before reaching the device. Of course, a shield can be fitted around the receiver; otherwise one can exploit the properties of the metal body of the locomotor and its internal separation walls to create chambers decoupled with respect to the external electromagnetic field. However, as well known from shielding theory, a shield is effective if the metallic continuity of all walls of the enclosure is assured; in fact, any openings of a size comparable with the wavelength of the external field re-radiates the external field inside the enclosure, thus strongly reducing the electromagnetic protection.

Topic	Improve the shielding effect of the locomotive body assuring electrical continuity to the locomotive roof, if metallic, or applying Rf absorbing material to non-metallic roofs
Description	Shielding is never total : this helps reducing the signal level
Type	Engineering rules
Involved bodies	Railway industry and operators

5.2.2. Technical requirements

To be effective as a shield, the enclosure must realize a metal box, inside which the receivers of possibly jammed signals are located. Metal parts must be welded together continuously or at least with welding points spaced of a distance much shorter than the interfering wavelength. As an example, for a GSM band around 900 MHz, the propagation wavelength in air is around 35; this implies that welding points or screws are separated by not more 10 cm apart (5 cm would be optimal).

The suggested provision is also indicated for the protection of transmission systems like TETRA and GPS. Finally, the suggested provision is not applicable for the Eurobalises protection, due to the different operation principles, frequency and location of such devices.

5.3. Secret_WP3_TecRec_019

5.3.1. Definition

This technical recommendation implies the introduction of TecRec to minimize/avoid the effect of jamming on sensitive reception devices. GSM-R signals propagate inside the train from the roof antenna to the receiver guided by coaxial cables. Coaxial cable is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. High-quality cables usually use double-shield construction in which one shield is a braid and the other is a thin, coated aluminum foil underneath the braid. External fields create a voltage across the inductance of the outside of the outer conductor. Grounding the second shield, the triaxial structure provides a greater rejection of interference than coax.

Topic	Use Rf double-shielded coaxial cables
Description	Shielding effectiveness of coaxial cables is not absolute; : interferences can leak through the locomotive body to the wiring
Type	Engineering rules
Involved bodies	Railway industry and operators

5.3.2. Technical requirements

Transfer impedance is the quantity most commonly used to describe shield effectiveness. In a receiving system, such as a radio link of interest for railways applications, the disturbed circuit is that of the coaxial cable transmission line and the disturbance comes from the electrical environment surrounding the cable. A cable shield with lower transfer impedance is better than one with higher transfer impedance – that is, a given disturbing current causes a smaller voltage disturbance in a cable with low transfer impedance than a cable with high transfer impedance. In addition, the terminal connector of a coax cable is critical for maintaining the high level of shielding; in fact, if a good electrical contact is not assured along the entire circumference of the cable, the shielding properties are highly degraded. Specific recommendations for systems assembly and maintenance are needed.

The suggested provision is also indicated for the protection of transmission systems like TETRA and GPS, although the practical realization may be more difficult than for the protection of GSM communication. Finally, the suggested provision is not applicable for the Eurobalises protection, due to the different operation principles, frequency and location of such devices.

5.4. Secret_WP3_TecRec_020

5.4.1. Definition

This technical recommendation implies the introduction of TecRec to minimize/avoid the effect of jamming on sensitive reception devices. GSM-R receivers are generally located inside the train body, in particular inside the locomotor below the roof antenna. Since jamming signals may directly interfere with the receiver, one should take care that the interfering power is attenuated before reaching the device. Metal shields are used for this purpose (in some cases, it can be whole metal body of the locomotor and its internal separation walls) to create chambers decoupled with respect to the external electromagnetic field. However, the shielding enclosure cannot have solid walls, since ventilation, exchange of signals through cables, sight and displays require holes in the walls. Such holes, may reduce the shielding effectiveness of the enclosure to small values, if appropriate design precautions are neglected.

Topic	Check if the locomotive vent holes are rightly sized Vs the radio-frequencies in use
Description	Slotted ventilation holes opened in metallic sheets can behave as antennas resonating to specific frequencies. In such cases they can relay signals
Type	Engineering rules
Involved bodies	Railway industry and operators

5.4.2. Technical requirements

The size of the holes influences the propagation of the disturbances across the walls: the larger is the hole size (almost irrespective of the shape), the less effective is the cavity in suppressing the electromagnetic noise,

To be effective as a shield, the enclosure must realize a metal box, inside which the receivers of possibly jammed signals are located. Ventilation holes, holes for cables, possible panels with displays need to have their largest dimension much shorter than the interfering wavelength, so that the external field reaching the aperture does not resonate and hence does not re-radiate toward the interior of the cavity.

As an example, for a GSM band around 900 MHz, the wavelength in air is around 35 cm; this implies that the largest size of holes must be confined below this value. If a large aperture is necessary (for example, for ventilation), it is advisable to implement as a number of (circular) holes, since the performance degradation is only proportional to the square root of the number of holes.

The suggested provision is also indicated for the protection of transmission systems like TETRA and GPS, although the practical realization may be more difficult than for the protection of GSM communication. Finally, the suggested provision is not applicable for the Eurobalises protection, due to the different operation principles, frequency and location of such devices.

5.5. Secret_WP3_TecRec_021

5.5.1. Definition

This technical recommendation implies the introduction of TecRec to minimize/avoid the effect of jamming coming from a location different from the train position. For a radio link, a narrow beam allows the flexibility of restricting as much as possible the communication between two devices, with the advantage that other signals or interferences coming from directions other than the direct line of sight between the two devices are strongly attenuated, because they fall on the edge of the main lobe or on side lobes, usually having small gain. Generally, squeezing the lobe in one direction has the effect of increasing the gain, thus increasing the performance of the communication link; on the other hand, a narrow beam in the context of railways communications requires a steering functionality, since the BTS must always point to the moving train.

Topic	Install very-narrow-beam antennas on BTS
Description	Meant to improve the system S/N
Type	Engineering rules
Involved bodies	TLC operators

5.5.2. Technical requirements

For a BTS receiving antenna, a narrow beam (with an electronic steering that maintains the beam always pointing to the train) will receive the communication from the moving train with high efficiency (due to higher gain reachable by narrowing the beam); all other spurious signals or interferences (like the possible case of a jamming generated on ground in the vicinity of the BTS) will come to the antenna with an angle for which the main lobe has a small gain or will intercept the side lobes of the antenna, having certainly very low gain. For a BTS transmitting antenna, a narrow beam (with an electronic steering that maintains the beam always pointing to the train) will communicate with the moving train with high power density (due to higher gain reachable by narrowing the beam); all other spurious signals or interferences (like the possible case of a jamming generated onboard the train or on the ground in the vicinity of the train) will most likely be overcome by the larger power directed by the BTS. This will increase the probability that the communication is not disrupted by the jamming.

The suggested provision is also indicated for the protection of transmission systems like TETRA and GPS, although the practical realization may be more difficult than for the protection of GSM communication. Finally, the suggested provision is not applicable for the Eurobalises protection, due to the different operation principles, frequency and location of such devices.

6. CONCLUSIONS

Based on the results provided by the different deliverables for jamming detection in WP1 and WP2, we were able to develop and propose some recommendations to avoid and minimize the impact of jamming on the system, and for the improvement of the network.

Starting from the preliminary analysis carried out in the initial phase of the project, we developed these TecRec and evaluated their practical implementation. At this level the recommendations proposed are feasible and seem to be efficient.