SECRET
PROJECT

SECURITY OF RAILWAYS AGAINST
ELECTROMAGNETIC ATTACKS

WHITE PAPER

Security of railways against electromagnetic attacks

November 2015

ACRONYMS

BTS	Base Transceiver Station
CENELEC	European Committee for Electrotechnical Standardization
EIRENE	European Integrated Railway Radio Enhanced Network
EM	ElectroMagnetic
EMF	ElectroMagnetic Fields
ETSI	European Telecommunications Standards Institute
EVM	Error Vector Magnitude
GSM	Global System for Mobile communications
GSM-R	Global System for Mobile communications - Railways
HSL	High Speed Line
IEM	Intentional ElectroMagnetic
I/Q	In-phase/Quadrature
LGV	Ligne à Grande Vitesse (High Speed Line - HSL)
MiMo	Multiple-input Multiple-output
MS	Mobile Station
ONF	Organization Normative Framework
PSD	Power Spectral Density
QoS	Quality of Service
RBC	Radio Block Centre
RF	Radio Frequency
SJR	Signal to Jamming Ratio
SR	Staff Responsible
TGV	Train à Grande Vitesse (High Speed Train – HST)
TVRA	Threat Vulnerability Risk Assessment

STANDARD REFERENCES

EMC

> Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility EMC) standard for radio equipment and services; Part 1: Common technical requirements: **ETSI EN 301 489-1**

> Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 23: Specific conditions for IMT-2000

> CDMA, Direct Spread (UTRA and E-UTRA) Base Station (BS) radio, repeater and ancillary

> equipment: **ETSI EN 301 489-23**

Radio

> Global System for Mobile communications (GSM); Harmonized EN for Base Station equipment covering the essential requirements of article 3.2 of the R&TTE Directive: **ETSI EN 301 502.**

> Global System for Mobile communications (GSM); Part 4: Harmonized EN for GSM Repeaters covering the essential requirements of article 3.2 of the R&TTE Directive: **ETSI EN 300 609-4.**

> Electromagnetic compatibility and Radio Spectrum Matters (ERM) – Electromagnetic Compatibility (EMC) standard for radio equipment and services – Part 1: Common technical requirements: **ETSI EN 301 489-1**

> Specific conditions for mobile and portable radio and ancillary equipment of digital cellular radio telecommunications systems (GSM and DCS) : **ETSI EN 301 489-7 Part 7.**

> Specific conditions for GSM base stations: **ETSI EN 301 489-8 Part 8.**

> Specific conditions for Terrestrial Trunked Radio (TETRA) equipment: **ETSI EN 301 489-18 Part 18.**

978-2-7461-2465-3 - © SECRET Consortium Member – 2015

CONTENT

INTRODUCTION

Cyber threats are an increasing concern for every business. Barely a week goes by without new reports of sophisticated IT systems – even of the largest organisations or intelligence services – 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 EU project addresses the issue of electro-magnetic attacks targeting rail infrastructure and contributes to reinforce the signalling systems. The electro-magnetic attacks considered in SECRET are low power intentional interferences that can break the communication links and affect voice communication and the good transmission of signalling information.

The SECRET consortium and its 10 members came together to assess the risks and consequences of electromagnetic (EM) 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.

SECRET approach

The project illustrated the risk by implementing some 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.

Then, the project opened 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, the project identified and proposed strategies in which each actor would be able to inspire itself in order to act towards resilience.

The strategies developed 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 means 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.

Target group for the project

The project main targets are:

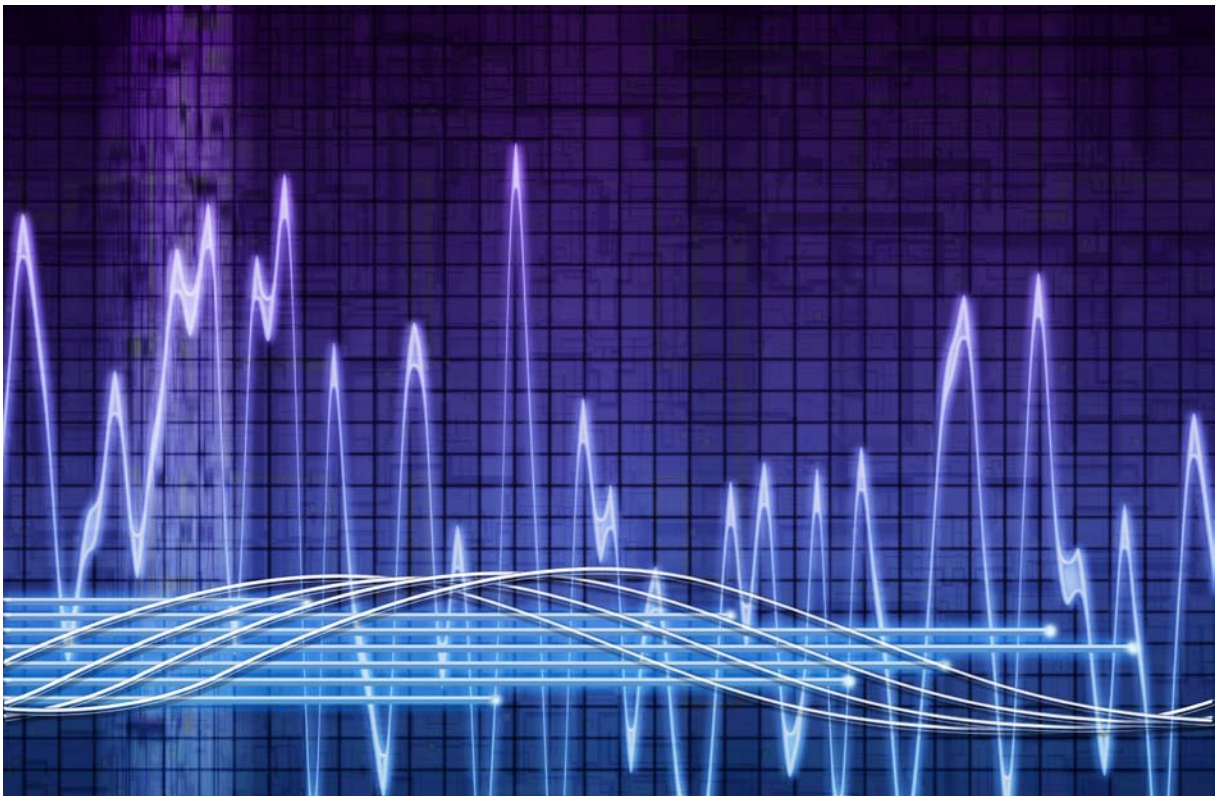
- Rail manufacturers,
- Rail operators,
- Rail Infrastructure Manager,
- Standardization Bodies,
- Telecommunication network actors,
- Other critical infrastructure (involving wireless communications) managers.

SECRET results

These results are summarized in the present document, so-called white paper.

About 40 recommendations at organisation, standardization and technical levels, have been identified, classified and described. These recommendations are organised in three categories:

- The first category called "**prevention from EM jamming effects**" groups the recommendations which can be adopted permanently and can permit to inhibit or reduce the impact of jamming signal (precautionary principle).
- The second recommendation category is dedicated to the **EM attack detection** solution. It presents the different detection technics which were studied in SECRET and presents their potential applications.
- The third category is "**Mitigation of EM jamming effect**". In this category, the recommendations are focused on solutions which can be activated temporally in situation of EM jamming. These recommendations are then conditioned by the existence of an attack detection solution.



1. PREVENTION FROM EM JAMMING EFFECTS

This section highlights recommendations which aim at **increasing the system immunity from potential EM attack.**

1.1 METHODOLOGY RECOMMENDATIONS

1.1.1 Planning security risk assessment study

Planning related emergency response on the railway infrastructure against EM jamming effect is critical. In order to prevent from jamming attacks on the railway environment the first recommendation that can be done is the provision of risk assessments.

The aim is to generate key risk assessment results that can be used for railway security and safety management.

Risk assessment defines whether existing risks are tolerable and risk control measures adequate. It incorporates the risk analysis and risk evaluation phases.

Risk analysis is the process of determining how secure and safe the object or process is, by the following steps:

1. **Scope definition**, hazard identification, and risk estimation;
2. **Risk identification** is the process of determining what can go wrong, why and how;
3. **Risk evaluation** is the process of examining and judging the significance of risk. It must answer the question: how secure and safe the process or object should be. The principal role of risk evaluation in risk assessment is the generation of decision guidance against which the results of risk analysis can be assessed.

This study of risk analysis is based on:

- **Risk assessment**, the overall process of estimating the level of risk of a particular hazard;
- **Hazard**, a source or situation with a potential for harm in terms of damage to the environment, injury or illness, damage to property, or a combination of the above;
- **Incident**, an unplanned event resulting in or having the potential to result in damage to the environment, health, property damage or other loss. An incident can be a single occurrence or a series of occurrences;
- **Risk**, measured in terms of a combination of the consequences of an incident and their likelihood;
- **Likelihood**, the probability of occurrence;
- **Consequence**, the severity of an outcome or incident.

In case of EM jamming, the different factors that impact the system and the risk assessment analysis are the following:

- **Train location**: For the definition of the environment profile, the first entry is the train location. The effect of the jammer on the train can be evaluated depending on its distance from the Base Transmission Station (BTS). This parameter is an important entry for the signal to jamming ratio (SJR);

- **Signal jamming signature;**
- **Jamming power and location**: Depending on the jammer location (on board the train, or outside the train) different situations are analysed with their respective impact on the system;
- **Communication quality**: The purpose of jamming detection and countermeasure is to maintain minimum level of communication quality. To reach this goal, the presence of jammer will have to be detected before the quality of communication becomes very bad or impossible;
- **Line categories**: The different line category need to be evaluated in the railway environments to develop the most adapted countermeasures.

1.1.2 Ensuring Interoperability of Risk Analysis Methods

A common vocabulary on attacks and impact to allow security analysis methodology interoperability must be established.

Multiple risk analysis methods can be used (e.g. risk analysis for EM incident and risk analysis for ICT incident) in a critical infrastructure. These methods are interdependent and must therefore interoperate.

The Bow-tie and TVRA were used in Secret to assess railway incidents and railway communication system incidents. It was realized in discussions with stakeholders familiar with one risk method that they frequently were not aware of the existence of the other method. A study of Bow-tie, TVRA, Cyberprep was then carried out using ontology tools, validating the need for common vocabulary.

1.1.3 Security Analysis in Confidential Settings

An organization scheme best practice must be set up which allows security analyses and keeps attack use cases confidential.

Attack use cases in railway critical infrastructures have to be confidential. Information on such attacks must be restricted to a small number of persons only. Consequently engineers building railway communication systems have to specify countermeasures without such information. An organization best practice must be put in place so that such engineers have access to requirements information instead of attack information. These requirements information can be illustrated by examples of attacks that are not confidential (e.g. description of an ICT WiFi attack instead).

1.1.4 Creating Knowledge Repository based on ISO 27034

A knowledge repository providing updated information on attack, associated measures, and practice must be maintained. It is recommended to follow ISO 27034 (Application security — Organization normative framework).

New attack patterns can be found out in the future. Technology may change (communication, processing architecture). Architecture for resilience may change. Guidelines for architecture resiliency evaluation must be provided.

This type of concern has been addressed in ISO 27034. It defines the concept of Organization Normative Framework (ONF), a knowledge repository consisting of a suite of application security-related policies, procedures, roles and tools.

As stated in ISO 27034, the approach is formal and bureaucratic, e.g. a committee is needed to oversee the ONF. This is most likely to suit organizations which have or want a highly structured way of securing applications they develop.

1.2 OPERATIONAL RECOMMENDATIONS

1.2.1 Minimizing train emergency brake impact

In case of intentional jamming, the main objectives of the offender can be to provoke an emergency braking to stop the train. An emergency brake induces significant consequences on railway traffic and it requires the train re-initialization for operation. Moreover, the train can be stopped in a section where the jamming is still active and no communication is possible with the control centre.

This technical recommendation implies the introduction of measures to minimize/avoid the effect of a train emergency brake when jamming is detected.

When jamming situation is detected both the train driver and control center shall perform necessary actions to avoid or reduce the effect on the infrastructure, by applying national rules.

The system proceeds to the emergency brake differently from one line category to another carrying out different distance apportionment. If train achieves an emergency stop, the signalman shall stop all other trains approaching the danger area according to national rules and inform all drivers as appropriate. The emergency stop order shall not be revoked before the trains are ready to restart. The train shall be immobilized until the signalman decides to revoke the immobilization.

Measures are taken according to the national rules in order to restart the train. This implies traffic arrangements, connection reestablishment, and synchronization...

To restart the signalman shall authorize the driver by means of ETCS Written Order, when:

- *all the conditions for the route are met according to national rules, he can establish in accordance with the national rules that the track is free and provide "additional instructions";*
- *check for speed limitations lower than the maximum speed for SR and include them in the ETCS Written Order 02;*
- *check if other restrictions and / or instructions are necessary and include them in the ETCS Written Order 02.*

According to the previous description, the emergency brake will initiate a special procedure that can imply a lot of time for the system to restart. Furthermore, if train is stopped in areas where no connection is available because of jamming, it seems impossible for the train to get orders from the signalman.

The proposed recommendation tries to avoid such critical situation by giving the train's driver the possibility to route their trains in a safe area not covered by jamming and where connection with signalman can be reestablished.

Consequently, following a jamming detection event, we propose to reduce automatically the train speed and switch the ETCS on-board mode from full supervision to on-sight staff (driver) responsible mode. Such transition does not exist today in the ETCS specification.

This new operational case shall be analysed in safety, as it would assume that the ETCS on-board shall be able to discriminate safely the jamming detection from other events.

1.3 ENGINEERING RECOMMENDATIONS

1.3.1 System Architecture

1.3.1.1 Design and evaluation architecture feature for resilience

An approach to evaluate a resilient architecture is needed, through evaluation methods or simulation, or implementation of use cases.

Because an architecture decision can have a far reaching impact on the system in terms of cost and cybersecurity preparedness, a wide consensus must be reached, i.e. technical and risk managers should be able to agree.

Figure 1: Methodology for evaluation of architecture resilience

The methodology is used by stakeholders who are:

- designing the architecture of a railway communication system. This case takes place when an entire system is designed from scratch;
- designing the additional architecture features of an existing railway communication system that need to address cybersecurity features. This case takes place when a design and architecture is already available.

The methodology includes the following steps as described by Figure 1:

- Step 1: Description of the architecture components. This can focus on the communication systems but also on the computing elements which are handling such systems (for instance the architecture of a controller system in a train);
- Step 2: Integration of the SECRET resilient architecture components (they are described in the next sections);
- Step 3: Evaluation of resulting integration. It is important to assess the cost effectiveness of such integration. We suggest using the ATAM (Architecture Tradeoff Analysis Method) and CBAM (Cost Benefit Analysis Method) methods.

1.3.1.2 Integrating Architecture Features for EM attack detection

Security analysis for railways communication resiliency covers architecture decisions in case of EM attack detection. It should consider the introduction of an EM attack detection system including the following features:

- A local Health Attack Manager (train HAM or trackside HAM),
- A Central health attack manager (CHAM).

These features will be described in the section ‘detection of EM jamming”.

1.3.1.3 Transport Technology Independence in ERTMS

Ensure that the transport technology specified in ERTMS is technology independent.

Nowadays, GSM-R is totally linked to the ERTMS specification. Thus, a modification of the wireless technology implies a considerable change in other fields of ERTMS such as the protocol stack for the ETCS message exchange or the definition of new

QoS requirements to fulfil. This monolithic design is a handicap to propose changes because any change can have a significant impact on all the ERTMS specification sets. Although, it is important to set one specific transport technology in order to have a realistic and feasible specification, the specification should take into account the future migration towards new wireless technologies and avoid an excessive dependence with the wireless technology.

1.3.1.4 Moving to IP in ERTMS

It is recommended to switch from OSI-based protocol stack to IP-based protocol stack in the ERTMS specification.

All the newer wireless technologies since GSM (GPRS, WiMAX, LTE ...) are based on packet switching technology and IP protocol. Current protocols used for ERTMS are based on OSI protocols which today are hardly used outside the railway domain. Adopting the IP family of protocols, one can use new technologies and protocols in ERTMS more transparently in the future. Furthermore, the custom requirements of the railway industry could be achieved with a detailed parameterization of the protocols.

1.3.1.5 Vertical handover on backup communication links

Considering different characteristics of communication (voice and data), alternative communication links could be integrated as "GSM-R backup". Two communications links with different communication protocols and frequency resources, one dedicated to voice transmission and another one dedicated to data transmission may offer better resilience to EM attack, better QoS for railway services and two different ways to manage operational security.

1.3.1.6 Integrating Multipath Communication in ERTMS

Use of Multipath protocols in the future IP-ERTMS specification will help to manage smooth transition with alternative communication links.

Multipath protocols can provide flexibility in complex issues such as horizontal and vertical handovers. They can provide even more independency with the wireless technology, easy migrations of technologies, and easy use of multiple technologies simultaneously and release applications from managing multiple connections.

1.3.2 Radio Network features

1.3.2.1 Install additional BTSs or repeaters in hazardous area

This recommendation aims to install additional BTSs in hazardous area to increase the coverage level of the existing network. Most of the time, BTSs are spaced approximately about 5 km, but in some case this distance can be higher. A solution can be to add BTSs to increase the received level. This can be the case in rural area where the distance between BTS is usually longer than 5 km.

The impact on network planning and handover performance should be investigated.

1.3.2.2 Mesh architecture and radio micro-cells

Multiple paths in mesh network can improve communication resilience in case of local jamming as well as on terminal or network side. This recommendation proposes to add supplementary antennas in order to create new communication links based on mesh architecture.

When a jammer is present for example inside the train, based on additional radio relay or router we can rely on the network architecture including these additional antennas in such a way that the information can be sent and ensure the continuity of the communication. We can consider such solution in railway stations. One possible implementation could be to introduce meshing network by using the mobile terminals of the railway staff as repeaters in the station.

In a radio micro-cell network, micro BTSs can be connected to antennas installed at lower height above the ground than the normal BTSs. These types of BTS are less expensive than normal BTS. Micro cells can improve the radio coverage at specific location of the network where higher risks of jamming were identified.

1.3.2.3 Frequency hopping

Frequency hopping in case of disturbance allows to use different frequencies (on hypothesis that jamming is not on all frequencies). The principle of frequency hopping is based on repeated switching of frequencies during radio transmission according to a certain "hopping" pattern. It was initially foreseen as a solution to minimize the effectiveness of "electronic warfare". By frequency hopping the signal pass through a different frequency channel and a different set of interfering signals so that the impact of jamming signal on the frequency will be minimized, especially when we are in presence of narrow band frequency jamming. In presence of a wide band jamming signal, this solution is not available: it will be necessary to commute over a frequency significantly different which is generally exploited by another network.

1.3.2.4 Channel hopping features

Channel hopping in case of disturbance, allows to use different time slot (on hypothesis that jamming is not on all slots at all times).

In the same principle when signal jamming is narrow band the channel hopping (slot hopping) seems to be a possible solution to minimize jamming effect on the signal, and avoid loss of data.

By switching from one user slot to another, in case of wideband jammers, we can avoid the effect of jammers not sufficiently fast to affect all the user slots of the frame at the same time.

1.3.3 Rolling Stock

1.3.3.1 Coach isolation

For an attack scenario which involves a jamming system on board the train, it can be interesting to reduce the coupling between the railway on board antennas and the jamming signal which are emitted inside the coach. Then, installation of EM field shielding in the train roof may allow to reduce the impact of the jamming on the operational received signal from the network.

1.3.3.2 Enlarge the ground plane below the train antenna and/or reduce the antenna profile

The objective is to minimize/avoid the effect of jamming coming from lower direction with respect to the horizontal plane.

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.

1.3.3.3 Protection of radio transceivers

The objective is 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 locomotive 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 locomotive and its internal separation walls to create chambers decoupled with respect to the external electromagnetic field. However, as is well known from shielding theory, a shield is effective if the metallic continuity of all walls of the enclosure is insured, i.e. any opening of a size comparable with the wavelength have been removed to avoid re-radiating the external field inside the enclosure, thus strongly reducing the electromagnetic protection.

1.3.3.4 Use RF double-shielded coaxial cables

The objective is 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.

1.3.4 Train antenna

1.3.4.1 Changing train antennas from E-plane isotropic antennas to E-plane high front-to-back ratio antennas

The idea of this recommendation is to change the actual GSM-R antenna to minimize or avoid the effect of the jammer by limiting the coupling level with it.

Since the existing antennas have quasi-isotropic radiation pattern in a horizontal plane, receiving almost equally electromagnetic signals from everywhere at the ground level, we propose to replace it by passive high gain antennas, which will provide a smaller coupling factor with the jammer.

As an example, changing train antennas from the existing E-plane isotropic antennas to E-plane high front-to-back ratio antennas (null pointing in the train direction) will limit coupling between potential jammers inside the train and train antennas. The impact on handover operation should be investigated.

1.3.4.2 MiMo antenna for mobile station

As presented in Figure 2, for mobile station, MiMo antenna with adequate distance between the antenna elements could provide an improved radio link to the BTS thus, providing a better resilience to local jamming.

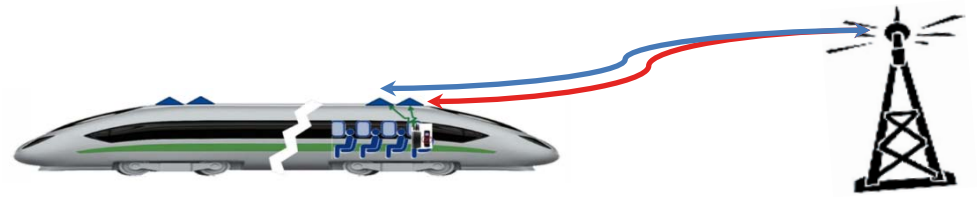


Figure 2: Multi communication paths with MiMo technology

1.3.5 BTS antenna

1.3.5.1 Install narrow-beam antennas on BTS

The objective is 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(s).

2. DETECTION OF EM JAMMING

2.1 JAMMER DETECTION TECHNIQUES

In the SECRET project, different detection techniques were studied which are based on the monitoring of different parameters. For efficiency managing jamming situation, the detection is a fundamental function. The detection can permit us to accurately diagnose and not imagine a technical failure. This distinction is essential for activating an appropriate response.

2.1.1 Detection based on the Error Vector Magnitude (EVM) monitoring

The EVM parameter is obtained by demodulation of a communication signal. The EVM is the difference between the position of a reference symbol in the In Phase and Quadrature (I/Q) representation and the position of the measured symbol at the monitoring instant.

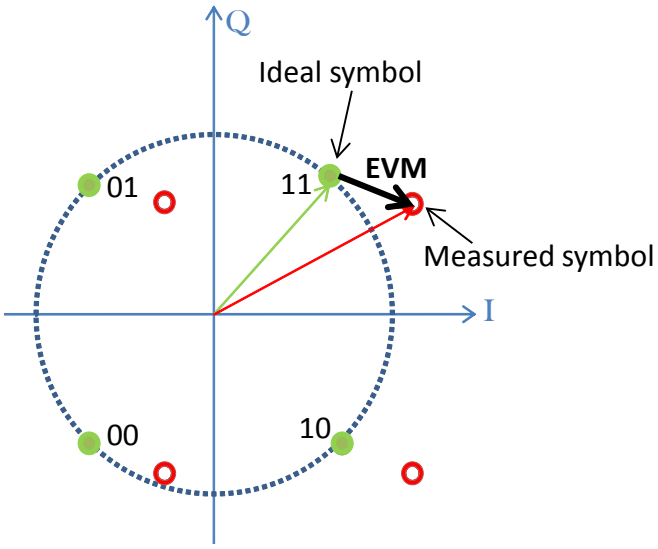


Figure 3: Representation of the Error Vector Magnitude (EVM)

In normal situation (no attack), the value of EVM does not vary significantly. Then, a strong variation is revealing the presence of interferences. The monitoring of the EVM also permits to distinguish a non-intentional interference from an intentional interference. Indeed, the main railway interferences which affect the EVM are the interferences associated to the sparks between the catenary and the pantograph. However, these interferences are really brief (some ns) and never affect more than one symbol. So, in monitoring the global EVM over one GSM-R burst, the presence of jamming signal is perfectly detectable.

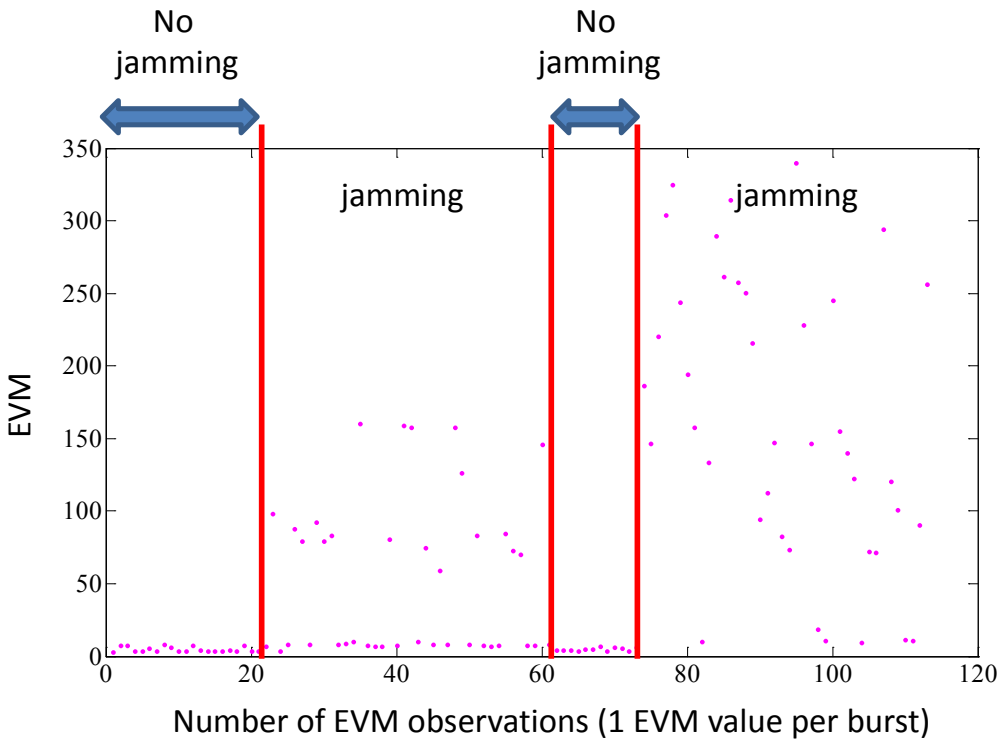


Figure 4: Variation of the EVM with and without jamming signal

GSM-R receiver includes an I/Q demodulator. The EVM can then be obtained by measuring I/Q distortions in adapting the GSM-R terminals. This solution allows the detection of jamming and can be implemented inside cab radio and BTS. In case of detection of a potential jamming the train driver and control centre can be informed.

The experimentation performed in SECRET showed that this detection technic is really sensitive, that means that we can detect the presence of low power jamming signals which are not yet sufficient to affect the quality of the communication. It can then permit to activate or send alarm before than the communication is lost.

However, this detection solution is focused on the monitoring of the used communication frequency channel. It then permits to protect only one communication system.

For more details about the detector implementation refer to the D4.4 on Cab-radio architecture.

2.1.2 Detection based on the monitoring of the frequency spectrum occupation

For a stable normal electromagnetic environment, a detection technic can be based on the comparison between a reference spectrum and monitored frequency spectra measured continuously. The spectrum may be divided into a number of channels. So the comparison has to raise the number of channels that contain a power greater than the power of the reference spectrum.

However, when the normal spectrum occupation is dense this technics is not really sensitive. Moreover, it requires a relatively stable spectrum occupation. It can then be efficient to implement detection along the tracks, at the BTS level or in train station.

For a more complex or dense EM environment, the detection consists in determining whether each new observed spectrum belongs or not by a stochastic process, to generative models estimated forward with said learning data. In our case these data represent a said "normal" EM configuration. Assuming that the model is representative of the normal environment, all spectra outside this / these processes will be considered suspect.

It is also possible, to constitute models including attack situations and to compare the probabilities that the monitored data belong to the "attack" or "normal" models.

This method is particularly interesting in train stations where the EM environment is generally dense. This approach can also permit to monitor different frequency bands corresponding to different communication systems.

2.1.3 Detection of an excess of energy in the operated band

One particular solution for detecting the jamming condition is to measure the presence of an excess of radiofrequency energy in the selected frequency range.

Although several methods can be derived for measuring the excess of energy in an observed bandwidth, one easily implementable solution consists in measuring the power spectral density (psd) in each communication channel by quickly scanning the band. Then, an indicator is built by summing these different channel measured data. Therefore, the indicator reflects the overall current activity in the observed frequency range. This indicator is stored. This process can be repeated and a mean value of the indicator computed, if necessary.

Depending on the selected tradeoff between sensitivity and low level of false detection, a guard value is then added to this indicator. We obtain a final threshold value below which the general activity in the band is considered normal.

Then, continuous scanning of the same frequency band is run and new values of the indicator are computed. If a new global computed value exceeds the previously computed threshold then, a potentially jammed condition is detected.

This method is based on the fact that the threshold value is computed in absence of jammer. It is particularly effective if many radio channels are free of radio activity, and of course in presence of a wideband jamming signal covering some or most of the observed channels.

2.1.4 Detection based on the monitoring of QoS

Certain solutions are already implemented to monitor the Quality of Services (QoS) linked to specific applications. The monitoring of these QoS is not necessary sufficient to detect jamming situation but the monitoring of these QoS parameters could be coupled to detection solutions in order to get complementary information or to improve the efficiency of the detection.

To illustrate this approach, the following result (obtained by simulation) illustrates the evolution of the end-to-end time delay of transmission, in presence of a jammer which would be placed in the middle of two successive BTS. We observe the significant increasing of transmission delay when the train is approaching the jammer location.

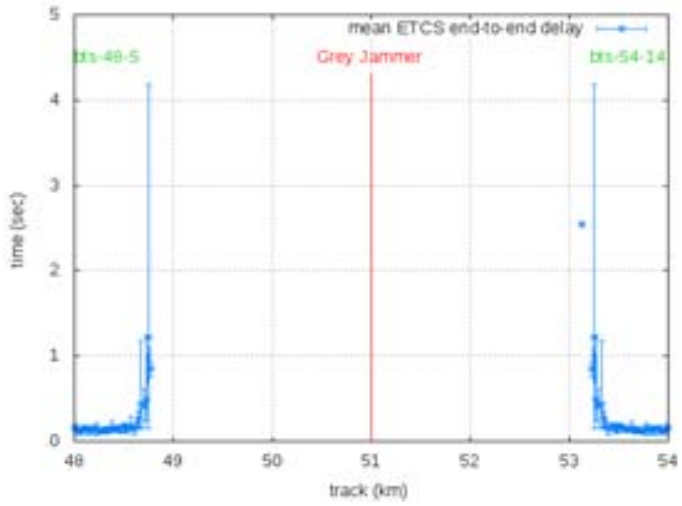


Figure 5: Simulation results - Evolution of the end-to-end delay of transmission along the track in presence of a jammer at a fixed position

2.2 JAMMER DETECTION APPLICATION

2.2.1 On board vehicle detector

On board a train, the more relevant communication system to monitor is the GSM-R. Moreover, it can be necessary to have quick and sensitive solution detection in order to be able to send alarm to the RBC before than the communication link is lost. It seem then interesting to develop solution included in the communication terminal, or at minimum connected to the GSM-R antennas in order to monitor the signals which are received by the cab radio. To permit to implement efficient mitigation process on-board, monitoring and detection have to be implemented for each on-board antenna.

Appropriate detection technic: Knowing that in this context, the priorities are monitoring GSM-R with a quick and sensitive solution, the detection technic based on the EVM value seems to be the most appropriate.

2.2.2 On-board portable detector

In case that a jammer would be introduced and activated on board the train, to come back to a normal operational solution, it could be necessary to locate the jammer and to switch off. On the base on the monitoring of the evolution of the power spectrum density according to the position of the detector, it could be possible to find the maximal position of energy.

This detector could be used by an agent in order to isolate or deactivate jammer (on ground or on-board).

Appropriate detection technic: Knowing that the localisation solution would be based on the monitoring of the power spectrum density, the most appropriate technic would be the technic based on the excess of energy in a global and given frequency band.

2.2.3 Track side (BTS proximity) Detector

On track-side and nearby the BTS, different detection solutions can be applied because the EM environment is relatively stable. Moreover, usually ground infrastructure has cable connexion for network transmission. So, even if the GSM-R communication link is jammed, the BTS can be able to inform the control centre of the jamming situation, under the assumption than an adequate process is already implemented. However, the BTS will not be able to send request information to the trains in its corresponding cell, except if another and non-jammed communication network is employed.

In this second case, the monitoring of several frequency bands corresponding to different communication network can be benefit.

Appropriate detection technic: Due to the relatively stable spectral occupation for certain BTS, detection based on the frequency spectrum occupation monitoring can be appropriate. According to the spectral occupation which can vary if the BTS is in rural or urban areas, the detection can be based on a reference spectrum for the rural area or on more complex models and stochastic process for urban areas. Both approaches can permit us to monitor several frequency bands simultaneously.

2.2.4 Track side mobile Detector

In case that a jammer would place on the track side between two successive base stations, to come back to a normal operational solution, it could be necessary to locate the jammer and to switch off. On the base on the monitoring of the evolution of the power spectrum density according to the position of the detector, it could be possible to find the maximal position of energy.

This detector could be used by a team in order to isolate or deactivate jammer.

Appropriate detection technic: Knowing that the localisation solution would be based on the monitoring of the power spectrum density, the most appropriate technic would be the technic based on the excess of energy in a global and given frequency band.

2.2.5 Train Station Detector

In train station, it is relevant to monitor several communication systems. Indeed, in train stations, according to the operators, several communication systems can be used for operational applications. In train stations, we have also to consider the security team which employ TETRA network to communicate. In this configuration, it could be interesting to have two or three monitoring and detection points, in order to have a full monitoring of the train station area and to implement a solution to locate the jamming source by comparison between the information at the different monitoring points.

Moreover, the requirements on the antennas for monitoring can be different from the other solutions to permit to simultaneously monitor several communication networks.

Appropriate detection technic: In train station, it seems essential to monitor several communication networks. Moreover, the spectral occupation is generally dense and complex. Consequently, an approach based on the frequency spectrum occupation monitoring is probably the most appropriate method. In such environment, the detection would require generative models estimated forward with learning data and to determine the probability that each new observed spectrum belongs or not to the models.

2.3 METHODOLOGY RECOMMENDATIONS

2.3.1 Jamming indicators: through harmonized indicators and reference conditions

The detection process can be based on preliminary defined thresholds or on graduate probability of jamming. Nevertheless, these parameters need to be relying to reference "jamming indicator".

The value taken by jamming indicators has to be defined for well-defined jamming conditions. The indicators could vary between the values 0 to 7, to vary according to an identical scale than the already used Reception quality indicator (called RXQual) already employed for GSM-R in railway. The 0 value could correspond to a zero jamming probability and 7 to a 100% jamming probability. Each level could correspond to a referent jamming situation, notably including the type of jamming signal and the Signal-Jamming Ratio.

Moreover, detection system could analyse several bands of frequency, representative of different services (TETRA, GSM, GSM-R, WiFi, LTE...). In case of jamming of these frequency bands, system could give a graduated probability of jamming for each frequency band. With this level of information, detection can help to redirect the information on a robust connection to the jamming in presence.

In consequence, it would necessary to have a global reflexion on the definition of the parameters which can define a "jamming" situation, in order that these parameters are adapted and harmonized for different communication protocols and networks. In terms of "jamming indicator", the harmonization should concern the different communication solutions, to permit the implementation of efficient countermeasures in situation of jamming.

Jamming indicators could also be considered for a combination or an extension of Quality of Services (QoS) indicators in existing protocols for a telecommunication technology.

2.3.2 Input to consider to design a dedicated EM attack detection solution

The choice of the detection solution can be done by considering several aspects.

Firstly, the antenna on which the detection is connected is predominant. Indeed, the frequency range covered by the antenna determines the communication networks which can be monitored. Onboard a train, if the antenna and the filters are specifically designed for GSM-R and filter all the other communication signals, it will be useless to implement a detection solution which permits to monitor several communication systems. In this case, the method based on the EVM can be the most adequate.

From a general point of view, the different detection solutions have to be assessed in employing the antenna on which they will be implemented.

The detection solution has also to be designed for a range of EM attack signal power. Indeed, the sensitivity that we want to reach is also a determining factor. The different detection solutions present significant difference in terms of sensitivity. Some detection solutions can be adapted to reach a given sensitivity.

The variation and complexity of the EM environment to monitor is also decisive. Certain detection solutions are not available is the environment permanently varies. Certain solutions are available for a variable EM environment but require a learning phase.

2.3.3 Resilient Architecture Components

The different countermeasures which were discussed in this white paper require adequate communication architecture coupled with the attack detection sensors. The Resilient Communication Architecture (RCA) proposed in SECRET project is composed of the following main:

- Health/Attack Manager (HAM),
- Central Health/Attack Manager (CHAM),
- Acquisition System Analyser (ASA),
- Sensors connected to the ASA,
- Multipath Communication Manager (MCM),
- Several communication devices behind the MCM.

The first three components are part of what has been called the protection subsystem (see figure below). The role of this subsystem is to continuously monitor the overall network for detecting EM attacks performed on the network.

The two remaining components are part of the MCM. The role of this second subsystem is to provide resilient communications between trains and the command center located at ground, in permitting to commute on another communication link robust to the detected EM attack signal.

HAMs are further subdivided in 2 categories according to their roles:

- Train Health/Attack Management,
- Trackside Health/Attack Management.

HAMs locally manage the detection information. It permits to analyze the detection information to avoid fault alarms and decide to activate local countermeasure. Thanks to the MCM, it is also in charge to inform a control center of the situation: Central Health/Attack Management.

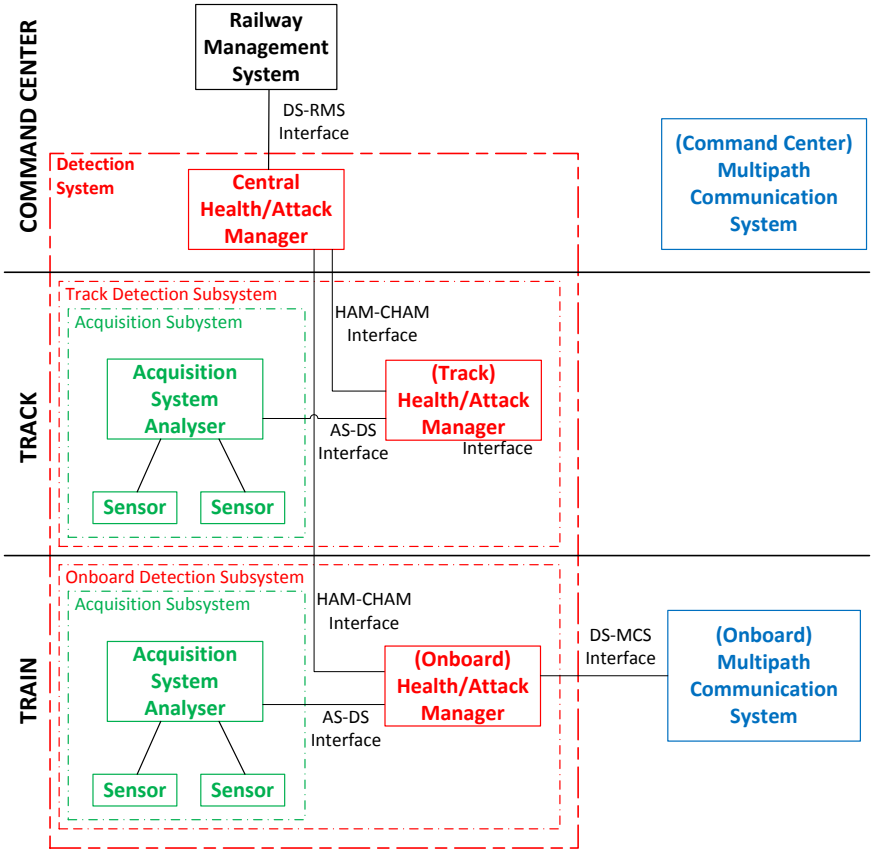
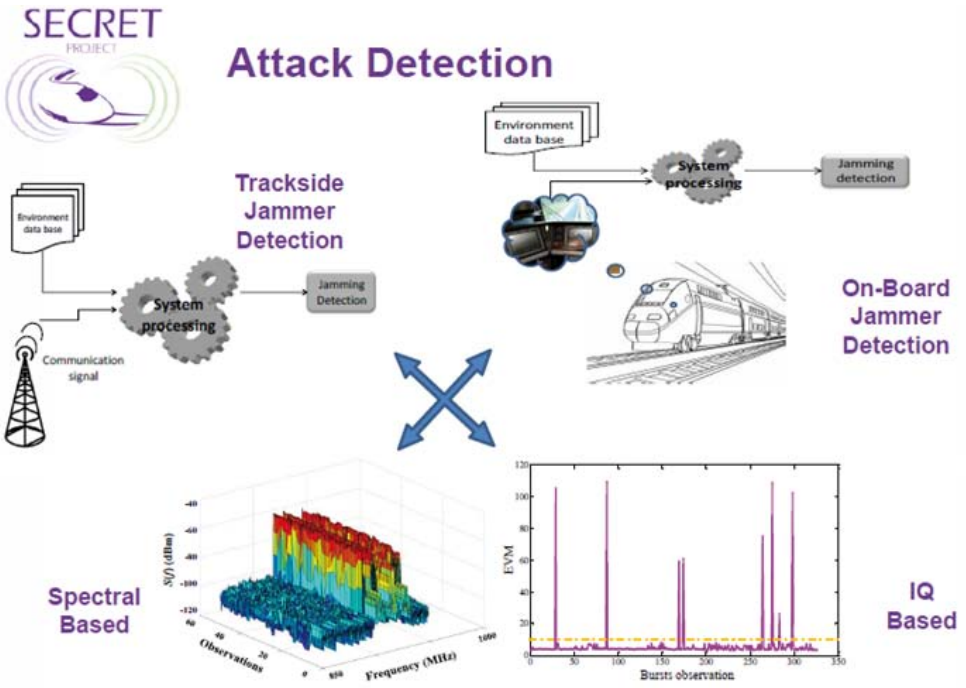


Figure 6: Secret resilience components



3. MITIGATION OF EM JAMMING EFFECTS ON TRAIN TO GROUND COMMUNICATIONS

Because permanent recommendations alone are not fully effective, and following the introduction of jammer detection systems, temporary recommendations must also be investigated.

These recommendations correspond to countermeasures which can be activated in case a jamming situation is detected in order to inhibit or minimize the impact of jamming.

Some of the recommendations focus on temporarily improving the system radio coverage. These recommendations shall meet the EIRENE specifications to ensure a minimum received radio level for voice or ETCS applications. The recommendations are not necessarily linked and, most of the time, can be implemented separately.

Such temporary recommendations require important guidelines to decide the conditions in which they can be used by taking into account the environmental criteria: jamming location, train location, level of communication degradation, railway lines category, and presence of alternative radio bearer. Their activation can be made automatically using the jammer detection system or manually from the train or control centres.

All recommendations in this category are classified as operational considering their activation will depend on the operational context.

3.1 OPERATIONAL RECOMMENDATIONS

3.1.1 Ground BTS

3.1.1.1 Increase temporarily the ground BTS output power level

The objective is to minimize/avoid the effect of jamming **by increasing the power level of the BTS**. It takes into consideration the location of the jammer (inside the train) and the detection signal process. These new power levels have to be in compliance with the ETSI standards and also meet the health recommendations.

Temporary increase of ground BTS output power level for example by 10 dB when a jamming situation is detected inside the train will increase the train received signal to jammer ratio. This necessitates managing and mitigating the impact of the corresponding correlative power increase delivered to the neighbouring cells (C/I level).

The recommendation considers environment profile when:

- Jammer is on board the train,
- Jammer output power is in the order of 1 W.

3.1.2 Train Mobile Station

3.1.2.1 Increase temporarily the train Mobile output power level

This recommendation is similar to the previous one, but now applied on the **mobile station**. In the same way it proposes to increase temporarily the power level of the mobile station to minimize/avoid the effect of the jammer when it is detected. It implies also to prove conformity with the ETSI standard.

The recommendation considers environment profile when:

- Jammer is located along the track,
- Jammer output power is in the order of 1 W.

Temporary increase of train MS output power level when a jamming situation is detected at ground increases the ground BTS received signal to jammer ratio. This necessitates managing and mitigating the impact of the corresponding correlative increase power delivered to the neighbouring cells (C/I level).

3.1.3 Train antenna

3.1.3.1 Switching from the train front cab radio equipment to the rear train cab radio equipment when a jamming situation is detected (i.e. space diversity)

This recommendation takes into consideration the length of the train and its position relative to the two adjacent BTSs. It proposes to improve the quality of the communication and avoid the effect of jamming by using both GSM-R cab radio equipment and antennas placed on board the train. The principle is to switch between the cab antennas when jamming is detected. This improves the transmission quality and signal to jamming ratio.

The train jamming powers received on the train are unlikely to be the same at both front and rear train antennas. Therefore, switching from front to rear cab radio equipment could improve the signal to jammer ratio at the train side.

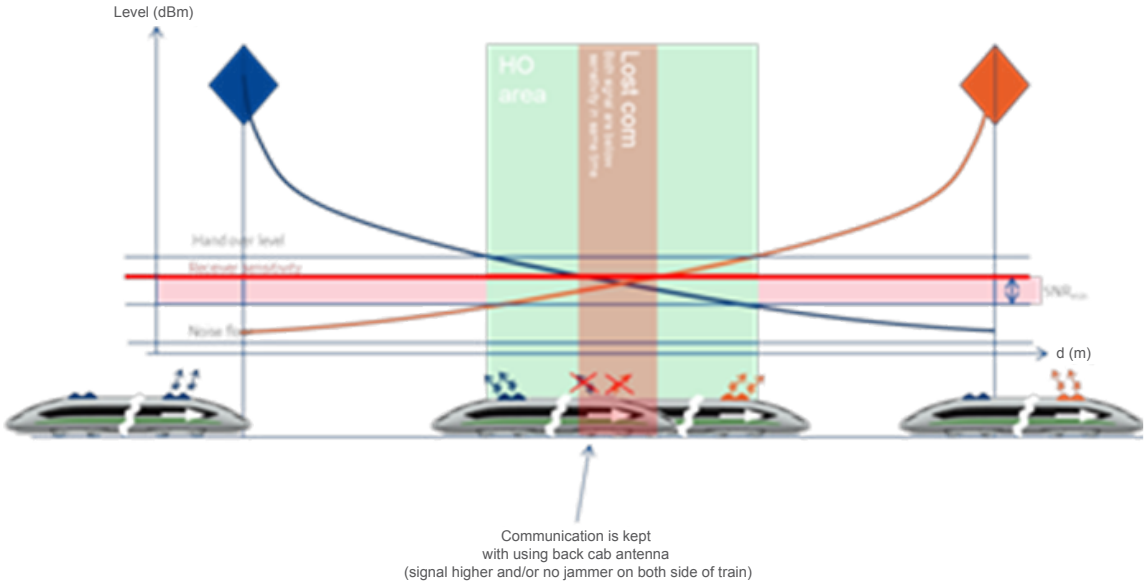


Figure 7: Switching between front and rear radio antenna

3.1.3.2 Use a special train antenna with managed diagram polarity to reject a close jamming signal (on the train or near the track)

This new recommendation proposes to modify the train antenna in order to avoid the effect of the jammer. In this case, the recommendation is to use an "active notch" antenna which is actively modifying its radiation pattern to cancel the jammer.

When a jamming signal is detected inside the train, a reflector is electronically switched on and added to only one train antenna (front or rear). This modifies the train antenna radiation pattern and attenuates the jamming received signal from the train area. A test is performed to evaluate the improvement whether the reflector is added to the rear or to the front train antenna. The impact on handover operation should be investigated.

The recommendation considers environment profile when:

- Jammer is located on board the train,
- Jammer output power is in the order of 1 W.

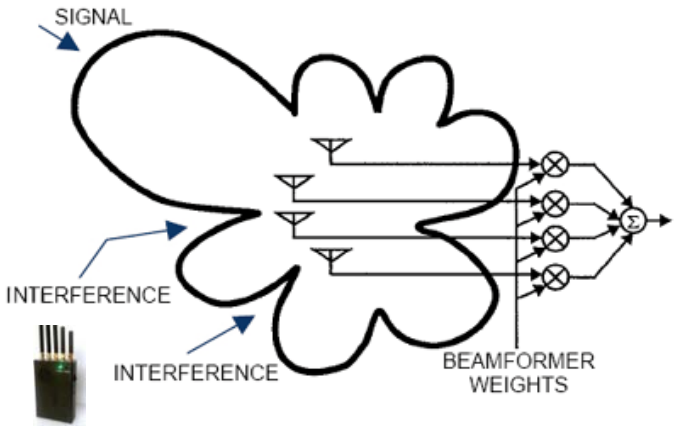


Figure 8: Principle of the "active notch" antenna

3.1.4 Radio Network

3.1.4.1 Electronically switching on emergency BTSs providing space diversity on emergency BTSs

In this recommendation, we propose to implement an intelligent network configuration by adding supplementary BTSs. These new BTSs will not work all of the time. They will be switched on only when jamming is detected, and never at the same time as the regular ones.

Based on space diversity we provide a reconfigurable network by switching on this new BTSs in case of attack detection, where the regular ones are turned off.

3.1.4.2 Install AIR Repeater as solution to improve GSM-R coverage

The purpose of this recommendation is the use of air repeater to ensure the GSM-R coverage everywhere with good *SJR* levels by using directional antennas to regenerate the local signal.

Working as bi-directional radio frequency amplifier, the repeaters amplify and transmit the signal received from MS, and, simultaneously amplify and transmit signal received from BTS.

Using an air repeater when a jamming situation is detected inside the train can increase the MS received signal to jammer ratio. This necessitates answering to the technical recommendation for coverage provided by the ETSI standard. The repeaters configuration and location need to be investigated before their placement.

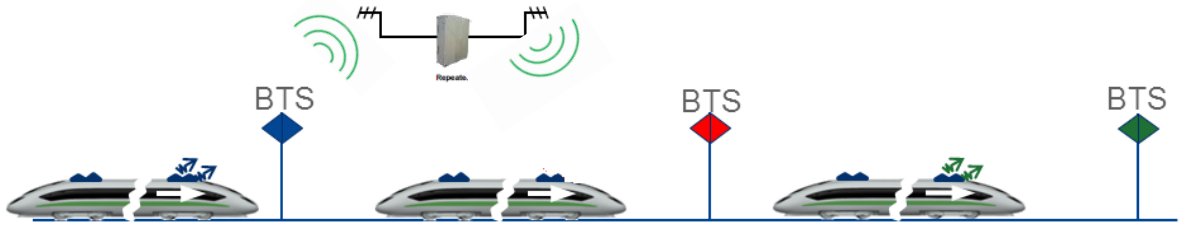


Figure 9: Air radio repeater

3.2 DECISION CRITERIA FOR MITIGATION ACTIVATION

When jamming is detected the most important information to get is jammer location: on-board the train or along the track. If the train maintains its movement authorization, it can move to confirm the jamming location and then provide countermeasures.

The jammer characteristic and its impact on the train communication shall than be measured.

As an example, we can say that 8W jamming power is a most common criterion.

	Train / Jammer location	Jamming power
Jamming on-board	Near BTS	≤ 1 W
		< 8 W
		≥ 8 W
	Bw two BTSs	≤ 1 W
		< 8 W
		≥ 8 W
Jamming trackside	Near BTS	≤ 1 W
		≥ 8 W
	Bw two BTSs	≤ 1 W
		≥ 8 W

Table 1: Evaluation criteria of jammer power level

In case of efficient jamming, a train cannot receive its movement authorization and so should require a secondary communication medium.

When a jamming condition is detected, an alarm should be sent to the control centre, using the jammed radio bearer if still available or otherwise a backup radio link based on alternative technology.

Some alternative radio technologies were analysed assuming that they can meet the railway requirements and maintain the communication established. These can be used to send alarms and emergency calls to the operation centre. Different countermeasures are then applicable to secure the situation of both the train and traffic.

	WiFi	LTE		5G	SATCOM	
		FDD	TDD		L Band	S Band
Frequency band	5,47 to 5.7 GHz	0.7 - 0.8 GHz Public Safety 1.7 - 1.9 GHz 2.5 - 2.6 GHz	1.9 - 2.5 GHz 3.5 GHz? 5.9 GHz?	< 6 GHz 6 GHz-60 GHz	1.525 - 1.66 GHz	2 - 2.35 GHz
Interference, Jamming	medium (OFDM)	medium (OFDM)	medium (OFDM)	frequency evading	more robust (directive antenna)	more robust (directive antenna)
Deployment	New sites	GSM-R and/ or new sites	GSM-R and/ or new sites	GSM-R and/ or new sites	No infrastructure	No infrastructure
Line categories	Dense area (urban/ stations)	Conventional and H-S lines	Conventional lines	To be investigated	Regional and low density lines	Regional and low density lines

Table 2: Possible alternative radio technologies

Normally, if the train has not received its movement authorization at the expected time, and has no information about the reason, the driver shall inform the operation centre about the situation.

The driver shall be authorized by the operation centre to start a movement in Staff Responsible mode (SR) by means of written order, except in case of starting a movement in level 1 with trackside signals.

The control centre may then decide which mitigation to activate according the operational context of the railway line.

Line Categories	Dedicated High-Speed Line	High-Capacity Line	Low-Capacity Line	Urban Railways Big Stations	Dedicated Freight
Typical Speed (km/h)	300	200	160	0 - 120	100
Traffic Type	Passenger	Passenger and freight	Passenger and freight	Passenger	Freight
Traffic Density (trains / h / dir.)	15	8 (mixed traffic) 15 (passenger)	2-10	30	Typically 12

Table 3: Operational context of the railway line

Regarding the temporary recommendations, we can further analyse their period of activation starting from the jammer detection up to the full recovery of normal system behaviour.

Starting from the detection of jammer, decision trees can be built as illustration of strategies that should be used for the activation of temporary recommendations.

When a jammer is detected along the tack, the environmental criteria can be evaluated in the following sequence:

1. Evaluate power of the jammer and spectral density,
2. Evaluate train location with respect to radio base station,
3. Evaluate line category.

An example of such decision tree is depicted here-below when a jammer is detected on the track side between two adjacent BTSs. If jammer power level exceeds 8 W and the operational context belongs to 'line category 1', the backup radio link can be based on LTE TDD technology operating in the 3 GHz frequency band or 5 GHz, or if not available the SATCOM can be considered.

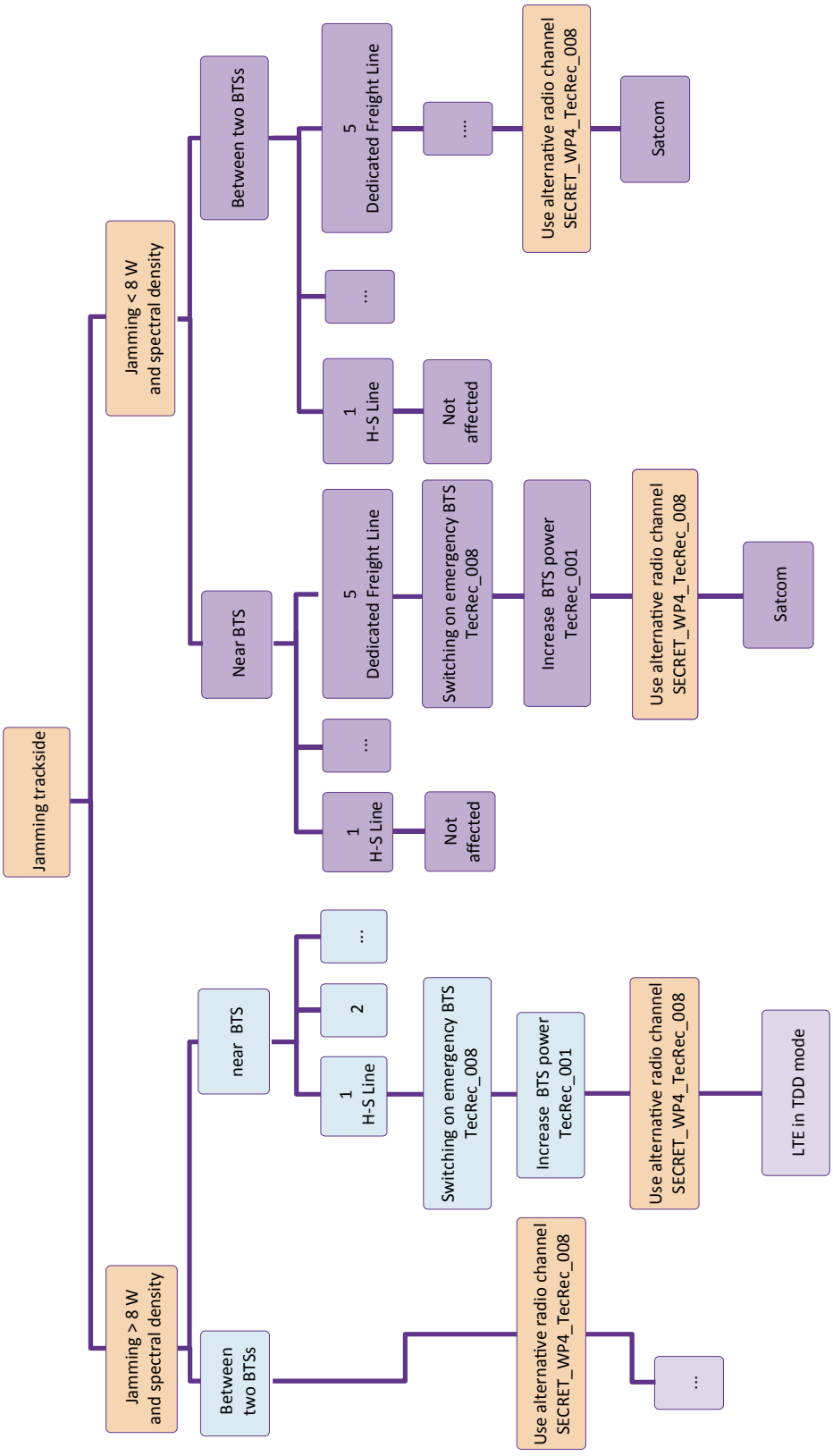


Figure 10: Decision tree for activation of temporary recommendations

CONCLUSION

In the European railway sector, the homogenisation of network technologies and the increasing use of wireless communications have made the scenario of an EM attack very likely. The communications could potentially be jammed, with trains being delayed, blocked or even diverted.

The secret project has contributed to this problematic by assessing the real risks concerning EM attacks, identifying areas for strengthening the railway network and developing detection solution and to designing a resilient architecture. As a result this white paper gives 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 technology.

The next step is to take into account these recommendations (especially regarding the system architecture) in the various existing standardization bodies (especially ETSI) and to incorporate the results into International Railway Standards.

For further information consult the deliverables on the project website at:

WWW.SECRET-PROJECT.EU

SECRET Consortium Member
Published by: UIC-ETF
Design: Coralie Filippini
Photo credit: Fotolia

ISBN: 978-2-7461-2465-3

THE SECRET CONSORTIUM

COORDINATOR

IFSTTAR

CONSORTIUM

Zanasi & Partners

Université de Liège

Politecnico di Torino

ALSTOM

Fraunhofer IAIS

SNCF

TRIALOG

Universidad del País Vasco / Euskal Herriko Unibertsitatea

UIC International Union of Railways

Contact us

Scientific Coordinator

Virginie DENIAU

French institute of science and technology for transport, development and networks (IFSTTAR)

Tel: +33 (0)3 20 43 89 91

Email: virginie.deniau@ifsttar.fr