





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 5.2

"Proposal for TecRec on preventive and recovery measures"

Submission date: 04/12/2015

Deliverable on Recommendations for a Resilient Infrastructure to EM Attacks
Date: 04/12/2015
Distribution: All partners
Manager: ALSTOM

Document details:

Title	**" Proposal for TecRec on preventive and recovery measures"**
Workpackage	WP5
Date	30/11/2015
Author(s)	ALSTOM
Responsible Partner	ALSTOM
Document Code	SEC-WP5-D5.2_Proposal for TecRec on preventive and recovery measures_v2.0 Final.docx
Version	2.0
Status	Final

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
0.1	20-10-2015	Alstom	Version for final review
1.0	30-11-2015	Alstom	Final version
2.0	04-12-2015	Alstom	Translate figure 8 from French to English

Table of content

1. Executive summary 6

2. Introduction 7

2.1. Purpose of the document 7

2.2. Definitions and acronyms 8

3. Requirements standard references 9

3.1. CEM 9

3.2. Radio 9

4. SECRET recommendation template reminder 10

5. Operational recommendations 11

5.1. Planning Risk management study : Secret_WP1_TecRec_001 11
5.1.1. Definition 11
5.1.2. Risk Assessment 11
5.1.3. Factors contributing to the risk assessment (environment profile) 12
5.1.3.1. Train location 12
5.1.3.2. Signal jamming signature 13
5.1.3.3. Jamming power and location 13
5.1.3.4. Communication quality 14
5.1.3.5. Lines categories 14

5.2. Minimizing train emergency brake impact : Secret_WP1_TecRec_002 16
5.2.1. Definition 16
5.2.2. Technical requirements 16

5.3. Infrastructure pulse signal : SECRET_WP1_TecRec_003 17
5.3.1. Definition 17
5.3.1. Technical requirements 17

5.4. Terminal pulse signal : SECRET_WP1_TecRec_004 18
5.4.1. Definition 18
5.4.1. Technical requirements 18

6. Engineering recommendations 19

6.1. Backup communication links : SECRET_WP1_TecRec_005 19
6.1.1. Definition 19
6.1.2. Technical requirements 19
6.1.2.1. Communication technologies candidate 20
6.1.2.2. Reconfiguration protocol 21

6.2. Mesh architecture : SECRET_WP1_TecRec_006 22
6.2.1. Definition 22
6.2.2. Technical requirements 22

6.3. Frequency hopping : SECRET_WP1_TecRec_007 22
6.3.1. Definition 22
6.3.2. Technical requirements 23

6.4. Channel hopping : SECRET_WP1_TecRec_008 23
6.4.1. Definition 23
6.4.2. Technical requirements 23

6.5. Coach isolation : SECRET_WP1_TecRec_009 24

6.5.1. Definition 24
6.5.2. Technical requirements 24
6.6. MiMo antenna for mobile station : SECRET_WP1_TecRec_010 24
6.6.1. Definition 24
6.6.2. Technical requirements 25
7. Detection recommendations 25
7.1. Multi band detection : SECRET_WP1_TecRec_011 25
7.1.1. Definition 25
7.1.2. Technical requirements 25
7.2. Spectrum sensing detection : SECRET_WP1_TecRec_012 26
7.2.1. Definition 26
7.2.2. Technical requirements 26
7.3. Coach detection system : SECRET_WP1_TecRec_013 26
7.3.1. Definition 26
7.3.2. Technical requirements 26
7.4. Infrastructure detector : SECRET_WP1_TecRec_014 26
7.4.1. Definition 26
7.4.2. Technical requirements 27
7.5. Individual detector : SECRET_WP1_TecRec_015 27
7.5.1. Definition 27
7.5.2. Technical requirements 27
7.6. Large band detection : SECRET_WP1_TecRec_016 27
7.6.1. Definition 27
7.6.2. Technical requirements 28
8. Conclusion 29
9. References 30
10. Annex : TecRec collected from Secret WP 1 31

List of Figures

Figure 1: Risk management process 11
Figure 2: Risk analysis procedure. 12
Figure 3: Train positions and respective radio transmission power diagram 13
Figure 4: Example of threat matrix 15
Figure 5: Example of Bow tie model for road user that fails to observe traffic control device. 16
Figure 6: ERA study for the future railway communication system. 20
Figure 7: Analysis Mason listed options for future railway communication system. 20
Figure 8: TDMA principle. 24
Figure 9: MIMO architecture. 25

List of Tables

Table 1: jamming effect according to train/jammer location 14
Table 2: Evaluation of the communication quality 14
Table 3: Lines categories definition 15
Table 4: Base station maximum output power 18
Table 5: Mobile station Output power 18
Table 6: Radio technology feasibility. 21
Table 7**:** Comparison of multipath transport layer protocols 22

1. Executive summary

A largest part of the WP5 involves carrying out Technical Recommendations (TecRec) based on the results of the different WP.

WP1 studies the different jamming devices able to disturb the railway infrastructure and their potential effect on the system. This work permits to identify the critical equipment of the infrastructure that needs to be protected.
In the same time it tries to identify the scenarios that provide critical events on the railway network to avoid them and to predict countermeasures.
However, these work results could highlight vulnerabilities of the railway network. Consequently, in order to avoid the disclosure of sensitive information, these results were confidential.

As results, the present deliverable D5.2 aims to provide technical recommendation in order to strengthen the system against risks related to EM attacks. Based on risk analysis different proposals were carried out to harden the railway system and ensure its security by recommending countermeasures.
However, for the same reason of confidentiality, the document couldn't contain all the possible recommendations.

Derived from risk assessments, potential system threats were identified and then a selection of TecRec has been proposed.
These recommendations aim to avoid reaching undesirable jamming effect on railway architecture. It aims also to carry out protective measures to reduce the catastrophic consequence of jamming.

Most of the time, the recommendations presented here refer to operational, engineering and attack detection aspects that can be applied differently by the railway operators.

A template of the recommendation in excel file is annexed to this document.

2. Introduction

2.1. Purpose of the document

This deliverable summarise the WP5 Task 2 by presenting technical recommendations issued from the risk analysis performed by the WP1. Based on potential scenarios of jamming, these recommendations will define preventive and recovery measures.
D5.2 provides in the same time hardening rules to strengthen the railway system when jamming occur as well as how to prevent from jamming.

> During the first part of the project, WP1 listed potential attack devices from public domain that can be used against railway infrastructure. In the second part, a study of their impact was carried out. These tasks established realistic inputs for the estimation of the vulnerability for safety-critical railway infrastructure.
> Based on the impact of potential EM attacks on railway infrastructure developed on WP1 and the consortium discussions we could investigate some rules to prevent from the effect of jamming devices.

We propose in the document three types of recommendations, operational, engineering and detection. These preventive recommendations aim to strengthen the existing rules to satisfy the constant evolution of the security needs. It works also to prevent from the jamming effect by adapting/improving the railway infrastructure according the risk assessment study.

Previous recommendations were presented in D5.1 [1] and will be developed in this present document.

In the following section we will describe the recommendation template defined previously. We will present a short reminder of the different topics considered by the TecRec.
Based on the technical template, we describe in more details the recommendations taking into account conformance with existing standard.

A conclusion to this deliverable will then be provided as well as acknowledgments and references.

2.2. Definitions and acronyms

	Meaning
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
GSM	Global System for Mobile communications
GSM-R	Global System for Mobile communications - Railways
HSL	High Speed Line
IEM	Intentional ElectroMagnetic
LGV	Ligne à Grande Vitesse (High Speed Line - HSL)
MS	Mobil station
QoS	Quality of service
SJR	signal to jamming ratio
SR	staff responsible
TGV	Train à Grande Vitesse (High Speed Train – HST)
UIC	Union international des chemins fer

3. Requirements standard references

3.1. CEM

- 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**

3.2. 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**.

4. SECRET recommendation template reminder

In this document we will use the TecRec standard template presented on D5.1 [1]. This section provides a short reminder of the information needed to define every TecRec.

- **TOPIC**:
  - Define what type of issue is addressed by the Technical Recommendation;

- **DESCRIPTION**:
  - Define how the addressed issue is mitigated/solved by the proposed TecRec;
  - A link to an external document can be added if additional details are required";

- **WP**:
  - The WPs of the SECRET project related to this TecRec;

- **TYPE**:
  - New standard: the proposed TecRec requires creation of a new standard;
  - Standard update: the proposed TecRec requires an update of an existing standard;
  - Engineering rules: the proposed TecRec indicates engineering rules best practices;
  - Operation: the proposed TecRec indicates operation best practices;

- **INVOLVED BODY**:
  - The bodies that have to consider the proposed TecRec (CENELEC, ETSI….);

- **TECHREC STATUS**:
  - New: technical recommendation has been created;
  - Open: technical recommendation has been submitted to SECRET board;
  - Instructed: technical recommendation has been fully processed by SECRET board;
  - Closed: technical recommendation has been processed, *i.e.* submitted to the involved bodies or cancelled;

- **MISCELLANEOUS**:
  - Column used for all other topics (identification of standard to be update, TecRec status decision rational, TecRec ID…).

5. Operational recommendations

5.1. Planning Risk management study : Secret_WP1_TecRec_001

5.1.1. Definition

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 of this study is to generate key risk assessment results that can be used for railway safety management.

The Bow-tie and TVRA methods were used in Secret to assess railways incidents and railways communication system incidents in the other WP deliverables.

Topic	Planning Risk management study
Description	The first study to do in order to prevent from jamming effect is the implementation of risk analysis.
Type	Operation
Involved bodies	Railway industry and operators

5.1.2. Risk Assessment

To provide a good estimation of preventive measures needed to manage jamming effect on the railway infrastructure, it is necessary to determine the level of risks assessment impacts.

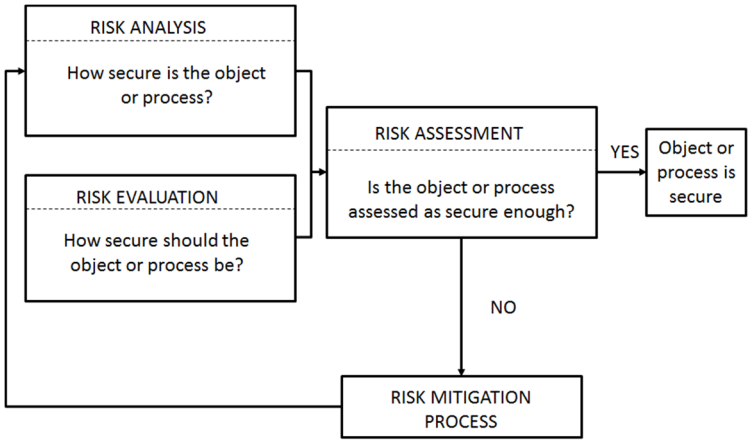


Figure 1: Risk management process

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 safe the object or process is, by the following steps: scope definition, hazard identification, and risk estimation.
Risk identification is the process of determining what can go wrong, why and how.
Risk evaluation is the process of examining and judging the significance of risk. It must answer the question how secure 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:

1. Risk assessment, the overall process of estimating the level of risk of a particular hazard
2. 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;
3. 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;
4. Risk, measured in terms of a combination of the consequences of an incident and their likelihood;
5. Likelihood, the probability of occurrence;
6. Consequence, the severity of an outcome or incident;

The study can be defined by the scheme on Figure 2.

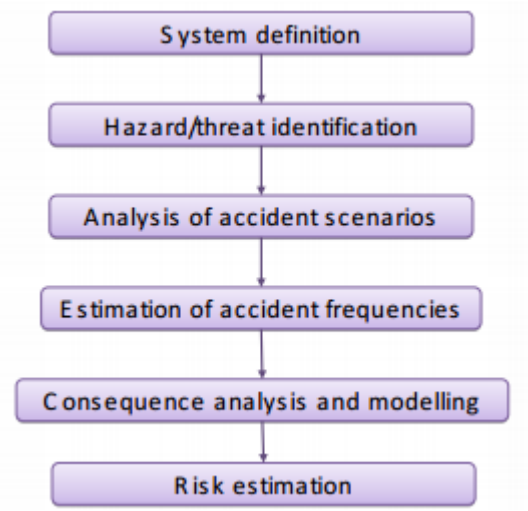


Figure 2: Risk analysis procedure.

This analysis should take in consideration EM system definition, potential targeted system in addition of different factors during the study.

5.1.3. Factors contributing to the risk assessment (environment profile)

The environment profile of the present document describes the different factors that impact the system and the risk assessment analysis.
According to the railway environment, different factors can be evaluated to carry out the study.
We start this section by the study presented on D5.1 [1], presenting the potential impact of jammer according to the Handover mechanism.

5.1.3.1. Train location

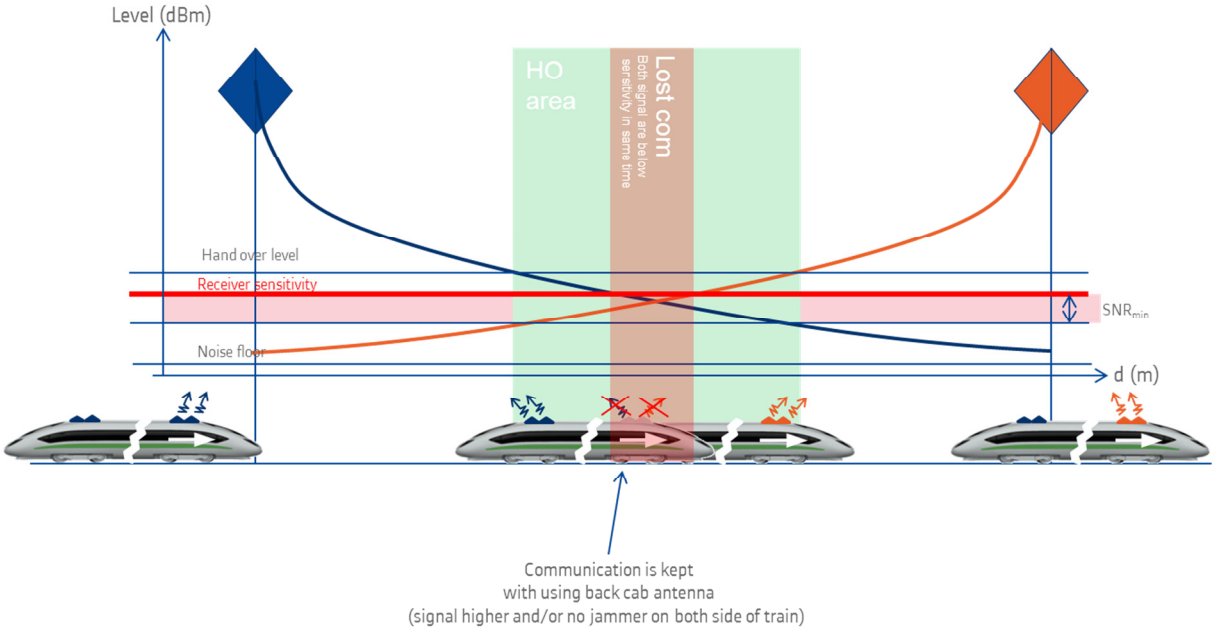


Figure 3: Train positions and respective radio transmission power diagram

During our work we have considered the jamming effect by studying the distance of the train from the radio base station (BTS). This study takes into account the evolution of transmission power (emission/reception) when the train is in the neighbours of the base station.
For example, Figure 3 presents the evolution of transmission level for two adjacent BTSs according to the movement of the train.
Two different situations are considered:

- when the train is near to the base station, which means that the transmission levels are good and the power signal to jamming ratio is high.
- when the train is far from the BTS or between two adjacent BTSs where the handover process is performed.

This position represents the worst case for the transmission levels when the power signals to jamming ratio can be critical. In this present document we shall propose technical recommendations to avoid this critical situation.

5.1.3.2. Signal jamming signature

Previous study carried out on WP1 made a survey of jamming devices. Firstly, an inventory of devices has been considered. Therefore, according to the specification of the different devices defined, a second task studied models of the waveforms to detect and regroup them according to:

- Model of narrowband waveform;
- Model of ultra wideband waveform;
- Model of damped sinusoidal waveform.

During our work we have then to differentiate jammers according to this waveform classification.

Also, choice has been made to consider in priority devices that:

- Can be easily found in the public domain (internet, electronic shop…)
- Require a low or average level of technical skills

5.1.3.3. Jamming power and location

In this paragraph we remind study done on WP3 [2] about the jamming power and location in relation of the train.
According to the jamming level and location, the following jammer impacts are presented into *Table 1*.

	Train/ jammer location	Jamming power	Effect

Jamming on-board the train	Near to the BTS	<= 1W	Negligible on uplink and downlink
		< 8W	Downlink is off negligible on the uplink
		> = 8 W	Downlink + uplink is off
	Between tow BTS	<= 1W	Negligible on the uplink downlink is off
		< 8W	Downlink + uplink is off
		> = 8 W	Downlink + uplink is off
Jamming along the track	Near to the BTS	<= 1W	Negligible on uplink and downlink
		> = 8 W	Downlink + uplink is off
	Between tow BTS	<= 1W	Negligible on uplink and downlink
		> = 8 W	Downlink + uplink is off

Table 1: jamming effect according to train/jammer location

Two initial situations were considered, when the jammer is inside the train or when the jammer is outside the train along the track. Different cases are possible.

Among all possible cases, we selected the relevant ones to continue the study.

5.1.3.4. Communication quality

Different detection algorithms were developed on WP3 and are able to detect the presence of jamming. The aim is to be able to detect the presence of this jamming before the deterioration of the link and the total loss of connection.
Previous study made on the communication resilience leads to the results presented on Table 2.

RxQual	Bit Error Rate (BER)	Quality of the communication
0	BER < 0.2%	excellent
1	BER= [0.2% à 0.4%]	good
2	BER= [0.4% à 0.8%]	
3	BER= [0.8% à 1.6%]	acceptable
4	BER= [1.6% à 3.2%]	
5	BER= [3.2% à 6.4%]	bad
6	BER= [6.4% à 12.8%]	
7	BER>12.8%	Very bad

Table 2: Evaluation of the communication quality

We can use the
Table 2 as a reference to determine an operation point, which represents the acceptability level from which it becomes necessary to detect jamming and apply countermeasures.

5.1.3.5. Lines categories

Other parameter that is important to consider is the line categories. Previous study indexes the different line categories on five classes. The Table 3 is derived from the results of this study [3] and presents the different line categories and there characteristics.

Line Category	1	2	3	4	5
Typical profile	Dedicated High-Speed Line	High-Capacity Line	Low-Capacity Line	Urban Railways	Dedicated Freight
Line Speed (km/h)	160-350	120-230	120-160	Up to 140	120
Typical Speed (km/h)	300	200	160	120	100
Traffic	Passenger	Passenger and freight	Passenger and freight	Passenger	Freight
Traffic Density (trains per hour per direction)	15	8 (mixed traffic) 15 (passenger only)	Typically 2-10	30	Typically 12
Operational processes which determine track capacity	2 successive trains (same direction)	2 successive trains (same direction) Track branch to allow overtaking at certain locations	Crossing of 2 trains of opposite direction on a single track line Change of running direction	2 successive trains (same direction) Track branch to allow overtaking at certain locations	2 successive trains (same direction)

Table 3: Lines categories definition

Actually, the presence of jamming and the loss of train communication can have different effect depending on the line categories. In fact, high speed line that needs a high quality of service doesn't react to 40 seconds loss of train communication in the same way as Urban Railways [3].

During the risk assessment study of the SECRET project, three axes needed to be evaluated:

– Treat assessment (determination, human and organisation, resources…)
– Vulnerability of a system (technical feasibility)
– Attack consequences and their potential level

For each axis, we can apply a specific risk analysis. Different methodologies exist today:

Generic Threat Matrix methodology:

The Generic Threat Matrix is a threat model used to characterize and differentiate threats against targets of interest.

THREAT LEVEL	THREAT PROFILE						
	COMMITMENT			RESOURCES			
	INTENSITY	STEALTH	TIME	TECHNICAL PERSONNEL	KNOWLEDGE CYBER	KNOWLEDGE KINETIC	ACCESS
1	H	H	Years to Decades	Hundreds	H	H	H
2	H	H	Years to Decades	Tens of Tens	M	H	M
3	H	H	Months to Years	Tens of Tens	H	M	M
4	M	H	Weeks to Months	Tens	H	M	M
5	H	M	Weeks to Months	Tens	M	M	M
6	M	M	Weeks to Months	Ones	M	M	L
7	M	M	Months to Years	Tens	L	L	L
8	L	L	Days to Weeks	Ones	L	L	L

Figure 4: Example of threat matrix

Failure Mode and Effect Analysis (FMEA) :

FMEA is a Failure Mode and Effect Analysis that was initially developed by the aerospace industry and used for reliability and safety analysis of engineering system.

Bow-tie method:

Bow-tie method is a qualitative risk assessment technique, used as a simple tool to determine how crashes occur, how they can escalate and how they can be managed. It consists in two steps:

- Determination of feared event;
- Identification of consequences of the event

It presents the benefits of a combination of consequence evaluation, qualitative evaluation and countermeasure identification.

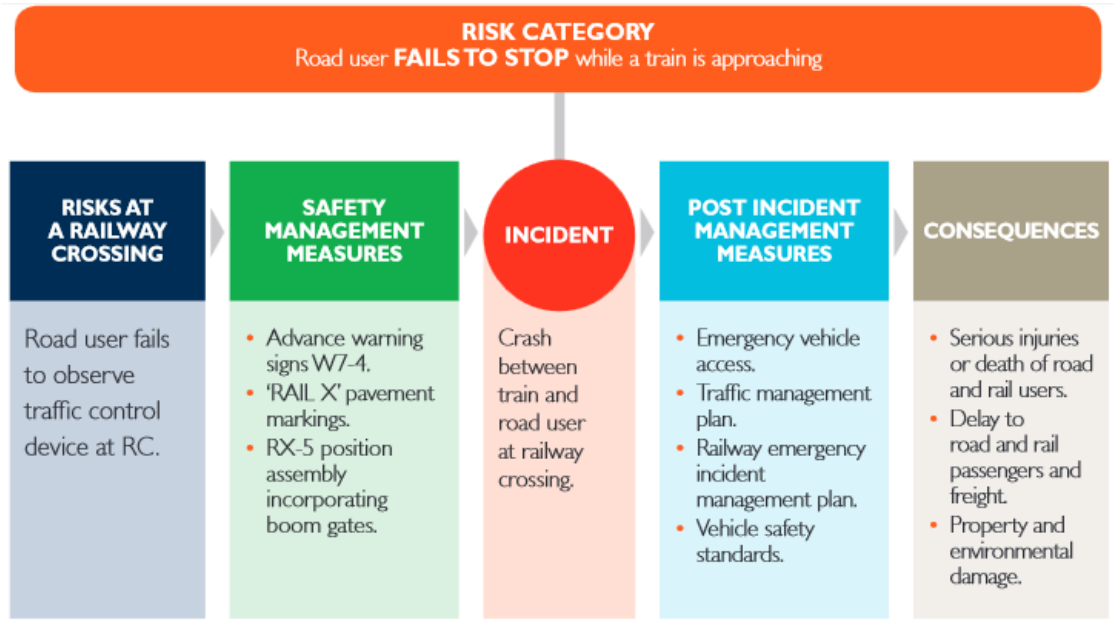


Figure 5: Example of Bow tie model for road user that fails to observe traffic control device.

5.2. Minimizing train emergency brake impact : *Secret_WP1_TecRec_002*

5.2.1. Definition

This technical recommendation implies the introduction of measures to minimize/avoid the effect of a train emergency brake over ERTMS system level 2&3 when jamming is detected.
In case of intentional jamming, the objectives of the offender can be to provoke an emergency braking in order 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.

Topic	Avoid emergency brake and run in staff responsible mode until no jamming area or/and communication available.
Description	When jamming is detected try a maximum to avoid emergency brake. The system can minimize the speed of the train using track signalling for navigation until jamming effects decrease or disappear. Try to re-initialize the train where radio coverage is available, and when train driver can contact control centres.
Type	Operation
Involved bodies	Railway industry and operators

5.2.2. Technical requirements

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 area where no connection is available because of jamming, it seems impossible for the train to get orders from the signalman.

The proposed TecRec 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 re-established.

5.3. Infrastructure pulse signal : SECRET_WP1_TecRec_003

5.3.1. Definition

The proposal is an application recommendation that sends a high pulse signal to the terminal when no response is provided by the cab radio.

Topic	Infrastructure pulse signal
Description	In case of no response of mobile, infrastructure sends high pulses for "keeping in touch" and then avoids case of complete loss of service (train stop for example). Radio terminal receiving this specific message from infrastructure could then alarm on a potential situation of jamming attack.
Type	New Standard
Involved bodies	Railway telecom industry

5.3.1. Technical requirements

GSM-R is a connected mode communication. This implies that there is a continuous link between the BTS and the Cab radio.
Where no signal from the radio network is received, this recommendation proposes that the radio network sends a higher signal pulse to the onboard equipment as a "keeping in touch" signal. This system polling aims to get a response from the cab radio after at least 3 attempts. In case no reaction from the cab radio is received, we may conclude that a jammer is active on-board.

Table 4: Base station maximum output power

transmission power class	Maximum output power
1	320-(<640) w
2	160-(<320) w
3	80-(<160) w
4	40-(<80) w
5	20-(<40) w
6	10-(<20) w
7	5-(<10) w
8	2.5-(<5) w

This measure needs to comply with the technical recommendation about BTS maximum output power permitted by the standards, as presented in SECRET_WP3_TecRec_001, with the acceptable levels of human exposure to electromagnetic fields (EMF).

This recommendation should be further studied and developed in future works.

5.4. Terminal pulse signal : SECRET_WP1_TecRec_004

5.4.1. Definition

This recommendation is similar to the previous one but propose to act on the cab radio by sending a pulse where no reaction is provided from the BTS to maintain the communication.

Topic	Terminal pulse signal
Description	In case of no response of BTS , radio terminal sends high pluses for "keeping in touch" and then avoid case of complete loss of location service on central system and inform that the terminal could be in case of jamming attack.
Type	New Standard
Involved bodies	Railway telecom industry

5.4.1. Technical requirements

Where no signal from the train radio is received, this recommendation proposes that the train radio network a higher signal pulse to the network as a “keeping in touch” signal. This system polling aims to get a response from the network after at least 3 attempts. In case no reaction from the network is received, we may conclude that a jammer is active on-board.

According to standards, the maximum output power of the GSM-R train radio [4] is at the maximum tolerated level, so increasing power seems to be impractical for pulse signal emission.

Table 5: Mobile station Output power

Power class	Maximum output power
1	…..
2	8 w (39 dBm)
3	5 w (37 dBm)
4	2 w (34 dBm)

5	0.8 w (29 dBm)

6. Engineering recommendations

6.1. Backup communication links : *SECRET_WP1_TecRec_005*

6.1.1. Definition

This TecRec is a preventive recommendation that proposes an alternative communication link to the GSM-R system working preferably in different frequency band.
In case of intentional EM attack, the impact is potentially high on man to man and machine to machine communications. Vertical handover on backup communication links could offer a real counter measure to EM attack but also, improve global QoS of railway communication in case of radio disturbance.

Topic	Vertical handover on backup communication links.
Description	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.
Type	Standard update
Involved bodies	Engineering rules

6.1.2. Technical requirements

GSM-R Networks are evolving over IP with the introduction of GPRS. Other IP evolutions will be considered in the future for the railway radio bearer. This new system must fulfil railways operational needs, and be able to co-exist with GSM-R for a long period of time.

The European Railway Agency (ERA) states that the IP network is about to be standardized in most of the railway system. Several projects are working in this direction:

- NGTC project works on the development of the IP-based radio communications and several possible use of satellite-related technologies,
- FRMCS projects (Future Railway Mobile Communication Systems) works on the migration to IP, including coexistence and interoperability with GSM-R.

The global migration from wired to wireless systems have been considered. The way in which the excess capacity can be used for commercial services has also been investigated [5].

ERA groups provide the study frame for the implementation of the new technology (
Figure 6).

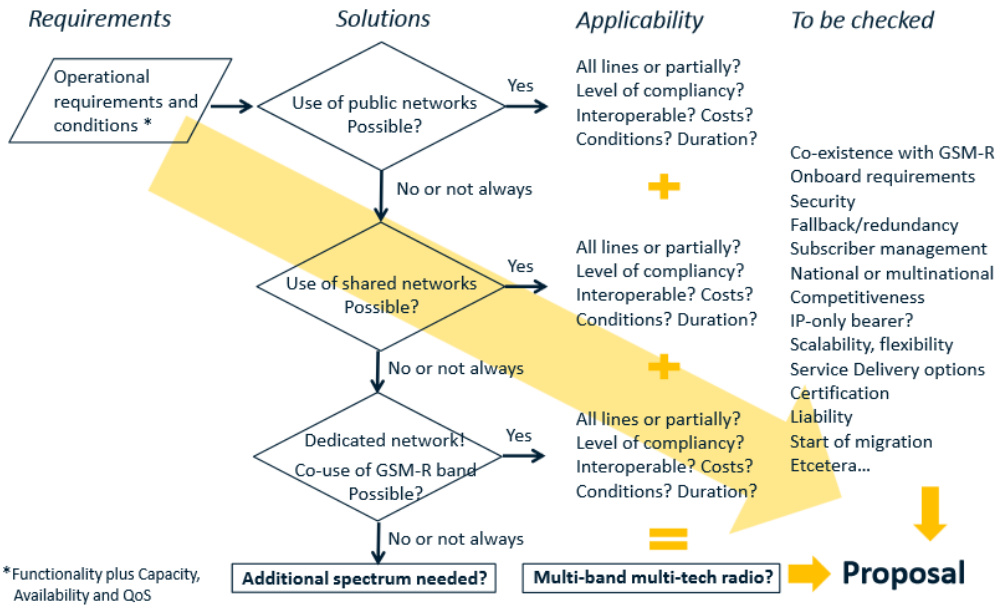


Figure 6: ERA study for the future railway communication system.

In this context a study was carried out by Analysis Mason which listed 6 options to be considered for the evolution of GSM-R (

Figure 7).

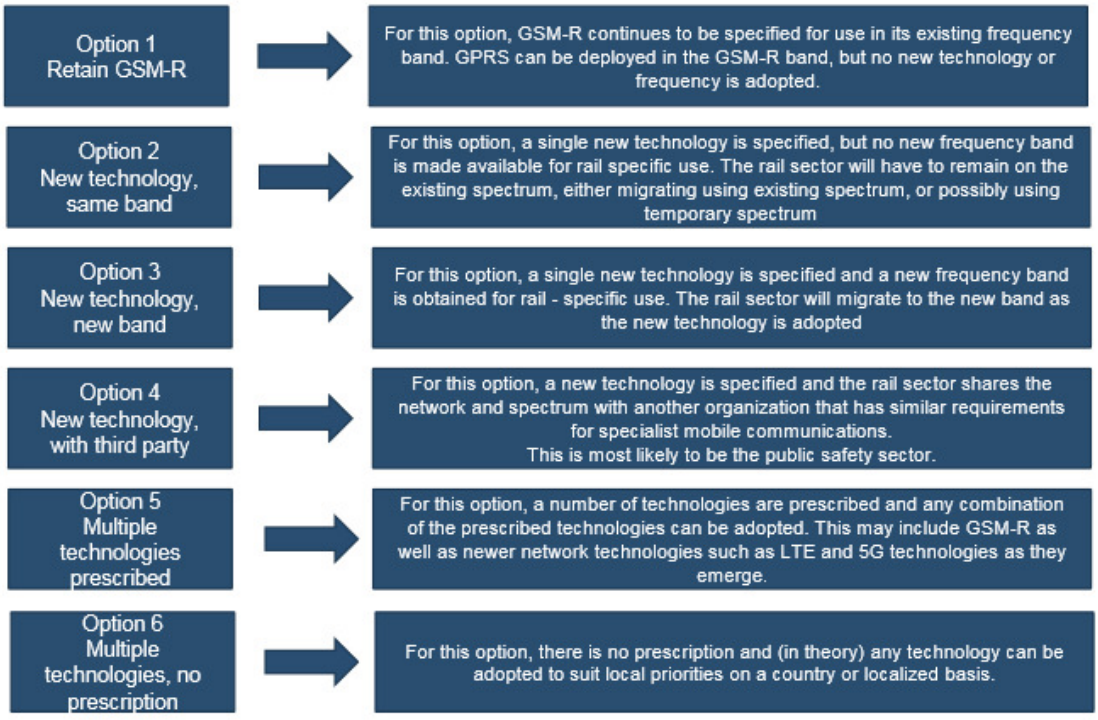


Figure 7: Analysis Mason listed options for future railway communication system.

In the same idea this recommendation propose to get two links to be sure that in case of jamming the second one working on different band could be maintained in case of radio jamming.

6.1.2.1. Communication technologies candidate

This section describes the alternative communication system that can provide a countermeasure based on reconfigurable technology against the jamming threat.

NGTC project is carrying out an initial research about the different radio-communication alternative solution for the GSM-R system.
When jamming is detected before the deterioration of the communication link, a change of radio bearer can be initiated.

According to the different line categories we present radio technologies that can be adequate alternatives in terms of frequency occupation and operational cases.

	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 wide-area 6 GHz - 60 GHz in dense area	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 in station or switch area	Existing GSM-R and/or new sites	Existing GSM-R and/or new sites	Existing GSM-R and/or new sites	No infrastructure	No infrastructure
Line categories	Dense area (urban, big stations)	Conventional and H-S lines	Conventional lines	To be investigated	Regional and low density lines	Regional and low density lines

Table 6: Radio technology feasibility.

Table 6 presents the different radio alternative technologies in the case of GSM-R failure. Different criteria are analysed and from them a solution for each kind of line can be derived.

One parameter that is important to take in consideration is also the frequency band of these communication technologies as it will be unpractical to shift to a radio technology that can also be affected by the jammers.

6.1.2.2. Reconfiguration protocol

When jamming is detected and reconfiguration needed, an adequate reconfiguration protocol is needed. Different protocols can be evaluated in terms of performances.
The initial suggestion was the multipath TCP (MPTCP) protocol. Defined as a TCP protocol, it includes a multipath network interface to increase the capacity of the system and avoid creation of a point-to-point reliable communication channel between to host machines at each time.
Based on TCP, it distributes the received data from normal socket interfaces into multiple TCP links. MPTCP can also send packets via any available network interfaces like wireless, wired or USB using point to point or point to multi point connection environment increasing significantly the speed of communication [6].
Currently MPTCP is in exploration mode. In future it could be accepted by IESG (Internet Engineering Steering Group) and standardized like TCP.
Other protocols using the multi path transmission can be retained, for instance the network interface card (NIC) Channel bonding and the CMT-SCTP (Concurrent Multipath Transfer for SCTP). From previous studies practical scenarios prefers the NIC bonding and MPTCP for their availability, usage and advantages.
Commonly used in computer networking, the Concurrent Multipath Transfer Stream Control Transmission

Protocol (CMT-SCTP) looks like the TCP protocol with ensuring similar services. Its difference lies in the possibility of multi-stream communication [7].
Table 7 presents a comparison of MPTCP and CMT-SCTP:

Protocols	Multipath TCP	CMT-SCTP
Transport layer packet type	Segment	Datagram
Connection oriented	Yes	Yes
Reliable transport	Yes	Yes
Ordered delivery	Yes	Yes
Data checksum	Yes	Yes
Explicit Congestion Notification	Yes	Yes
Multiple streams	Yes	Yes
Multi-homing	Yes	Yes
Nagle	Yes	Yes

Table 7**:** Comparison of multipath transport layer protocols

According to the parameters presented in the table, the MPTCP provides the best solution when it is possible to implement it.

6.2. Mesh architecture : SECRET_WP1_TecRec_006

6.2.1. Definition

In the purpose of communication quality improvement against jamming this recommendation proposes to change the existing network configuration on mesh architecture that could provide a better resilience in case of local jamming.

Topic	mesh architecture
Description	Multiple paths in mesh network improve communication resilience in case of local jamming as well as on terminal or network side.
Type	New Standard
Involved bodies	Engineering rules

6.2.2. Technical requirements

This recommendation proposes to add supplementary antennas in order to create a new communication link based on mesh architecture.
When 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. For example, 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.

This recommendation should be further studied and developed in future works.

6.3. Frequency hopping : SECRET_WP1_TecRec_007

6.3.1. Definition

This recommendation proposes to integrate the principle of frequency hopping when jamming is detected.

Topic	Frequency hopping
Description	In case of disturbance try different frequencies (on hypothesis that jamming is not on all frequencies)
Type	New Standard
Involved bodies	Engineering rules

6.3.2. Technical requirements

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 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.

Nowadays, frequency hopping is not deployed on GSM-R, maybe because of the restricted frequency band allowed to the railway communications, it should be interesting to reassess its use in the future.

6.4. Channel hopping : SECRET_WP1_TecRec_008

6.4.1. Definition

This recommendation proposes to integrate the principle of channel hopping when jamming is detected.

Topic	Channel hopping
Description	In case of disturbance try different channel (on hypothesis that jamming is not on all channels at all times)
Type	New Standard
Involved bodies	Engineering rules

6.4.2. Technical requirements

In the same principle when jamming is narrow band the (slot hopping) channel 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 large band jammers, we can avoid the effect of the jammer not sufficiently fast to affect all the user slots of the frame at the same time.

The channel hopping can be a jamming protection in the time domain, similar to the frequency hopping in the frequency domain.

Such technique needs to be further investigated before any conclusion can be made.

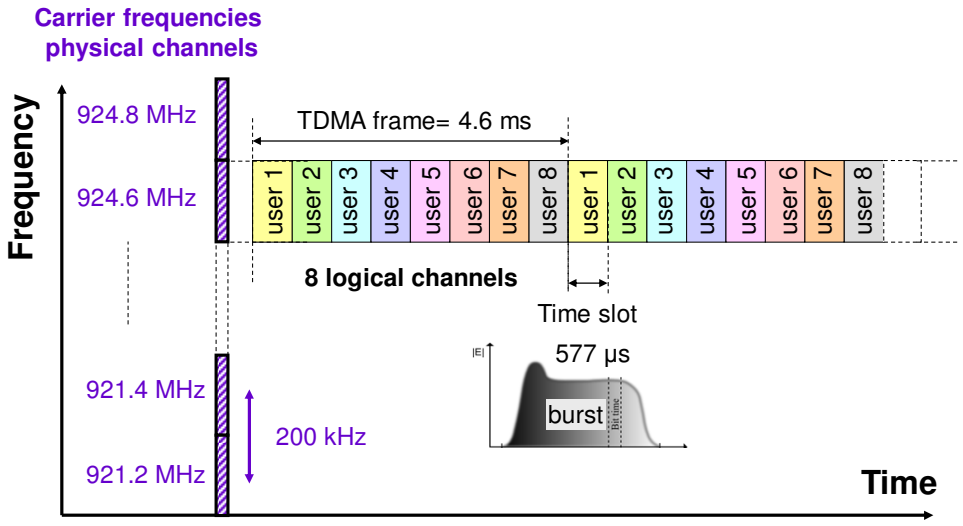


Figure 8: TDMA principle.

6.5. Coach isolation : SECRET_WP1_TecRec_009

6.5.1. Definition

This recommendation provides the installation of coach isolation on the roof of the train to ensure EM shielding.

Topic	coach isolation
Description	Installation of EM field shielding in the train roof
Type	New Standard
Involved bodies	Engineering rules

6.5.2. Technical requirements

Based on several immunity tests provided on trains we propose to carry out this recommendation in order to improve the EM shielding of the train.
This recommendation is more detailed in SECRET_WP2_TecRec_002;

6.6. MiMo antenna for mobile station : *SECRET_WP1_TecRec_010*

6.6.1. Definition

For the purpose of communication quality improvement against jamming this recommendation proposes to change the existing system antenna's to MIMO antenna's that could provide a better resilience in case of local jamming.

Topic	MiMo antenna for mobile station
Description	For mobile station MiMo antenna with long distance between the different antennas could provide a better resilience in case of local jamming

Type	New Standard
Involved bodies	Engineering rules

6.6.2. Technical requirements

The principle of MIMO antenna could be implemented on railway equipment. It could deliver possible benefits making wireless networks faster and more reliable. Moreover, because all the antennas transmit at the same frequencies, no extra per-user bandwidth is required from the standard.

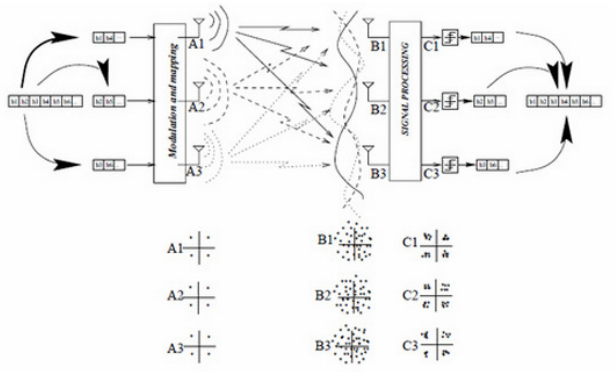


Figure 9: MIMO architecture.

Studies were done to investigate the impact of MIMO on GSM. In order to ensure compatibility, test has been performed on GSM/EDGE. A 8–ary phase–shift keying (8PSK) modulation, burst structure, and transmit pulse shape of GSM/ EDGE have been used. Bandwidth–efficiency of GSM/ EDGE can be doubled by MIMO transmission. Using reduced–complexity joint detection, good performance is achieved compared to SISO and SIMO systems which have lower overall transmission rates at the expense of some additional complexity [8].

It seems interesting to investigate the utility of the MIMO for GSM-R against jamming and also on the future communication candidate system standard.

7. Detection recommendations

7.1. Multi band detection : *SECRET_WP1_TecRec_011*

7.1.1. Definition

This TecRec is providing recommendation on detection process information. It aims to deliver quantitative information about the jamming impact.
It is also an input for the next generation of railway communication. In case of MTCP communication system this recommendation selects the alternative communication protocol when jamming is provided.

Topic	Detection of QoS of different services and operational measures
Description	In terms of detection, system could analyse for example 3 bands of frequency representative of 3 different services (GSM, WiFi,..). In case of jamming of these frequency bands, system give a graduated probability of jamming (for 1 service level 1, 2 services level 2, 3 services level 3).
Type	New Standard
Involved bodies	Engineering rules

7.1.2. Technical requirements

In terms of detection, system could analyse for example 3 bands of frequency representative of 3 different services (GSM, WiFi,..). In case of jamming of these frequency bands, system give a graduated

probability of jamming (for 1 service level 1, 2 services level 2, 3 services level 3).
The evolution of railway network predicts the use of alternative technology when jamming is present. In our use-case demonstration we provide measures with the MCM system through WIFI and WIMAX.
The process initiated during the demonstration is the switching on WIMAX when WIFI is disturbed and switching from WIMAX to WIFI when WIFI is free from jamming, or when WIMAX is jammed.

7.2. Spectrum sensing detection : *SECRET_WP1_TecRec_012*

7.2.1. Definition

This recommendation works on the detection process proposing a new method of work. Based on the recorded data base of spectrum measurements developed for the WP 3 we propose to implement a six sigma analysis.

Topic	Spectrum sensing and database reference
Description	Base on comparison of real time spectrum sensing and data collected previously in database. Detection should be done with geolocation. 6 sigma analysis based on knowledge of EM environment (samples are defined considering ground architecture and speed).
Type	New Standard
Involved bodies	Engineering rules

7.2.2. Technical requirements

Based on comparison of real time spectrum sensing and data collected previously in database, this recommendation considers six sigma methods to analyze the recorded data base of the normal environment and compare it to the real environment of test.
It proposes this new method integrating geolocation tracing process in addition of detection based on knowledge of EM environment (samples are defined considering ground architecture and speed).

7.3. Coach detection system : *SECRET_WP1_TecRec_013*

7.3.1. Definition

This recommendation provides the exploitation of systems already existing for the protection of human safety in order to detect intensity of EM field that can be recognised as jamming.

Topic	Coach detection system
Description	Large band analyser used for EM human exposition. In case of unexpected illegal signal level the analyser send an alarm to controllers giving coach location and probability of jamming attack considering signal level.
Type	New Standard
Involved bodies	Operation

7.3.2. Technical requirements

Different measures are made to evaluate the human exposure to the EM field [9] [10]. This recommendation proposes to exploit these measures to send an alarm when threshold of exposure field is reached. The probability of jamming should be important at this level.

7.4. Infrastructure detector : *SECRET_WP1_TecRec_014*

7.4.1. Definition

The study provided on WP 3 proposes several detectors based on the wireless system used for railway communication. In order to transmit the detection information this recommendation proposes to use the wired communication network, to be sure that the information is transmitted and should not be jammed.

Topic	Detector infrastructure
Description	Usually ground infrastructure has cable connexion for network transmission. On this base, integrate jamming detection system in radio infrastructure.
Type	New Standard
Involved bodies	Engineering rules

7.4.2. Technical requirements

Railway networks support signaling and control cables. These signaling cables interconnect electronic interlocks with signals, point machines, level crossings, supervision and control signals, axle counters, speed and traffic control balises. And as presented in previous study, available jamming devices cover a large range of frequencies.
This implies that detection devices should be able to transmit the jamming detection information without using wireless communication links in the frequency of jammers.
This recommendation provides the exploitation wired communication network already available to reliably transmit the information about presence of jamming.

7.5. Individual detector : *SECRET_WP1_TecRec_015*

7.5.1. Definition

Again in the scope of detection, this recommendation proposes an interesting method of detection combining both detection and localisation of jamming attacks. The final aim of this recommendation is the isolation of the jamming disturbances and their eradication.

Topic	Individual detector
Description	Accurate jamming detector giving distance of location of jamming device. This detector could be used by an agent in order to isolate or deactivate jammer (on ground or onboard).
Type	New Standard
Involved bodies	Railway telecom industry

7.5.2. Technical requirements

Different detection methods were developed on WP 3, combining detection and classification of attacks but never the location.
Developed specially for the mobile equipment dedicated to the onboard staff, these detection features can improve their operating mode by adding the localization aspect.
Discrete and mobile, such new detectors represent a mean for the railway staff to detect, discover the location of jammers and act quickly to deactivate the jamming.

In fact, when jamming is present onboard the train, based on the spectral detection methods, this detector can measure the power level of the train environment and, according to the position of both the detector and the jammer, provide different power levels that will increase when approaching near the jammer .

7.6. Large band detection : *SECRET_WP1_TecRec_016*

7.6.1. Definition

Again in the scope of detection, this recommendation proposes another way of detection directly based on the equipment outputs. It considers the level of signal from the radio mobile terminal as a descriptor for the detection process.

Topic	Large band detection
Description	Detectors operating on large frequency band (for a dedicated service like GSM), able to realise multiple carrier frequency measures (4 or 5) at a time. In case of "excessive" level of signal on many channels, system raises an alarm of potential jamming for the dedicated service.
Type	New Standard
Involved bodies	Railway telecom industry

7.6.2. Technical requirements

Different from the others, this detection process uses the signal level derived from the mobile terminals. When an anomaly is detected on one channel it can be tolerated. But, as this procedure proposes to analyze simultaneously different channel, if an anomaly is present for the majority of them it should be an indication of jamming.
This recommendation should be studied and developed in future works.

8. Conclusion

This deliverable describes the recommendations coming from different studies performed in WP1 “Threat analysis and risk assessment of attacks EM scenarios”.

The proposed TecRec are evaluated as much as possible considering their conformance with the existing standard and feasibility.

Based on works and discussion of the different partners of the project we were able to present this list of recommendations in order to prevent/avoid and minimize the impact of jamming in the system, from the detection of jammers to the improvements of the network and train radio equipments.

Different jamming devices were modelled and studied. However, the SECRET project did not cover all possible jamming detection and impacts. Therefore, several proposed recommendations should be further investigated in the future.

9. References

[1] ALSTOM, «Deliverable D 5.1, Repository of elements relevant for proposal,» 2014.

[2] IFSTTAR, «Delivrable D3.2,» 2012.

[3] European Economic Interest Group-European Rail Traffic Management System, «ETCS/GSM-R Quality of Service – Operational Analysis,» 2005.

[4] ETSI TC-SMG, «Digital cellular telecommunications system (Phase 2+); Radio transmission and reception (GSM 05.05),» European Telecommunications Standards Institute, 1996.

[5] European railway agency, «Evolution of GSM-R,» Lille, 2014.

[6] A. Ford, C. Raiciu, M. Handley, S. Barre et J. Iyengar, «Architectural Guidelines for Multipath TCP Development,» Internet Engineering Task Force (IETF), 2011.

[7] T. Dreibholz, M. Becke, J. Pulinthanath et E. P. Rathgeb, «Implementation and evaluation of concurrent multipath transfer for SCTP in the INET framework,» chez *3rd International Conference on Simulation Tools and Techniques, SIMUTools*, Malaga, Spain , 2010.

[8] N. Patrick , G. Wolfgang , S. Robert et K. Wolfgang , «Analysis of MIMO Transmission for GSM/ EDGE,» *43rd Allerton Conference on Communication, Control, and Computing, Monticello,IL, USA;,* 2005.

[9] ETSI TR 101 870, «Exposure to non-ionising electromagnetic fields Guidelines for working conditions,» ETSI, 2001.

[10] H. Junji et T. Yoshiaki, «Design of Electric Field Meter to Assess Human Exposure in Environment with Mobile Base Station,» chez *EMC'14*, Tokyo, 2014.

[11] R.-J. Y, «D6.2 Coice of technologies to study,» Next generation of train control systems 'NGTC project ', 2015.

10. Annex : TecRec collected from Secret WP 1

Reference	TecRec TOPIC	TecRec DESCRIPTION	TecRec Type	Involved bodies	TecRec Status	WP
SECRET_WP1_TecRec_001	Planning Risk management study	The first study to do in order to prevent from jamming effect is the implementation of risk analysis.	Operation	Railway industry and operators	New	
SECRET_WP1_TecRec_002	In case of intentional jamming, the objectives of the offender can be to provocke an emergency braking in order to stop the train. An emergency braking induces significant consequences because it can damage the brakes and it requires that the train being restored for operation. Moreover, the train can be stopped in a section without communication with the control center if the jamming is still activated.	When jamming is detected try a maximum to avoid emergency brake. The system can minimize the speed of the train using track signalling for navigation until jamming effects decrease or disappear. Try to re-initialize the train where radio coverage is available, and when train driver can contact control centres.	Operation	Railway industry and operators	New	1

SECRET_WP1_TecRec_003	Infrastructure pulse signal	In case of no response of mobile, infrastructure sends high pluses for “keeping in touch” and then avoids case of complete loss of service (train stop for example). Radio terminal receiving this specific message from infrastructure could then alarm on a potential situation of jamming attack.	Operation	Railway telecom industry	New	1
SECRET_WP1_TecRec_004	Terminal pulse signal	In case of no response of BTS , radio terminal sends high pluses for "keeping in touch" and then avoid case of complete loss of location service on central system and inform that the terminal could be in case of jamming attack.	Operation	Railway telecom industry	New	1
SECRET_WP1_TecRec_005	Communication resilience. GSM-R is a european standard for railway communications and applications (ETCS, ERTMS). In case of intentional EM attack impact is potentially high on man to man and machine to machine communications. Technological handover on backup communication links could offer a real counter measurement to EM attack but also, upgrade QoS of railway systems working on GSM-R just in case of radio disturbance	Considering types of data transmission (voice and data) characteristics, 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.	Standard update	Railway telecom industry	New	1
SECRET_WP1_TecRec_006	mesh architecure	Multiple paths in mesh network improve communication resilience in case of local jamming as well as on terminal or network side.	New standard	Engineering rules	New	1
SECRET_WP1_TecRec_007	Frequency hopping	In case of disturbance try different frequencies (on hypothesis that jamming is not on all frequencies)	Engineering rules	Railway telecom industry	New	1
SECRET_WP1_TecRec_008	Channel hopping	In case of disturbance try different canals (on hypothesis that jamming is not on all communication canals)	Engineering rules	Railway telecom industry	New	1

SECRET_WP1_TecRec_009	Coach isolation	Installation in roof of EM field shielding	New standard	Engineering rules	New	1
SECRET_WP1_TecRec_010	MiMo antenna for mobile station	For mobile station MiMo antenna with long distance between the different antennas could provide a better resilience in case of local jamming	New standard	Engineering rules	New	1
SECRET_WP1_TecRec_011	Detection of QoS of different services and operationnal measures	In terms of detection, system could analyse for example 3 bands of frequency representative of 3 different services (GSM, WiFi,..). In case of jamming of these frequency bands, system give a graduated probability of jamming (for 1 service level 1, 2 services level 2, 3 services level 3).	New standard	Engineering rules	New	1
SECRET_WP1_TecRec_012	Spectrum sensing and database reference	Base on comparison of real time spectrum sensing and data collected previously in database. Detection should be done with geolocation. 6 sigma analysis based on knowledge of EM environment (samples are define considering ground architecture and speed).	New standard	Engineering rules	New	1
SECRET_WP1_TecRec_013	Coach detection system	Large band analyser used for EM human exposition. In case of higher signal level than reglementation limit analyser send an alarm to controlers giving coach location and probality of jamming attack considering signal level.	New standard	Railway operators	New	1
SECRET_WP1_TecRec_014	Detector infrastructure	Usually ground infrastructure has cable connexion for network transmission. On this base, integrate jamming dectection system in radio infrastructure.	Engineering rules	Railway telecom industry	New	1
SECRET_WP1_TecRec_015	Individual detector	Accurate jamming detector giving distance of location of jamming device. This detector could be used by an agent in order to isolate or deactivate jammer (on ground or onboard).	Operation	Railway operators	New	1

SECRET_WP1_TecRec_016	Large band detection	Detectors operating on large frequency band (for a dedicated service like GSM), able to realise multiple channel measures (4 or 5) at a time. In case of "excessive" level of signal on many channels, system raises an alarm of potential jamming for the dedicated service.		Railway telecom industry	New	1