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 5.4
" Proposal for TecRec on EM attack detection”

Submission date: 30/11/2015

Document details:

Title	**" Proposal for TecRec on EM attack detection"**
Workpackage	WP5
Date	30/11/2015
Author(s)	Alstom
Responsible Partner	Alstom
Document Code	SEC-WP5-D5 4_Proposal for TecRec on EM attack detection_v1.0 Final.docx
Version	1.0
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 internal review
0.2	22/10//2015	Alstom	Version for external review
1.0	30/11/2015	Alstom	Final version

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. Environment profile 10

4.1. Train location 10

4.2. Jamming location 10

4.3. Communication quality 11

4.4. Lines categories 12

4.5. Communication technologies for the reconfiguration process 12

4.5.1. Network performance requirement 14

4.5.2. Radio Coverage requirement 15

5. SECRET recommendation template reminder 15

6. Operational recommendations 17

6.1. Increasing temporarily ground BTS output power : Secret_WP3_TecRec_001 17

6.1.1. Definition 17

6.1.2. Technical requirements 17

6.2. Increasing temporarily train MS output power : SECRET_WP3_TecRec_002 18

6.2.1. Definition 18

6.2.2. Technical requirements 19

6.3. Switching of cab radio : SECRET_WP3_TecRec_003 19

6.3.1. Definition 19

6.3.2. Technical requirements 20

6.4. Electronically switching on a quarter wave reflector : SECRET_WP3_TecRec_005 20

6.4.1. Definition 20

6.4.2. Technical requirements 21

6.5. Electronically switching on emergency BTSs : SECRET_WP3_TecRec_008 21

6.5.1. Definition 21

6.5.2. Technical requirements 22

6.6. Install AIR Repeater : SECRET_WP3_TecRec_010 22

6.6.1. Definition 22

6.6.1. Technical requirements 22

7. Engineering recommendations 23

7.1. E-plane high front-to-back ratio directive antennas : SECRET_WP3_TecRec_004 23

7.1.1. Definition 24
7.1.2. Technical requirements 24

7.2. antenna with managed diagram polarity : SECRET_WP3_TecRec_006 24
7.2.1. Definition 24
7.2.2. Technical requirements 24

7.3. Install additional BTSs in hazardous area : SECRET_WP3_TecRec_007 25
7.3.1. Definition 25
7.3.2. Technical requirements 25

7.4. Create microcells at handover overlap area: SECRET_WP3_TecRec_009 29
7.4.1. Definition 29
7.4.2. Technical requirements 30

8. Detection recommendations 30

8.1. characterization of the EM rail environment : SECRET_WP3_TecRec_011 31
8.1.1. Definition 31
8.1.2. Technical requirements 31

8.2. Deploy sensors network : SECRET_WP3_TecRec_012 32
8.2.1. Definition 32
8.2.2. Technical requirements 32

8.3. Integrate a monitoring system based on spectrum: SECRET_WP3_TecRec_013 32
8.3.1. Definition 33
8.3.2. Technical requirements 33

8.4. Implementation of EVM jammer detector : SECRET_WP3_TecRec_014 33
8.4.1. Definition 33
8.4.2. Technical requirements 34

9. Implementation of recommendations 34

9.1. Decision tree in case of jammer detection on-board the train 36

9.2. Decision tree in case of jammer detection along the track 38

10. Conclusion 40

11. References 41

12. Annex : TecRec collected from Secret WP 3 42

List of Figures

Figure 1: Train positions and respective transmission power diagram 10
Figure 2: Downlink evolution power according to the BTS distance. 18
Figure 3 : SECRET_WP3_TecRec_003: Use back cab alternative 20
Figure 4: SECRET_WP3_TecRec_004-005: Lower aggression strength 21
Figure 5 : SECRET_WP3_TecRec_010 repeater configuration 23
Figure 6 : Air repeater configuration and power for uplink and downlink. 23
Figure 7 : Propagation diagram in hilly terrain for two adjacent BTS. 26
Figure 8 : Jamming power received level and maximum cell covering in hilly terrain in presence of 1 W jamming. 27
Figure 9 : 1 W Jamming power received level and maximum cell covering in hilly terrain with additional BTS. 28
Figure 10 : 8 W Jamming power received level and maximum cell covering in hilly terrain with additional BTS. 29
Figure 11 : Hierarchical cell structure 30
Figure 12 : Detection process 31
Figure 13 : Environment data base, a: spectrum domain, b: IQ domain. 32
Figure 14 : Jamming onboard train countermeasure procedure flowchart. 35

List of Tables

Table 1: jamming effect according to train/jammer location 11
Table 2: Evaluation of the communication quality 11
Table 3: Lines categories definition 12
Table 4: Radio technology feasibility. 13
Table 5: Jammer characteristics. 13
Table 6: Call setup times defined by EIRENE. 14
Table 7: Summary of QoS requirements (ETCS over GPRS) 15
Table 8: Base station maximum output power 17
Table 9: Mobile station Output power 19
Table 10: SJR ratio and consequences 26

1. Executive summary

A largest part of the WP5 involves carrying out Technical Recommendations (TecRec) based on the results of the different WP. The previous deliverable D5.2 and D5.3 were dedicated to the risk and susceptibility analysis. Developed on WP1 and WP2, these analyses were used for the establishment of TecRec on preventive and recovery measures and on static hardening rules.

This deliverable represents the task 5.4 of the project and requires the output results of the WP3. Based on attack detection, the WP3 presents different methods to identify the presence of jamming signals. Two different methods were studied and developed.
One based on the Quadrature representation (using two descriptors: *TT* and *EVM*) and the second ones based on the spectrum analysis considering the *psd* as a descriptor. We will present in the document detection recommendations for the two methods according to the assumptions and results presented in the D3.3.
Derived from discussion considering EM detection a selection of TecRec was proposed to be presented for UIC/UNIFE standardization. These recommendations aim to prevent the effect of jamming on railway system.

The first part of the recommendations aims to improve the network coverage by increasing the signal to jamming ratio when a jammer is present. According to the ERTMS requirements, it expects the improvement of the existing BTS, the installation of supplementary ones or air repeater for most of them. The second part advises the setting up of detection system to avoid the jamming effect by the adequate countermeasures before the communication loss.

Different configurations of railway equipment and architecture are proposed to fulfil the TecRec and to be further analysed standardization bodies.

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

2. Introduction

2.1. Purpose of the document

The purpose of this document is to provide technical recommendations based on the jammer detection study. These recommendations will propose a set of methods to minimize the impact of jammer on train to ground communications.

Previous recommendations were presented in D5.1 [1], these ones will be improved in this present document.

The deliverable starts with a first main section that describes the environment profile considered for the study.

For the definition of the environment profile, the first entry is the train location. Based on the study developed previously, the effect of the jammer on the train can be evaluated depending on its distance from the BTS. This parameter is an important entry for the signal to jamming ratio (*SJR*).

The second considered entry is the jammer 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.
A third considered entry for the profile study is the communication quality. An early evaluation of the jamming power effect was made and will be used as an entry for the recommendations.

The forth considered entry is the line category; in fact countermeasures are proposed according to the line category of the trains. The different line category evaluated in the railway environments will be presented in this section.

The last chapter of this first section will describe a reconfiguration process that will provide the train with the possibility to use another communication mean based on another technology.

Communication Technology candidates will be described with their characteristics.

Therefore, we describe the different recommendations regrouped on:

- Operational recommendations
- Engineering recommendations
- Detection recommendations.

Based on the technical template presented, different solutions to be investigated and proposed to the specific standardization bodies and/or railway operators are described.

In the last section of this document, the implementations of the different recommendations are described. Using a decision tree and according to the environment profile the appropriate TecRec and their conformance requirements are identified.

And finally, a conclusion is provided followed by acknowledgments and references.

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

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
ETSI	European Telecommunications Standards Institute
GSM	Global System for Mobile communications
EVM	Error Vector Magnitude
GSM-R	Global System for Mobile communications - Railways
HSL	High Speed Line
LGV	Ligne à Grande Vitesse (High Speed Line - HSL)
MS	Mobil station
psd	power spectral density
SJR	signal to jamming ratio
SR	staff responsible
TGV	Train à Grande Vitesse (High Speed Train – HST)
TT	Radius of the IQ constellation
UIC	Union international des chemin 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. Environment profile

The environment profile of the present document describes the different parameters taken into account to evaluate the system.
According to the railway environment, different situations can be evaluated to carry out recommendations.
We start this section by the study presented on D5.1 [1], introducing the potential impact of jammer according to the Handover mechanism.

4.1. Train location

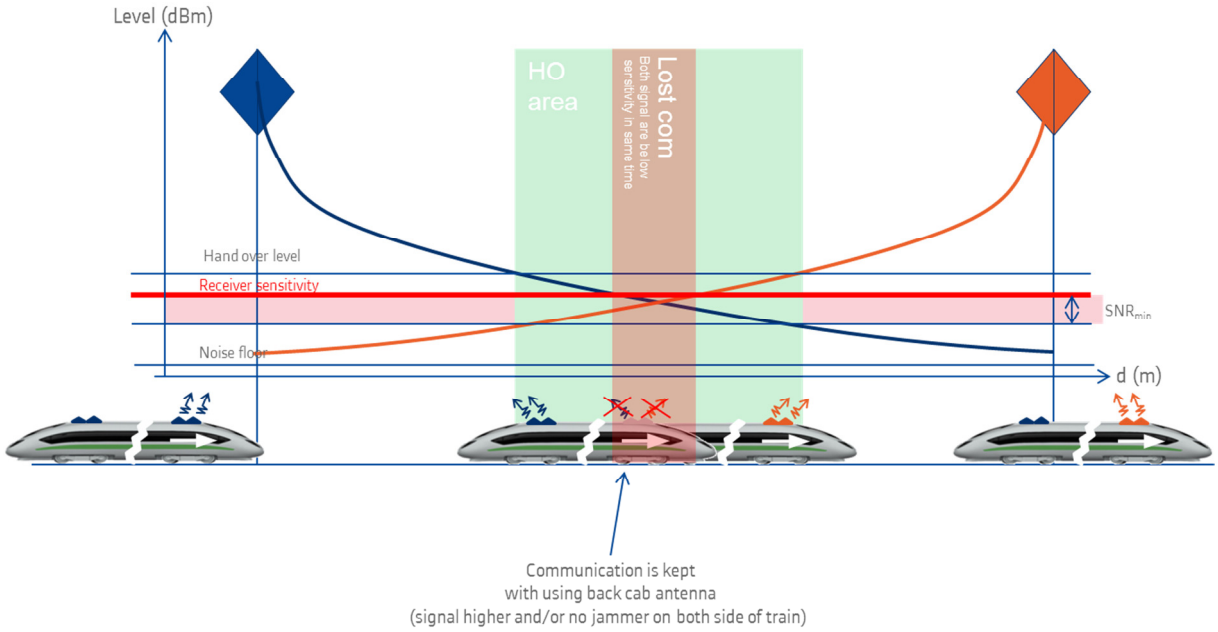


Figure 1: Train positions and respective transmission power diagram

During the study, the jamming effect has been analysed by studying the distance of the train from the 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 1 presents the evolution of field-strength received by the GSMR on board radio from two adjacent BTSs when the train is running.
Two different situations are considered,

- first case: the train is near to the base station. It means that the transmission levels are good and the power signal to jamming ratio is high.
- second case: the train is far from the BTS or between two adjacent BTSs in the overlap area between the two BTS where the handover take place.

This second case is the worst case, because when the train is located in the overlap area the received field-strength from the base stations will be the lowest. If a jammer is present in this area, its impact will be the strongest on the downlink path. Technical recommendations will be provided to mitigate the impact of jammer in the coming chapters.

4.2. Jamming location

In this paragraph we remind the study done in WP3 [2] about the impact of jammer. Two cases are considered: the jammer is located on-board the train and the jammer is located along the track.
According to the jammer transmit power and its location, we can obtain to the results 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 jammed
	Between two BTS	<= 1W	Negligible on the uplink downlink is jammed
		< 8W	Downlink + uplink is jammed
		> = 8 W	Downlink + uplink is jammed
Jamming along the track	Near to the BTS	<= 1W	Negligible on uplink and downlink
		> = 8 W	Downlink + uplink is jammed
	Between two BTS	<= 1W	Negligible on uplink and downlink
		> = 8 W	Downlink + uplink is off

Table 1: jamming effect according to train/jammer location

During its movements the train can be affected differently by the jammers. The impact of jammers will depend on the jammer power levels and the train distance from the BTS.

There is huge number of possibilities. Only the most relevant ones have considered.

4.3. 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.

The system shall also remain stable and false detection of jammer shall be limited.

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 jamming before the deterioration of the link and the total loss of communication.

Previous study made on the communication resilience leads to the results presented on Table 2**Erreur ! Source du renvoi introuvable.**.

Table 2: Evaluation of the communication quality

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

To dimension the detections system, it is necessary to define threshold for communication quality. When the communication quality is below the threshold, actions will be performed to restore a minimum level of communication quality.

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

4.4. Lines categories

Another 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.

Table 3: Lines categories definition

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)

Actually, the presence of jamming and the radio communication loss of the train 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 communication loss like the Urban Railways [3].

4.5. Communication technologies for the reconfiguration process

This section describes the alternative communication technology that can be used as a backup solution in case of jammer detection

The deliverable [4] presents an initial study of the next generation of communication systems. NGTC project carried out an initial research about the different radio-communication solution for the GSM-R system.

Because Railway communication shall have a high level of availability,
In case of jammer detection, it makes sense to consider switching to backup radio link based on another technology

However, there are conditions: the backup radio link shall meet the EIRENE requirements and this shall be transparent to the operator as far as it can be.

Based on these two constraints, different radio technologies will be analysed to evaluate their adequacy to railway application.

Table 4: Radio technology feasibility.

	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 4 presents the different radio technology alternatives that can be considered as candidate to be used in case of GSM-R failure. For each radio technology, different criteria are analysed and a solution for each kind of line is proposed.

One important parameter that is considered for the analysis and selection of radio technology alternatives is their operating frequency.

It makes sense to avoid shifting to a backup radio link based on a radio technology that can also be affected by the jammers.

For this purpose, the characteristics of typical jammer available on the market are listed in the next table. (Also listed in the previous study [5]).

Table 5: Jammer characteristics.

Frequency interference	
iDEN – CDMA - GSM	845 -975 MHz
DCS - PHS	1785 – 2000 MHz
3G 2110	2110 – 2170 MHz
WiFi – Bluetooth	2400 – 2485 MHz
Radiation range 10 - 20 meters	
Power interference 1200 mW	

Table 5 shows that radio technology operating in frequency bands below 2.5 GHz are not good candidate as backup solutions.
Radio technology operating in 3 Ghz and 5 GHz frequency bands will be better candidate as backup solutions.

Radio technology based on WLAN (G5 / 802.11p) operating in 5 GHz frequency bands can be considered for urban rail. LTE TDD radio technology operating in 3.5 GHz and 5.9 GHz frequency bands can be considered for main line and urban rail. The SATCOM in L- and S-bands can be considered for the main line.

The alternative Radio technology shall meet the railway EIRENE requirements for the main line solution.

In the next section main performance requirements ensured by the GSM-R are presented.

4.5.1. Network performance requirement

During the process of moving from one EIRENE network to another, the system must minimize the inconvenience for the railway system.
The alternative radio technology shall meet the EIRENE requirements and shall be in conformance with:

- Network requirements;
- Network configuration;
- Mobile equipment specification;
- Controller equipment specifications;
- Functional numbering and location dependent addressing;
- Subscriber management;
- Text messaging;
- Railway emergency calls;
- Shunting mode;
- Direct mode.

The aim is to provide a consistent level of service based on the quality requirements of GSM-R presented in Table 6 [6].

Table 6: Call setup times defined by EIRENE.

Call type	Call setup time
Railway emergency call	≤ 1s
Mobile-to-mobile urgent group call	≤ 2s
Group calls between drivers in the same area	< 5s
All low priority calls	< 10s
All operational mobile-to-fixed calls not covered by the above	<5s
All operational fixed-to-mobile calls not covered by the above	< 7s

All operational mobile-to-mobile calls not covered by the above	<10s

As for the GSM-R, the required call set-up times shall be achieved in 95% of the cases, where 99% of the cases shall not be more than 1.5 times.

In the same way, ETCS communication requirements shall be compliant to UNISIG SUBSET-093. The QoS requirements are currently established in case of ETCS over GPRS (Table 7)

Table 7: Summary of QoS requirements (ETCS over GPRS)

QoS Parameter	Value
GPRS attach delay	≤ 5s (99%)
PDP context activation delay	≤ 3s (99%)
ETCS DNS lookup delay	≤ 3s (99%).
Transaction transfer delay • 100 octet (OBU originated) • 320 octet (RBC originated) • 560 octet (RBC originated)	 ≤ 1.3s (95%), ≤ 2.6s (99%) ≤ 2.0s (95%), ≤ 3.0s (99%) ≤ 2.5s (95%), ≤ 3.5s (99%)

4.5.2. Radio Coverage requirement

Generally, the following are the minimum required planning data for GSM-R radio network planning [6]:

- Minimum receive level of –90 dBm for 95% location/time probability at 100m (ETCS 97%, Shunting 99 %)
- Mobile station output power 2W (33 dBm) or 8W (39 dBm)
- Mobile station RX sensitivity –102 dBm
- C/I_C 20 dB co-channel interference
- C/I_A 5 dB adjacent channel interference
- Antenna gain (typically 12 to 17 dB) and height above ground
- Losses in feeder cable and other components
- Fading margin (slow, fast)

These radio planning specifications have been defined to guarantee the QoS requirements listed in the previous table.

For each alternative radio technology, such radio planning specification shall be defined to meet the requirements listed in Table 6 & Table 7.

5. SECRET recommendation template reminder

In this document we will use the TecRec standard template defined in D5.1 [1]. From this previous document we present in this section a short reminder of the main topics that defines the template. The different sections presented below are 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…).

6. Operational recommendations

6.1. Increasing temporarily ground BTS output power : Secret_WP3_TecRec_001

6.1.1. Definition

This technical recommendation implies the introduction of TecRec 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.

Topic	Increasing temporarily ground BTS output power level (8 to 80 W).
Description	Temporary increase of ground BTS output power level (10 dB) when a jamming situation is detected inside the train. This increases 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).
Type	Standard update
Involved bodies	ETSI

The recommendation considers environment profile when:

- Jammer is on board the train
- Jammer power from 1 w to 8 w.

6.1.2. Technical requirements

The Table 8 lists the maximum output power levels allowed by the ETSI standard for a BTS [7].

These levels represent the base station transmitter maximum output power, measured at the RF connector of the BSS transmitter.

Table 8: 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

The output power presented in Table 8 from the ETSI standard varies from 2.5 w to 320 w. So it's possible to increase the power level to 80 w or more.
For example, for GSM 900 the Max EIRP of 50 W matches MS class 2 of max peak output power 8 W [8].
According to this table we can conclude about the conformance of this TecRec. This implies the possibility to increase the BTS output power level in case of jamming detection to increase the *SJR*.

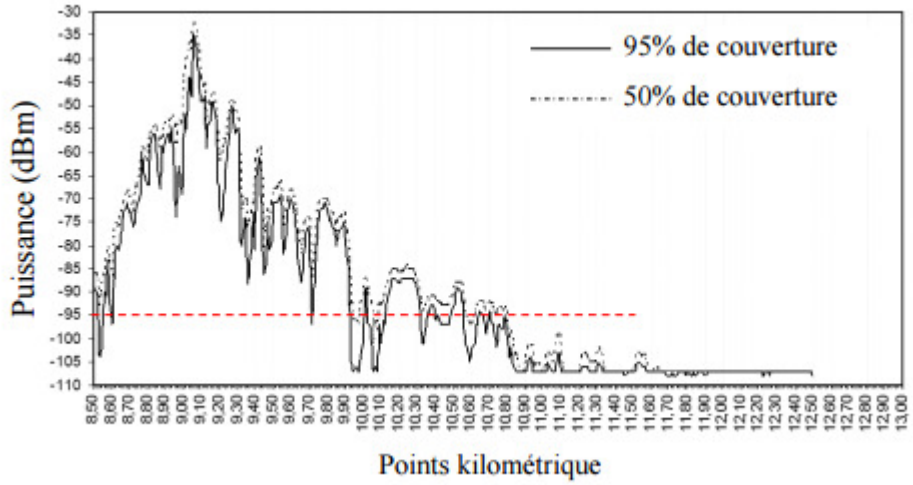


Figure 2: Downlink evolution power according to the BTS distance.

For example, Figure 2 presents the field-strength received from the BTS during the movements of the train. It can be observed that at a certain distance the minimum level requirement of -95 dBm is achieved. The EIRENE specification accepts that the received level is below -95 dBm maximum 5 % of the time and space.
In case of presence of jammer in area where the received field strength is below -95 dBm, the communication will be disturbed.
In order to minimize the impact of the jammer the TecRec_001 proposes to increase temporarily the ground BTS output power level.

Therefore the system has to include requirements for:

- Health recommendations
- Maximum power supported
- Field strength measurements (radiated emission)
- Cell dimensioning
- Antenna patterns
- Maximum power level supported by the mobile station receiver.

6.2. Increasing temporarily train MS output power : SECRET_WP3_TecRec_002

6.2.1. Definition

This TecRec is similar to the previous one; the difference is that one proposes to act on the mobile station. In the same way this TecRec 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 power from 1 w to 8 w.

Topic	Increasing temporarily train MS output power level (8 to 80 W).
Description	Temporary increase of train MS output power level when a jamming situation is detected on the ground side. This increases the RF signal level received by the BTS and the Signal to jammer ratio. This necessitates to manage and mitigate the impact of the corresponding correlated increase power delivered to the neighbouring cells (C/I level)
Type	Standard update

Involved bodies	ETSI

6.2.2. Technical requirements

The Table 9 lists the maximum output power level allowed by the ETSI standard to a Mobile station [7].

Therefore the system has to include requirements for:

- Maximum power supported
- Field strength measurements (radiated emission)
- Cell dimensioning
- Antenna patterns

Table 9: 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)

The maximum output power proposed by the ETSI standard for MS is fixed at 8 w, which is the maximum power actually provided by the MS and so in contradiction with the proposed TecRec. This proposal is not conform to the actual standard.

6.3. Switching of cab radio : SECRET_WP3_TecRec_003

6.3.1. Definition

This recommendation takes into consideration the length of the train and its position from 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.

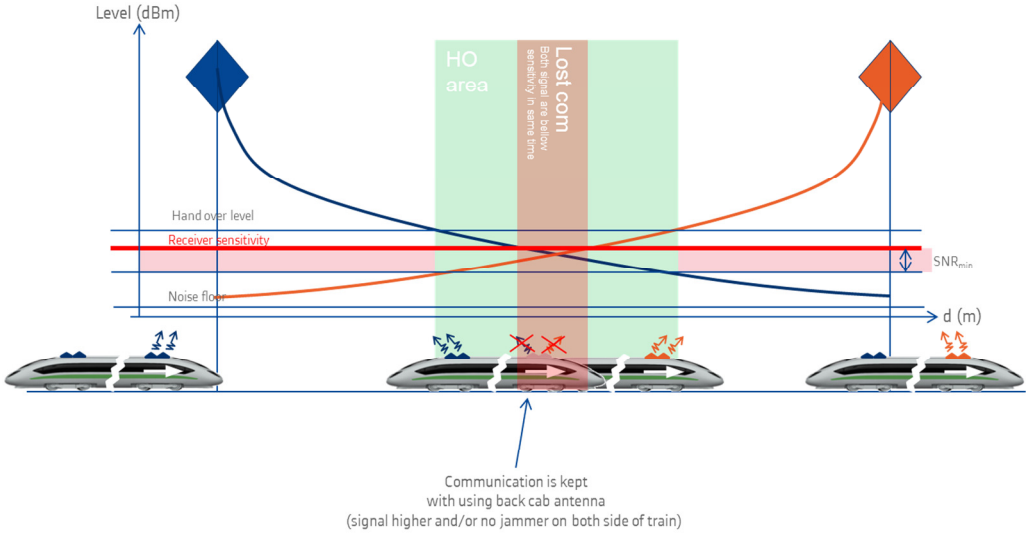


Figure 3 : SECRET_WP3_TecRec_003: Use back cab alternative

Topic	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).
Description	The train received jamming powers are unlikely to be the same at both front and rear train antennas. Therefore, switching from front to rear cab radio equipment could improve, inside the train, the signal to jammer ratio. This engineering rule could already be operational for handover operations.
Type	Engineering rules
Involved bodies	Railway industry and operators

6.3.2. Technical requirements

The use of the two train antenna represents a good solution to minimize the effect of the jammer on the handover process position. This recommendation requires signal from the two antennas alternatively. There is no conformance problem as the first one doesn't interfere with the second one. However it requires that a wired communication network is available along the train consists (not applicable to freight trains).

Therefore the system has to include requirements for:

- Electromagnetic Compatibility Requirements
- Radiated emission
- Cell dimensioning

6.4. Electronically switching on a quarter wave reflector : SECRET_WP3_TecRec_005

6.4.1. Definition

Likewise the previous TecRec this new recommendation propose to change the used antenna to avoid the effect of the jammer. In this case we propose to use an "active notch" antenna which is actively modifying its radiation pattern to "isolate" the jammer

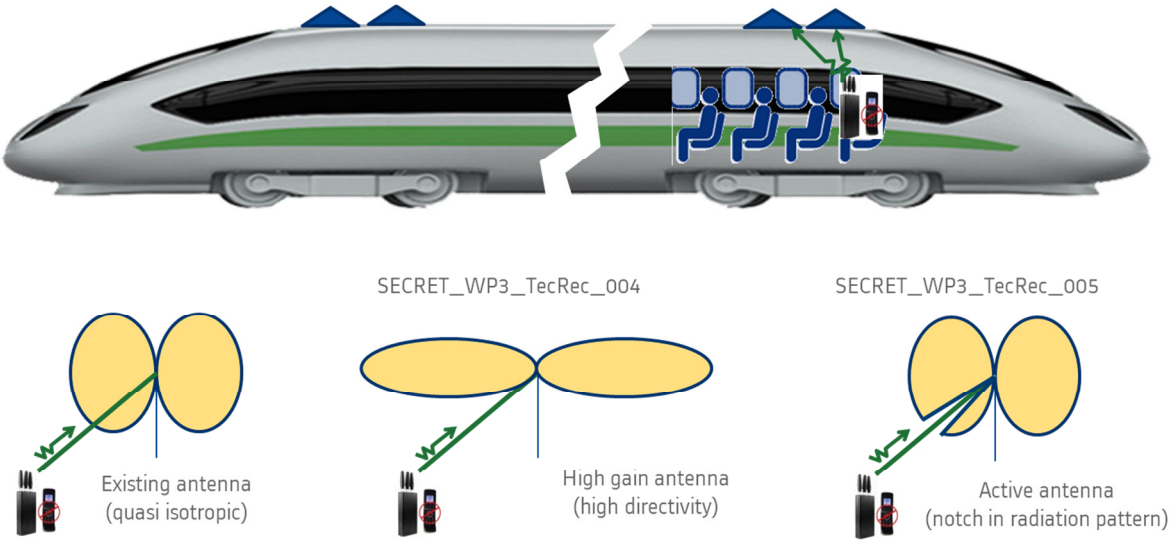


Figure 4: SECRET_WP3_TecRec_004-005: Lower aggression strength

The recommendation considers environment profile when:

- Jammer is located on board the train.
- Jammer power from 1 w to 8 w.
-

Topic	Electronically switching on a quarter wave reflector behind an existing front or rear train antenna to reject an inside the train jamming signal.
Description	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.
Type	Engineering rules
Involved bodies	Railway industry and operators

6.4.2. Technical requirements

As presented in Figure 4, this TecRec needs jamming detection information to change characteristics of the GSM-R antenna. In this case we propose to use an “active notch” antenna which preserves the quasi-isotropic radiation pattern. This seems to be good proposal that satisfy the conformity of the railway standard.

Therefore the recommendation has to include requirements for:

- Electromagnetic Compatibility Requirements (emission/ immunity)
- Radiated emission Requirements
- Cell dimensioning and coverage
- Antenna pattern
- Channel use

6.5. Electronically switching on emergency BTSs : SECRET_WP3_TecRec_008

6.5.1. Definition

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

Topic	Electronically switching on emergency BTSs providing space diversity
Description	When jamming signal is detected, network is electronically switched from the initial configuration to the new one using the additional BTSs. This modifies the radio coverage level at the train and attenuates the SJR.
Type	Engineering rules
Involved bodies	Railway industry and operators

6.5.2. Technical requirements

The usage of this reconfigurable network consists of adding BTS antenna. These additional BTSs are placed near the initial ones and turned off until jamming disappears.

These supplementary BTSs shall be installed without interfering with the existing network configuration.
Cell configuration and frequency allocation shall be studied carefully in order to maintain the communication link.

Therefore the recommendation has to include requirements for:

- Electromagnetic Compatibility Requirements (emission/ immunity)
- Radiated emission Requirements
- Cell dimensioning and coverage
- BTS Configurations antenna pattern
- Frequency allocation and channel usage
- Receiver diversity
- Power supply options

6.6. Install AIR Repeater : SECRET_WP3_TecRec_010

6.6.1. Definition

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

Topic	Install AIR Repeater as solution to improve GSM-R coverage
Description	Use an air repeater when a jamming situation is detected inside the train. This 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.
Type	Engineering rules
Involved bodies	Railway industry and operators

6.6.1. Technical requirements

Solution for GSM-R coverage improvement with repeater is usually proposed [9] to ensure good network coverage at lower cost than BTS. These repeaters need to be certified and conform to standards for coverage and for EMC limits, taking in consideration the maximum output power supported by the environments (health recommendations) and BTS receiver levels [10] [11].

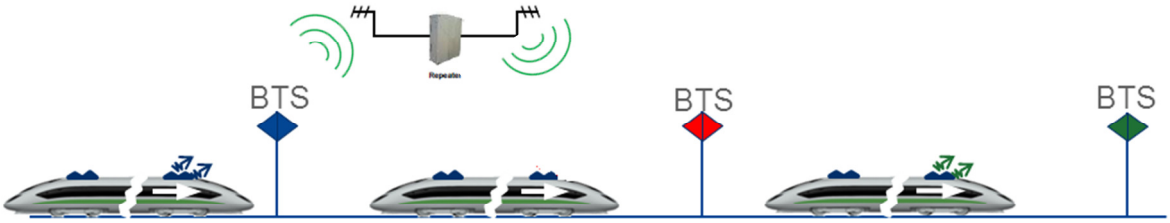


Figure 5 : SECRET_WP3_TecRec_010 repeater configuration

Installed along the track in order to improve power levels in handover area, they can minimize signal to jamming ratio and reduce impact of the jamming.

The ETSI requirements specify that the maximum repeater output power per carrier for the repeater will be limited by the number of carriers to be enhanced.
Based on the ETSI standard we propose the typical power level value of uplink and downlink for a repeater (Figure 6). Power level at the input of the repeater is approximated between -50 to -70 dBm [7].

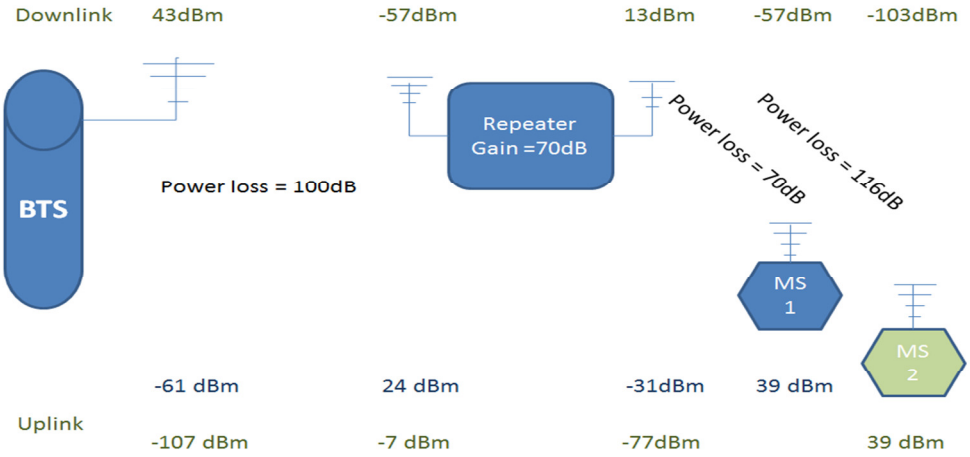


Figure 6 : Air repeater configuration and power for uplink and downlink.

The dimensioning shall consider the impact of signal to noise ratio degradation, and also the impact of delay introduced by repeaters. Signal to noise ratio degradation and delay can reduce cell range. For example an increase of delay of 8 microseconds can reduce the radio cell length at around 2.4 km. [7]

Therefore the recommendation has to include requirements for:

- Electromagnetic Compatibility Requirements (emission/ immunity)
- Radiated emission Requirements
- Cell dimensioning and coverage
- BTS Configurations and antenna pattern
- Frequency allocation and channel usage
- Receiver diversity
- Power supply options

7. Engineering recommendations

7.1. E-plane high front-to-back ratio directive antennas :

SECRET_WP3_TecRec_004

7.1.1. Definition

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.

Where the existing antenna have quasi-isotropic radiation pattern receiving Electromagnetic signal from everywhere, we propose to replace it by passive high gain antennas, which will provide a smaller coupling factor with the jammer.

Topic	Changing train antennas from E-plane isotropic antennas to E-plane high front-to-back ratio directive antennas.
Description	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.
Type	Engineering rules
Involved bodies	Railway industry and operators

7.1.2. Technical requirements

The Figure 4 presents the proposed antenna compared with the existing one. As we can observe, the limitation of this recommendation remains the directivity of the antenna. According to the railway track and the position of the different BTSs, this can induce reception problems. The BTSs and the antennas are placed in order to get a maximum coverage with good transmission levels, which cannot be satisfied by the new antennas.

Therefore the recommendation has to include requirements for:

- Electromagnetic Compatibility Requirements (emission/ immunity)
- Radiated emission Requirements
- Cell dimensioning
- Antenna pattern
- Adjacent channel leakage power

7.2. antenna with managed diagram polarity : SECRET_WP3_TecRec_006

7.2.1. Definition

This TecRec is a combination of the two previous ones. The principal interest is to use an intelligent antenna. This antenna rejects any suspect signal. The diagram of the antenna is constantly moving to identify the jamming signal and reject it.

Topic	Use a special antenna with managed diagram polarity
Description	The aim of this antenna is to reject any suspect signal. The diagram of the antenna is constantly moving to identify the jamming signal and reject it.
Type	Engineering rules
Involved bodies	Railway industry and operators

7.2.2. Technical requirements

In this case we propose to use an antenna which changes its radiation pattern continuously to identify jamming signals and reject them.

It is interesting to use a radio antenna that configures its radiation diagram (space or lobes or beams …) [12] . It allows a base station antenna switching their radio beams on the network. Moved to be oriented in space, its graph Electromagnetic radiation is oriented in the desired direction.

These smart antennas offer the possibility to increase the capacity of systems, reduce interference in the downlink and in the uplink. Using as base station antenna it offers the possibility of forming antenna pattern rejection in the direction of interference reception signals.

This seems to be a good proposal that satisfy the conformity of the railway standard.

Therefore the recommendation has to include requirements for:

- Electromagnetic Compatibility Requirements (emission/ immunity)
- Radiated emission Requirements
- Cell dimensioning and coverage
- Antenna pattern
- Channel use
-

7.3. Install additional BTSs in hazardous area : SECRET_WP3_TecRec_007

7.3.1. Definition

This TecRec 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 can be higher than 5 km..

Topic	Install additional BTSs in hazardous area.
Description	In hazardous area when the coverage level is very low we can install additional BTSs. This modify the BTS radiation diagram and increase the transmission Levels. The impact of the jammer decrease. The impact on handover should be investigated.
Type	Engineering rules
Involved bodies	Railway industry and operators

7.3.2. Technical requirements

This solution involves the study of the propagation diagram of these additional BTSs. The Figure 7 presents the propagation diagram of supplementary antenna with the presence of jammer.

In the specific area this TecRec presents a good solution against jamming effect with conformance to ETSI and railway standard.

We start our simulation by an ideal case where BTSs are spaced at maximum of 6.2 Km

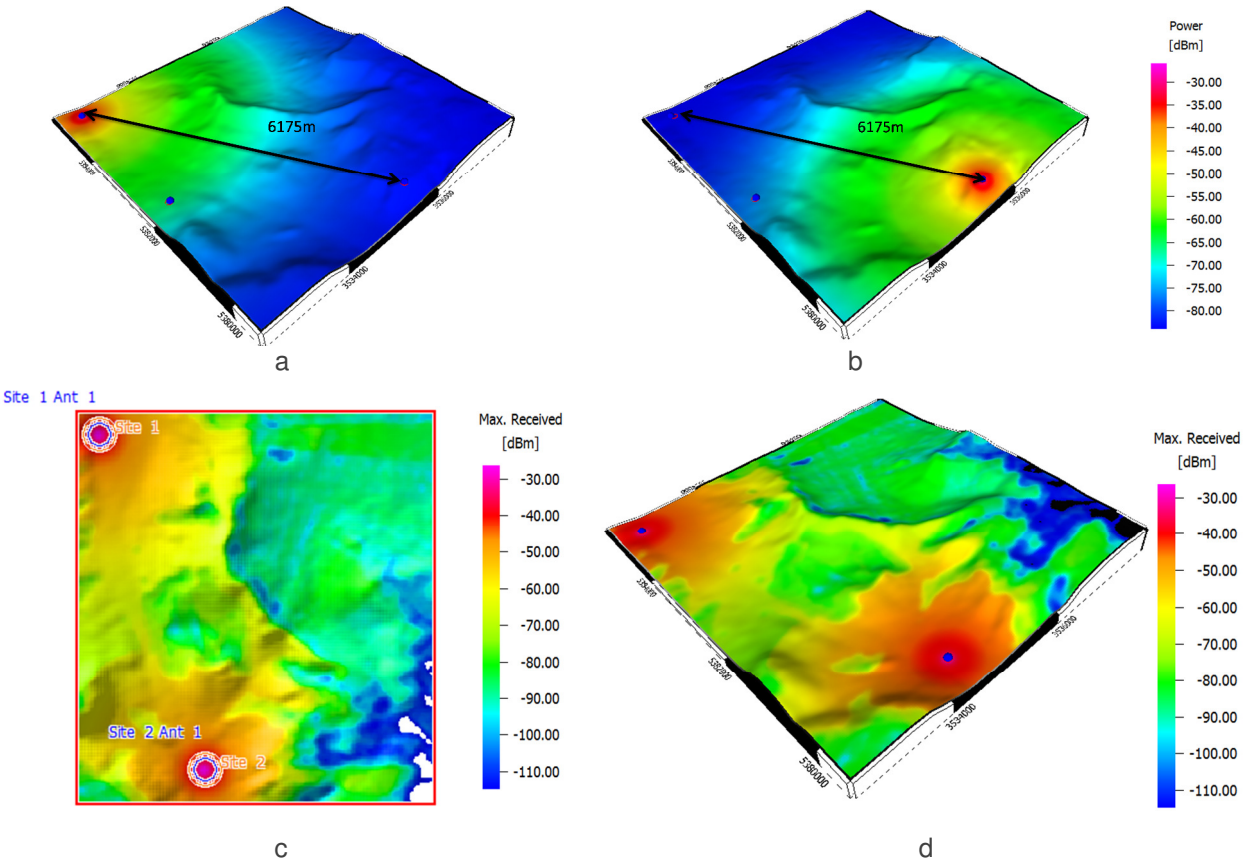


Figure 7 : Propagation diagram in hilly terrain for two adjacent BTS.

We present in this section the propagation diagram in rural area (hilly terrain). In this example, two BTSs are spaced by 6175 m and transmitting at a power level of 8 W. Their antennas are installed at 25 m above the ground.

The Figure 7 a and b show the 3d representation of the area with the corresponding field-strength radiated by BTS1 and BTS2.

The Figure 7 c and Figure 7 d, show the field-strength received by a Train antenna when the train is moving.

Let us introduce EM jamming in to the area.

On Figure 8 a, we can observe the diagram level of an EM jammer placed between the two BTS with an output power of 1 W and installed at 5 m about the floor level .

Figure 8 b presents the field-strength received when the jammer is present between the two BTSs.

In order to identify the contribution of each one (BTS1, BTS2 and Jammer) at the train antenna we represent on Figure 8 c and Figure 8 d the coverage of BTS1, BTS2 and the Jammer.

The coverage of BTS1, BTS2 and the jammer are shown respectively in green, red and blue.

It is clear that when a train arrives near the jammer its GSMR receiver will be strongly disturbed.
As shown by the WP3 results, (cf Table 10) a *SJR* of 6 dB could have an important effect on the communication.

Table 10: *SJR* ratio and consequences

P_GSM-R (dBm)	P_JAM (dBm)	BER_*f1* *Pure sinus jammer*	BER *FM mod* *75 kHz dev* *jammer*

-38	-36	Loss of comm.	No connection
-38	-37	12,6	No connection
-38	-38	5,6	No connection
-38	-40	2,1	14,7
-38	-42	0,8	7,8
-38	-44	0,2	2,7
-38	-46	0,1	0,6
-38	-48	0,06	0,2
-38	-50	0,02	0,04

The addition of a BTS between BTS1 and BTS2 will contribute to reduce significantly the impact of a jammer in this area of the line

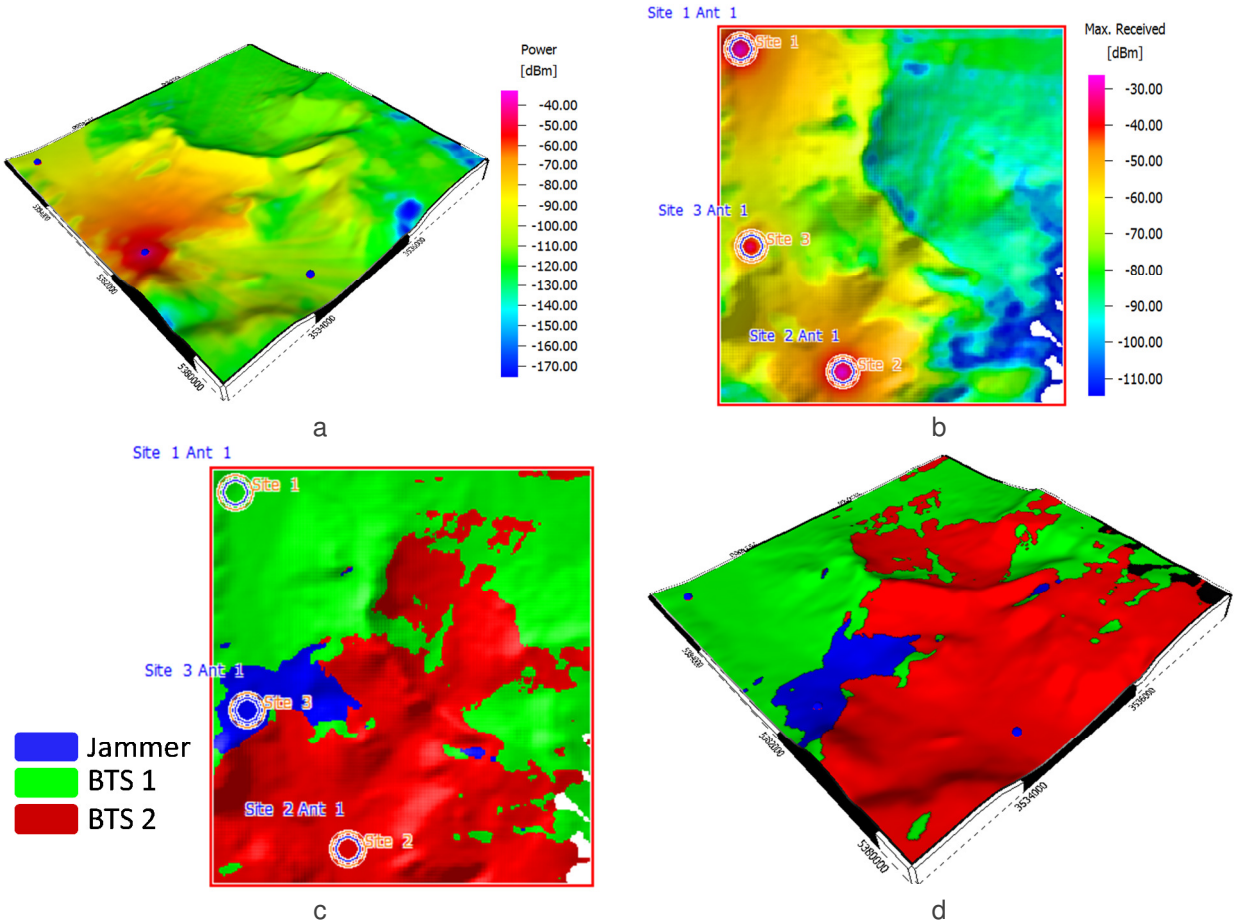


Figure 8 : Jamming power received level and maximum cell covering in hilly terrain in presence of 1 W jamming.

The TecRec proposes to add new BTSs in order to improve the quality of the coverage, Figure 9 a and Figure 9 b shows the field-strength received when the jammer is present with an improved Radio coverage. The positive impact of the addition of a BTS can be observed: the quality of the coverage has been improved and the contribution of the jammer is reduced.

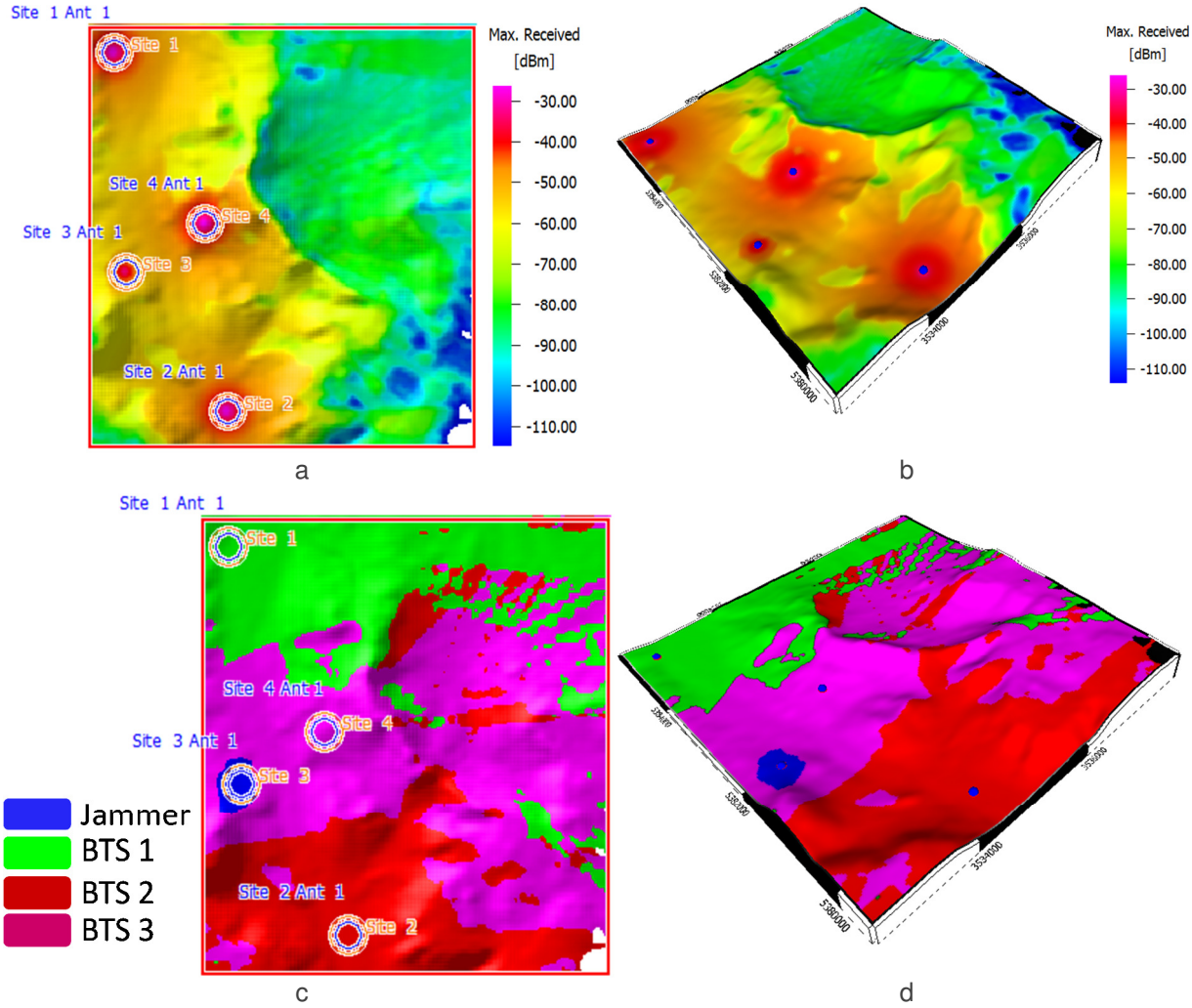
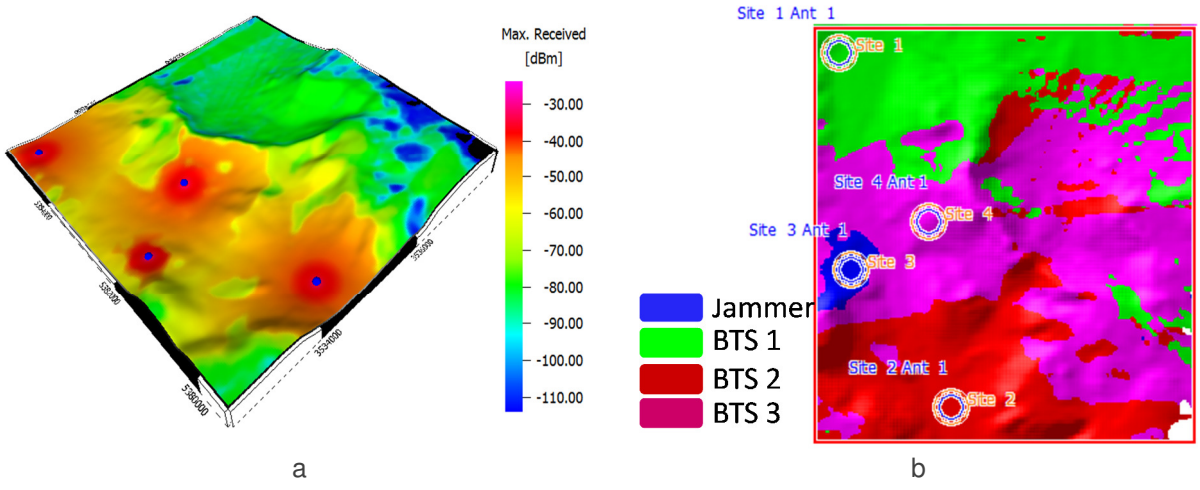
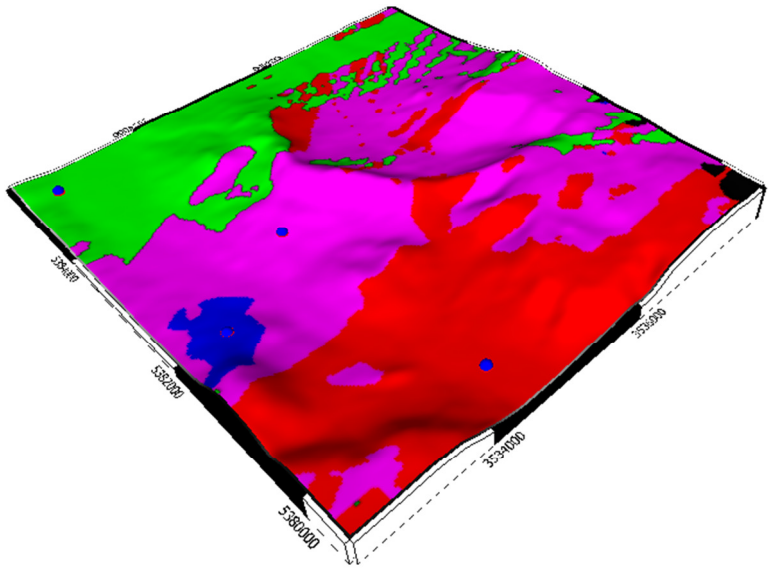


Figure 9 : 1 W Jamming power received level and maximum cell covering in hilly terrain with additional BTS.

On the next figure, we consider the same environments but with a jammer radiating a higher power of 8W.





c

Figure 10 : 8 W Jamming power received level and maximum cell covering in hilly terrain with additional BTS.

On Figure 10 a, it can be observed that the jammer in this case has an impact in the three Radio Cells.

The area disturbed by the Jammer is more important. The Train communication will be impacted on a longer distance.

To minimize the impact of the 8W Jammer, an extra BTS can also be added. It means that the area will be covered by 3 BTS instead of 2.

Figure 10 b shows that the addition of the third BTS to cover the area reduces the impact of the jammer while it remains strong enough to impact train communications.

Therefore the recommendation has to include requirements for:

- Electromagnetic Compatibility Requirements (emission/ immunity)
- Radiated emission Requirements
- Cell dimensioning and coverage
- BTS Configurations antenna pattern
- Frequency allocation and channel usage
- Receiver diversity
- Power supply options

7.4. Create microcells at handover overlap area: SECRET_WP3_TecRec_009

7.4.1. Definition

As for the previous TecRec the purpose of this recommendation is to improve the radio coverage. We propose to add a micro BTS in the handover overlap area.

This micro BTS can be connected to antennas installed at lower height above the ground than normal BTS. These types of BTS are less expensive than normal BTS.

Micro BTS will implement micro cells to solve a particular problem.

Topic	Create microcells with additional micro BTS at handover overlap area
Description	Creating micro BTS cells by adding smaller BTS to minimize the impact of a jammer in the Handover area

Type	Engineering rules
Involved bodies	Railway industry and operators

7.4.2. Technical requirements

The mobile industry has conducted to the emergence of “small cells” as a solution to help operators to optimize their network architecture and face the rapidly growing demand for coverage and capacity. Small cells or micro cells can also be a solution to face the problem of interferences and jamming.

Basically in the GSM standard, as presented in Figure 11 we can find different sizes of cells called hierarchical cell structure and characterised as picocells, microcells, macrocells.

Generally, micro cell BTS can be smaller than the original BTS and are a cheaper solution. A good study has been made based upon the Minimum Coupling Loss expected between MS and the microcell BTS to choose the appropriate implantation.

A specification was made based on a frequency spacing of 6 MHz between the microcell channels and the channels used by any other cell in the vicinity when choosing to use the microcell BTS [8].

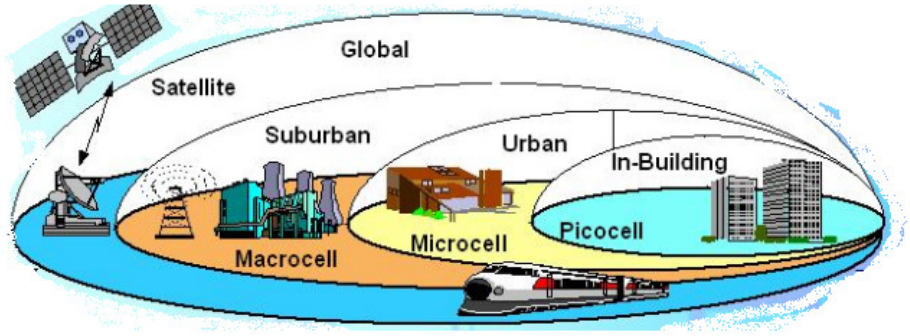


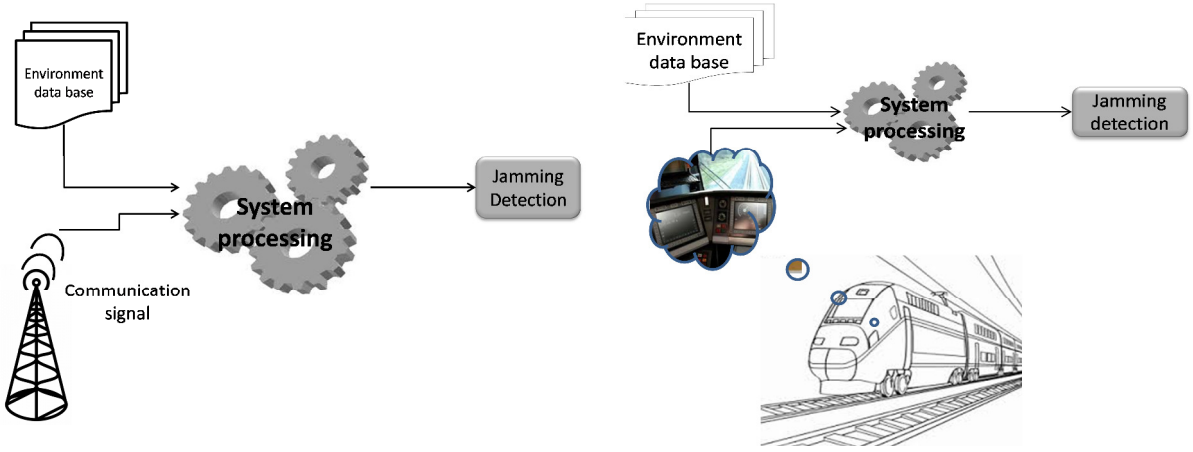
Figure 11 : Hierarchical cell structure

Therefore the recommendation has to include requirements for:

- Electromagnetic Compatibility Requirements (emission/ immunity)
- Radiated emission Requirements
- Cell dimensioning and coverage
- BTS Configurations antenna pattern
- Frequency allocation and channel usage
- Receiver diversity
- Power supply options

8. Detection recommendations

The recommendations presented in the following section focus on the detection system developed in WP3. For both the two detection methods we shall propose an implementation TecRec based on the diagram in Figure 12. The important step stays in populating the environmental data base. This represent the first entry of the detector process recorded when no jamming is present. This data base represents both of the IQ data and spectral data and includes the different environment crossed by the train.



a : along the track b : onboard the train

Figure 12 : Detection process.

8.1. characterization of the EM rail environment : SECRET_WP3_TecRec_011

8.1.1. Definition

The recommendation presented here takes in consideration the detection system itself. The interest is based on the characterization of the EM environment representing the system in its nominal condition.

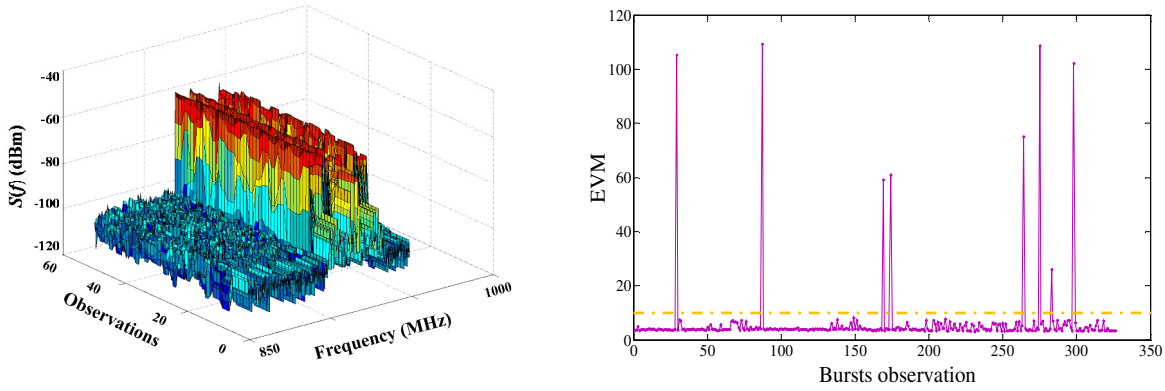
The detection methods will then use this characterization as an input to decide if there is a jammer present or not.

Topic	characterization of the EM rail environment, segmented into trains, stations and track
Description	In order to provide a detection system able to sensitively detect a jammer, we can specify for the different methods several environment representing the railway network
Type	Engineering rules
Involved bodies	Railway industry and operators

8.1.2. Technical requirements

Based on the detection methods provided by the WP3, the first step shall consist in sampling and saving the radio-electric environment in nominal conditions. All these observations shall be stored in an environmental database in relation with train location and additional information such as antennas type and its radiating diagram.

The second step consists to monitor continuously the environment. Different detection method can be used based on IQ domain or on spectrum domain as shown on Figure 13. Jammer will be detected by comparing the continuous real time recording with initial recording corresponding to nominal condition.



a b

Figure 13 : Environment data base, a: spectrum domain, b: IQ domain.

8.2. Deploy sensors network : SECRET_WP3_TecRec_012

8.2.1. Definition

The recommendation presented here takes in consideration the detection system. Based on the output of WP3 we propose to implement sensors network along the track to detect jamming signal and inform the control centres.

These sensor networks are composed of antennas connected to a control unit, which will perform spectrum analysis and send alarms when jamming conditions are detected. They can be implemented directly on the BTSs.

Topic	Deploy sensors network along the track to detect attacks.
Description	Additional sensors can be deployed along the track to detect the presence of jammer. These sensors are connected to the control center. Information provided by the sensor is used to define actions: locate jammers, reroute temporarily the trains on another route.
Type	Engineering rules
Involved bodies	Railway industry and operators

8.2.2. Technical requirements

Coming before the appearance of jamming, this solution proposes to continuously monitor the environment to detect the presence of jammer and then inform the traffic manager in the control center and trains.
Based on passive antennas to observe the environment, this recommendation has to be in compliance with requirements for:

- Electromagnetic Compatibility Requirements (emission/ immunity)
- Radiated emission Requirements
- Antenna pattern
- Frequency allocation and channel usage
- Power supply options

8.3. Integrate a monitoring system based on spectrum: SECRET_WP3_TecRec_013

8.3.1. Definition

This recommendation concerns a detection method based on spectrum analysis defined in the WP3. The proposed detector based on this method analyses directly the signals received from the antennas of the BTS or cab radio to identify the presence of jammer.

Topic	Integrate a monitoring system based on spectrum analysis in onboard radio transceiver and in BTS.
Description	A Detector performs a spectral analysis of signals received from the BTS antenna or onboard antenna to provide jamming information.
Type	Engineering rules
Involved bodies	Railway industry and operators

8.3.2. Technical requirements

This approach requires:

- the capture of the signal at the I/Q down-converter to perform spectral analysis of the signal received from the BTS antenna or on board antenna.
- the implementation of signal processing algorithm to obtain the power spectral density of the received signal
- a control unit that will receive the information (power spectral density) from each sensor.

Each sensor will be composed of an antenna connected to processing unit.

This recommendation has to be in compliance with requirements for:

- Electromagnetic Compatibility Requirements (emission/ immunity)
- Radiated emission Requirements

This recommendation shall also specify the location of the detectors. Depending from the results of wp3, the method for spectral analysis may be appropriate to monitor the station where several communication systems must be operational.

8.4. Implementation of EVM jammer detector : SECRET_WP3_TecRec_014

8.4.1. Definition

This recommendation is based on the detection methods based on the measure of the Error Vector Magnitude (EVM);
GSM-R receiver are based on an I/Q demodulator. The EVM can be obtained by measuring I/Q distortions. 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.
In normal operation, the train driver should not be immediately involved, especially in case of false alarms, this would be impracticable and even unsafe.
A train alarm should be sent to the control centre using degraded channel (when the communication is still usable) or alternative communication channel if available;
The process needs to be conforming to the ETSI standard. For more details about the detector implementation refer to the D4.4 on Cab-radio architecture.

Topic	Implementation of EVM jammer detector in both the onboard equipment and the BTS
Description	Use the existing system to incorporate an EVM indicator. This solution allows the detection of jamming and to inform the control centre and, when confirmed, the train driver to react in case of attacks. The process need to be conforming to the ETSI

	standard.
Type	Engineering rules
Involved bodies	Railway industry and operators

8.4.2. Technical requirements

This recommendation implies the modification of the GSM-R receivers. Signal processing algorithm shall be added in the receiver to compute the EVM. High EVM shall be used to generate alarms that will be sent to the control centre and, when confirmed, to the train driver. This recommendation implies additional process unit to read the EVM and provide jamming information. It has to be in compliance with ETSI standard.
From the different results of the WP3, we can adapt detectors and deploy them according to their efficiency. This means that for the different locations we can select the best detector to be deployed. For example, The IQ method can be adapted on the train where detection must be very fast (before the interruption of the connection) to switch to a degraded mode of less restrictive movement as an emergency stop.

9. Implementation of recommendations

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

Normally, if the driver has not received movement authorization at the expected time, and has no information about the reason, he shall inform according to the ERTMS specifications the operation centre about the situation.

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

In case of efficient jamming, a train cannot receive movement's authorization and then will require a secondary communication technology.

Some technologies were selected assuming that they can meet the railway requirements and maintain the communication established. Otherwise, alternative communication technologies 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.

When train sensors detect jamming, the preconized procedure is described in the flowchart of Figure 14.

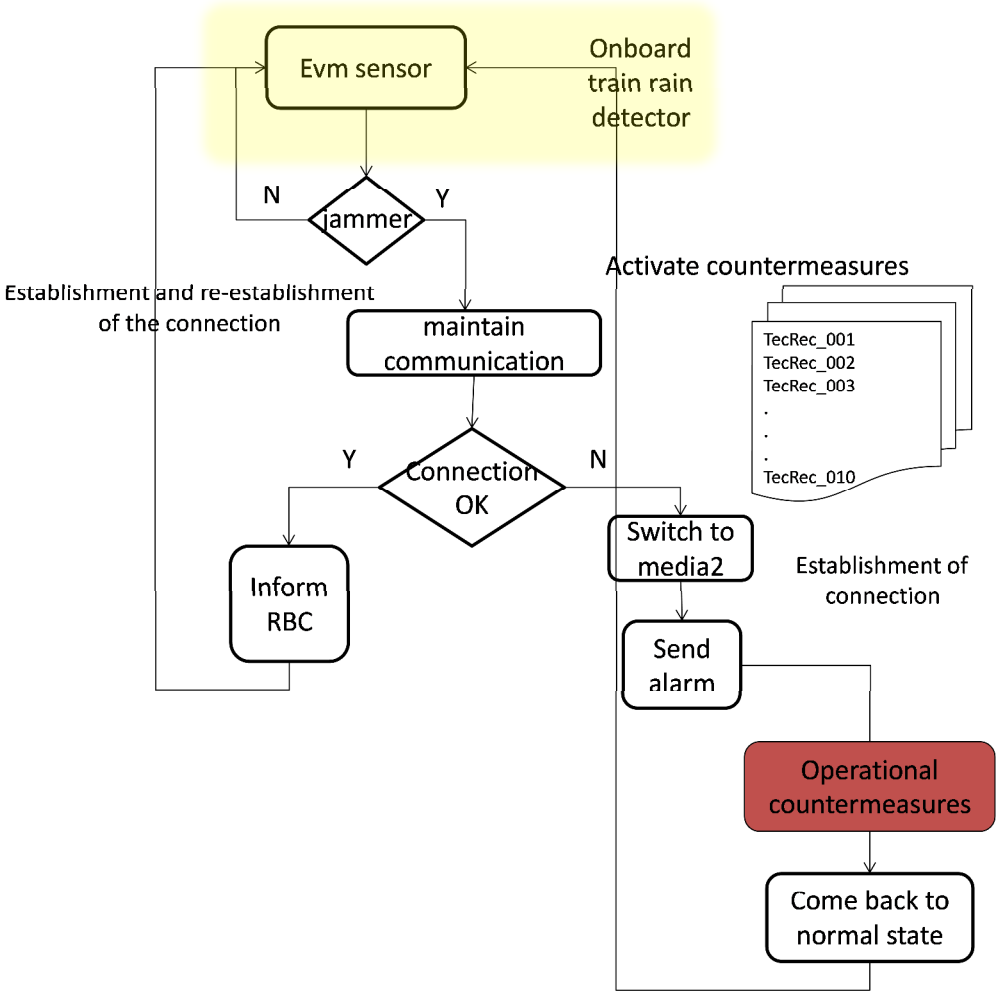


Figure 14 : Jamming onboard train countermeasure procedure flowchart.

The process is as following: when a jammer is detected, the communication is maintained so that an alarm can be sent to the RBC by the train and after this one switch to the backup radio link based on the alternative technology.

For example, when a jammer is detected on the track side between two adjacent BTSs with a power level that exceeds 8 W in 'line category 1', the backup radio link can be based on LTE TDD technology operating in the 3GHz frequency band or 5 GHz , or if not available the SATCOM can be considered.

The TecRec can be classified in two different categories:

1. The permanent recommendation which should be applied permanently in order to improve the infrastructure and prevent from jamming attacks
2. The temporary recommendations, which should be applied temporarily in order to mitigate the jammer conditions.

The list below summarizes these recommendations in the two categories.

❖ Permanent recommendations

- SECRET_WP3_TecRec_004 : Changing train antennas from E-plane isotropic antennas to E-plane high front-to-back ratio directive antennas.
- SECRET_WP3_TecRec_006 : Use a special antenna with managed diagram polarity.
- SECRET_WP3_TecRec_007: Install additional BTSs in hazardous area where coverage can be easily affected by jamming.
- SECRET_WP3_TecRec_009: Create microcells by additional BTS at the position of the handover.

- SECRET_WP3_TecRec_011: Characterization of the EM rail environment, segmented into trains, stations, track
- SECRET_WP3_TecRec_012: Deploy sensors network over the whole communications network to detect attacks.
- SECRET_WP3_TecRec_013: Integrate a monitoring system based on the spectrum analysis on the cab antenna and on the BTS
- SECRET_WP3_TecRec_014: Implementation of EVM jammer detector on both the onboard system equipment and on the radio control centers equipment.

❖ Temporary recommendations

- SECRET_WP3_TecRec_001: Increasing temporarily ground BTS output power level (8 to 80W).
- SECRET_WP3_TecRec_002: Increasing temporarily train MS output power level (8 to 80 W).
- SECRET_WP3_TecRec_003: 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).
- SECRET_WP3_TecRec_005: Electronically switching on a quarter wave reflector behind an existing front or rear train antenna to reject an inside the train jamming signal.
- SECRET_WP3_TecRec_008: Electronically switching on emergency BTSs providing space diversity.
- SECRET_WP3_TecRec_010: Install AIR Repeater as solution for GSM-R coverage.

Technical but also non-technical criteria, like cost, efficiency,… will constraint the implementation of all recommendations. The technical criteria have to be assessed according the environment profile described in chapter 4.

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

To allow such analysis, other recommendations established in WP1, WP2 and WP3 should be included.

In the following and for sake of simplicity, we will only consider the additional recommendation SECRET_WP4_TecRec_008, where an alternative radio link communication is established over a different radio frequency band not disturbed by jamming.

Starting from the detection of jammer on-board or trackside, two decision trees have been built as illustration of strategies that could be used for the activation of temporary recommendations.

Such decision trees are proposed in the following paragraphs.

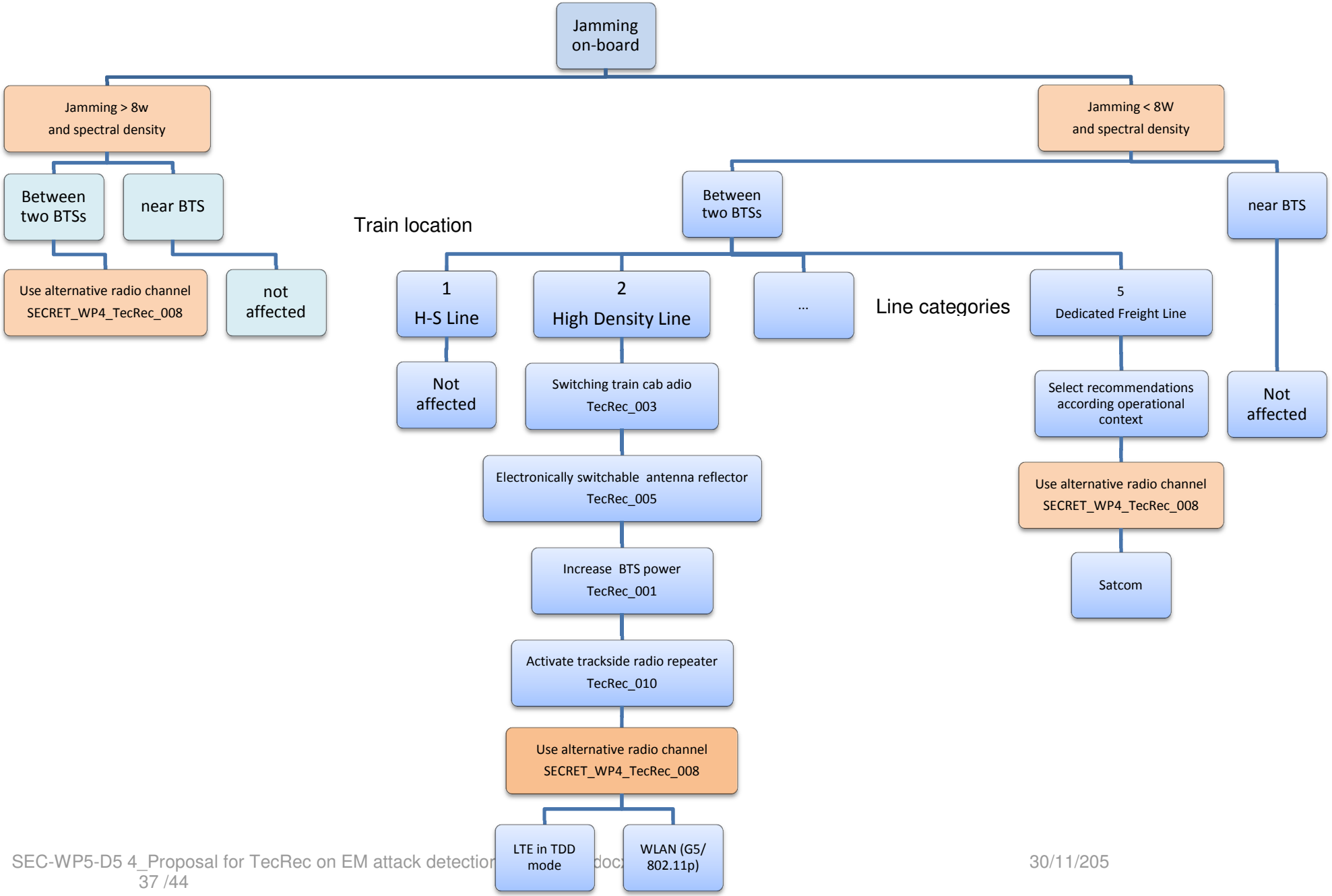
9.1. Decision tree in case of jammer detection on-board the train

When a jammer is detected onboard the train, 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

The possible recommendations are proposed for each step in the sequence.

The decision tree presented below in an example describing the process and proposed recommendations. It should be further developed in the future.


Jamming on-board
Jamming > 8w and spectral density
Jamming < 8W and spectral density
Between two BTSs
near BTS
Between two BTSs
near BTS
Use alternative radio channel SECRET_WP4_TecRec_008
not affected
Train location
1 H-S Line
2 High Density Line
...
Line categories
5 Dedicated Freight Line
Not affected
Switching train cab adio TecRec_003
Select recommendations according operational context
Not affected
Electronically switchable antenna reflector TecRec_005
Use alternative radio channel SECRET_WP4_TecRec_008
Increase BTS power TecRec_001
Satcom
Activate trackside radio repeater TecRec_010
Use alternative radio channel SECRET_WP4_TecRec_008
LTE in TDD mode
WLAN (G5/ 802.11p)

9.2. Decision tree in case of jammer detection along the track

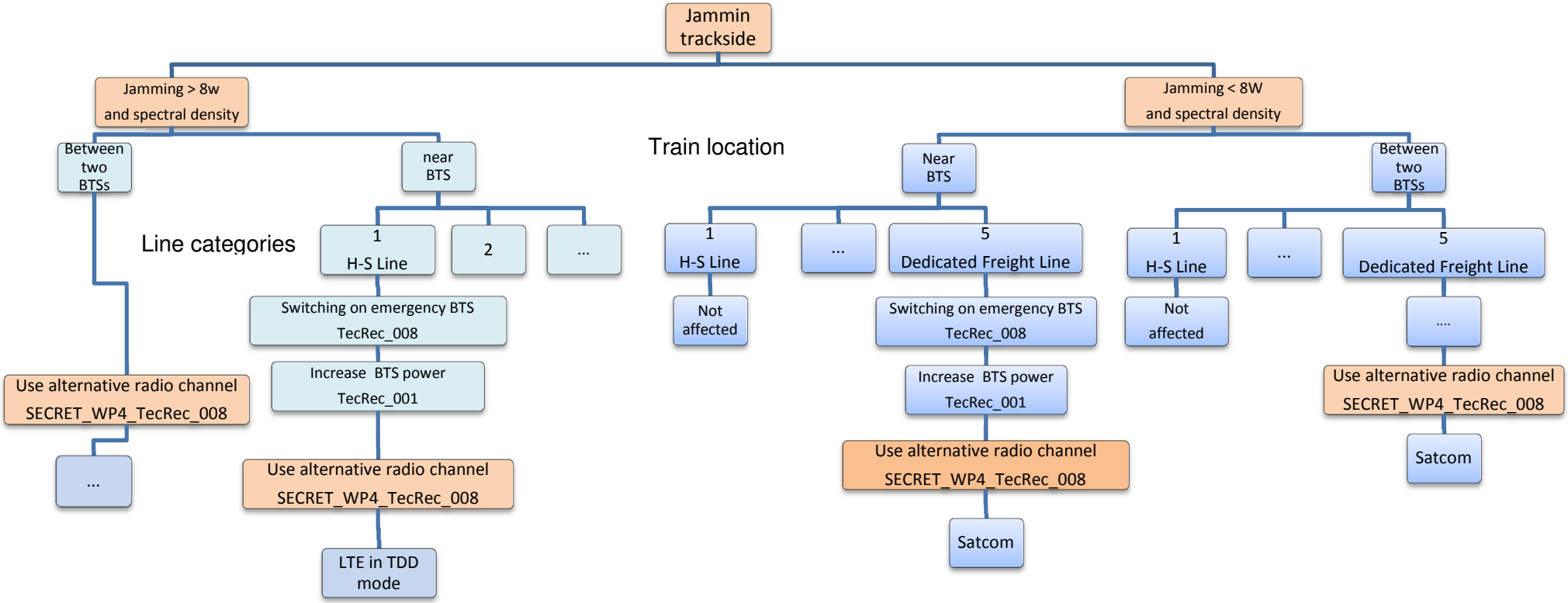
When a jammer is detected along the tack, the environmental criteria can be evaluated in the same sequence:

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

However, the possible recommendations proposed for each step in the sequence are different compared the case of jammer detection on-board the train

In such a case, the train should be able to continue its movement, i.e. under low speed staff responsible mode, in order to exit from the jamming area.

The decision tree presented below in an example describing the process and proposed recommendations. It should be further developed in the future.


Jammin trackside
Jamming > 8w and spectral density
Jamming < 8W and spectral density
Train location
Between two BTSs
near BTS
Near BTS
Between two BTSs
Line categories
1 H-S Line
2
...
1 H-S Line
...
5 Dedicated Freight Line
1 H-S Line
...
5 Dedicated Freight Line
Switching on emergency BTS TecRec_008
Not affected
Switching on emergency BTS TecRec_008
Not affected
....
Use alternative radio channel SECRET_WP4_TecRec_008
Increase BTS power TecRec_001
Increase BTS power TecRec_001
Use alternative radio channel SECRET_WP4_TecRec_008
...
Use alternative radio channel SECRET_WP4_TecRec_008
Use alternative radio channel SECRET_WP4_TecRec_008
Satcom
Satcom
LTE in TDD mode

10. Conclusion

This deliverable describes the recommendations coming from different studies performed in WP3 “Monitoring the EM environment and detection of EM attacks”.

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 equipment.

Some of the recommendations focus on 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, shall be provided separately.
Some other recommendations focus on jammer detection techniques to alert about jamming presence.
Remaining recommendations are based on operational measures applicable when jamming is detected.

Finally, the recommendations were classified according to their permanent or temporary characteristics.

Such classification provides important guidelines to decide the conditions in which the recommendations can be used taking into account the environmental criteria: jamming location, train location, level of communication degradation, railway lines category and presence of alternative radio bearer.

The proposed recommendations seem all very promising and should be further investigated in the future.

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

[5] IFSTTAR, «DELIVRABLE D3.1».

[6] EIRENE EUROPEAN INTEGRATED RAILWAY RADIO ENHANCED NETWORK, «Functional Requirements Specification,» 2014.

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

[8] ETSI TECHNICAL REPORT, «European digital cellular telecommunication system (Phase 2); Radio network planning aspects (GSM 03.30),» 1993.

[9] SELECOM, «AIR Repeater™ RF/RF GSM-R 900,» 2011.

[10] ETSI , «Universal Mobile Telecommunications System (UMTS);UTRA repeater conformance testing,» 2009.

[11] ETSI, «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,» 2012.

[12] S. Breyer, G. Dega, V. Kumar et L. Szabo, «The path towards UMTS - Technologies for the information society,» Alcatel, 1998.

[13] 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.

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

[15] 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.

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

[17] 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.

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

12. Annex : TecRec collected from Secret WP 3

Reference	TecRec TOPIC	TecRec DESCRIPTION	TecRec Type	Involved bodies
SECRET_WP3_TecRec_001	Increasing temporarily ground BTS output power level (8 to 80 W?).	Temporary increase of ground BTS output power level (10 dB) when a jamming situation is detected inside the train. This increases the train received signal to jammer ratio. This necessitates managing and mitigating the impact of the corresponding correlative power increase delivered to the neighboring cells (C /I level).	Standard update	ETSI
SECRET_WP3_TecRec_002	Increasing temporarily train MS output power level (8 to 80 W?).	Temporary increase of train MS output power level when a jamming situation is detected at ground. This increases the ground BTS received signal to jammer ratio. This necessitates to manage and mitigate the impact of the corresponding correlative increase power delivered to the neighboring cells (C/I level)	Standard update	ETSI
SECRET_WP3_TecRec_003	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).	The train received jamming powers are unlikely to be the same at both front and rear train antennas. Therefore, switching from front to rear cab radio equipment could improve, inside the train, the signal to jammer ratio. This engineering rule could already be operational for handover operations?	Engineering rules	Railway industry and operators
SECRET_WP3_TecRec_004	Changing train antennas from E-plane isotropic antennas to E-plane high front-to-back ratio directive antennas.	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 inside the train jammers and train antennas. The impact on handover operation should be investigated. A correlative train antenna front gain increase (4-5 dB) will also result from the introduction of the reflector, improving radio coverage.	Engineering rules	Railway industry and operators

SECRET_WP3_TecRec_005	Electronically switching on a quarter wave reflector behind an existing front or rear train antenna to reject an inside the train jamming signal.	When an inside the train jamming signal is detected, 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. A correlative corresponding train antenna front gain increase (4-5 dB) will also result from the introduction of the reflector, improving radio coverage.	Engineering rules	Railway industry and operators	
SECRET_WP3_TecRec_006	Use a special antenna with managed diagram polarity	The aim of this antenna is to reject any suspect signal. The diagram of the antenna is constantly moving to identify the jamming signal and reject it.	Engineering rules	Railway industry and operators	
SECRET_WP3_TecRec_007	Install additional BTSs in hazardous area where coverage can be easily affected by jamming.	In hazardous area when the coverage level is very low we can install additional BTSs. This modify the BTS radiation diagram and increase the transmission Levels. The impact of the jammer decrease. The impact on handover should be investigated.	Engineering rules	Railway industry and operators	
SECRET_WP3_TecRec_008	Electronically switching on emergency BTSs providing space diversity.	When jamming signal is detected, network is electronically switched from the initial configuration to the new one using the additional BTSs. This modifies the train antenna radiation pattern and attenuates the jamming signal.	Engineering rules	Railway industry and operators	
SECRET_WP3_TecRec_009	Create microcells by additional BTS at the position of the handover.	Creating micro BTS cells by adding smaller BTS and minimize the effect of the jammer on the handover operation position.	Engineering rules	Railway industry and operators	
SECRET_WP3_TecRec_010	Install AIR Repeater as solution for GSM-R coverage.	Use the air repeater when a jamming situation is detected inside the train. This increases 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 disposition needs to be investigated before their placement.	Engineering rules	Railway industry and operators	

SECRET_WP3_TecRec_011	characterization of the EM rail environment, segmented into trains, stations, track	In order to provide a detection system able to sensitively find intrusion, we can specify for the different methods several environments representing the railway network.	Engineering rules	Railway industry and operators	
SECRET_WP3_TecRec_012	Deploy sensors network over the whole communications network to detect attacks.	Based on the railway antenna we can deploy an additional sensor network to detect the presence of jamming along the track. Connected to the control center we can achieve this information to secure the area by acting directly to find jammers and by reroute the trains by another way.	Engineering rules	Railway industry and operators	
SECRET_WP3_TecRec_013	Integrate a monitoring system based on the spectrum analysis on the cab antenna and on the BTS	A second method tested is to use the spectrum signal to detect jamming. The proposed detector considers directly signals from the railway antennas (BTS or cab radio) to provide jamming information.	Engineering rules	Railway industry and operators	
SECRET_WP3_TecRec_014	Implementation of EVM jammer detector on both the onboard system equipment and on the radio control centers equipment.	Use the existing system to incorporate an EVM indicator. This solution permits the detection of jamming and inform both of the train driver and the control center to react face to attacks. The process need to be conforming to the ETSI standard.	Engineering rules	Railway industry and operators	