



# 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 8.3

Final report

**Deliverable on third periodic report**
**Date: 28/10/2015**
**Distribution: PP**
**Manager: IFSTTAR**

## Document details:

| | |
|---|---|
| Title | **Final report** |
| Workpackage | WP8 |
| Date | 25/01/2015 |
| Author(s) | E.BESSMANN , V. DENIAU |
| Responsible Partner | IFSTTAR |
| Document Code | SEC-D8.3-A-10 2015-Third periodic report-Ifsttar-draft |
| Version | A |
| Status | Draft |

## Dissemination level:

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

| | | |
|---|---|---|
| **PU** | Public | |
| **PP** | Restricted to other programme participants (including the Commission Services) | x |
| **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 |
|---|---|---|---|
| 1 | 28/10/2015 | E.BESSMANN | First draft |
| 2 | 25/01/2016 | E.BESSMANN | 2nd draft |
| 3 | 28/01/2016 | V.DENIAU | 3nd Draft |

## Table of content

# 1. Publishable summary

## 1.1 Summary description of project context and objectives

SECRET project aims to study the impact of EM attacks on the European rail network and provide solutions to strengthen the resilience of the rail system against such attacks.
This project is directly related to the context of the deployment of ERTMS (European Railway Traffic Management System) over the European railway network. Indeed, the ERTMS is notably based on the deployments of the GSM-R communication system and ETCS (European Train Control System) in order to homogenize the communication, signalling and train control solutions inside the European territory. However, this homogeneity of the technologies employed in Europe also conducts to the homogenization of the vulnerability points to the EM interferences.
Thus, when a malicious person has a intentional EM emissions device capable of disrupting the rail network in Berlin, for instance, the same device will have the same attack capacity in all European cities. This will cause at least immediate economic consequences and possibly more….
Harmonization thus facilitates the implementation of organized and simultaneous EM attacks. Our project notably aims to complete the harmonization solution to ensure its resilience and robustness against EM attacks.
Meanwhile, the technologies and frequencies employed in the railway field are similar to technologies and frequencies used for applications available to the general public. Indeed, the railway no longer develops technology "owners" but adapts general public technologies. That increases the vulnerability of the railway because it is easy to obtain emission devices capable of disrupting rail technologies. With relatively basic electronics knowledge and the performance of electronic components and antennas available on the open market, these emission devices can be combined with amplifiers to increase the capacity of EM attacks.
Knowing that today the state of deployment of ERTMS is not the same in the different European country and the European rail system is still very diverse in terms of supporting technologies and knowing that its EM vulnerability is directly depending on the technologies involved, the consortium decided to prioritize the work on the technologies expected within ERTMS level 2 and SECRET consortium aims to provide recommendations for strengthening the ERTMS security aspects.
The methodology followed in the project to extract available recommendations is composed of 4 main activities.
The threat assessment and risk analysis: the project's first objective is to conduct a systemic analysis of the management of a railway network to identify the different scenarios, which may occur in the case of an EM attack and evaluate its consequences. In parallel, a list of potential EM attacks equipment available in the public domain is established. A lot of effort are also involved in the implementation of demonstration EM attacks and produce a clear and quantified vision of the threats and risks in the case of an EM attack on the railway network. Preventive and recovery measures at a systemic level have to be identified.
Technical protection: the issue of protection of railway wireless systems is addressed in order to ensure the resilience of the railway infrastructure regarding EM attacks. The project then aims at a global EM protection solution consisting of monitoring the EM environment to detect and characterize EM attacks, adopting redundancy and complementarity in information transmission links and finally a dynamic protection permitting the selection of robust transmission links relative to the characteristics of the EM attack, thus providing resiliency quality to the whole infrastructure recommendations for a resilient railway infrastructure:
Finally, in order to optimize the contribution of this project to a secure and harmonized European railway network, a WP is focused on recommendations and guidelines for policy makers, operators and the rail industry and will contribute to improving European standardization.

### 1.2 Description of work performed and main results

This report is structured in compliance with EC requirements for project reporting (core report).
It relates to the third period of the project (1/08/2014-30/11/2015).
Are documented in this report:

- Project objectives of the period
- Work progress and achievements during the period
- Project management during the period

### 1.2 Expected final results and potential impacts

These results are summarized in the so-called White Paper.
"Security of Railways against electromagnetic attacks"

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

- The first category called "**prevention from EM jamming effects**" groups the recommendations which can be adopted permanently and can permit to inhibit or reduce the impact of jamming signal (precautionary principle).

- The second recommendation category is dedicated to the **EM attack detection** solution. It presents the different detection technics which were studied in SECRET and presents the potential applications.

- The third category is "**Mitigation of EM jamming effect**". In this category, the recommendations are focused on solutions which can be activated temporally in situation of EM jamming. These recommendations are then conditioned by the existence of an attack detection solution.

## 2. Project objectives for the period

### 2.1 Overview of the project objectives of the period

The project illustrated the risk by implementing some electromagnetic attacks and analyzing their effects, thereby inciting the different railway actors to work together to strengthen the resilience of a system that must remain effective and safe for the serenity of our society.

Then the project opened ways to resilience solutions regarding this type of attack. Preferring to avoid unconstructive and alarming rhetoric, which is unjustified as the European railway system is above all a very safe means of transport, the project identified and proposed strategies in which each actor would be able to inspire itself in order to act towards resilience.

The strategies developed mainly concern:

- The tests that can be performed to assess the susceptibility of individual network components dealing with intentional interferences and allowing each designer, integrator or operator to build, evaluate and compare the susceptibility of these products and the design rules which can permit us to improve the immunity level of the communication systems (prevention from EM jamming).

- The methods of detection of electromagnetic attacks that are essential for several reasons: Detecting is to be able to demonstrate that we have been a victim of an electromagnetic attack, detecting avoids confusing an electromagnetic attack with a technical failure which could unduly jeopardize the operator, who could initiate unnecessary diagnostic inquiries. And, finally a reliable detection can instigate a fast and appropriate reaction to the threat.

- The resilient architecture which is a compulsory issue when we consider a critical infrastructure which is a network. The resilient architecture has to ensure the maintenance of communication for the transmission of critical information, thus maintaining the control of the network. We worked on an adapted architecture permitting us to assess the impact of certain technological solutions on reliability and responsiveness.

**Target group for the project**

- The project main targets are
- Rail manufacturers
- Rail operators
- Rail Infrastructure Manager
- Standardization Bodies
- Telecommunication network actors
- Other critical infrastructure (involving wireless communications) managers

The project concept can be summarized in three domain categories and in five technical work packages, i.e.:

- Threat assessment and risk analysis (WP1)
- Innovative solutions for technical protections to be implemented in order to protect the railway against EM attacks (WP2, WP3, WP4)
- Recommendations for a resilient architecture (WP5)

WP6, WP7, WP8 are respectively in charge of the dissemination, the project technical management and administrative/financial management.

The work plan of the project was based on a 36 months.and has been extended to 40 months according to the project's 5$^{th}$ amendment.

**The objectives of each WP throughout the project were:**

**WP1 Threat analysis and risks assessment of EM attack scenarios for Railway**

- Identification of potential electromagnetic threats based on public-domain devices
- List of potential victim equipment or system (GSM-R, TETRA, Eurobalise, GPS….)
- List and definition of potential attack devices and attack EM signals
- Analysis and consequences of EM attacks on the railway infrastructure and identification of countermeasures
- Definition and Selection of EM attack scenarios
- Threat assessment and Risk analysis
- Specification/experimentation of EM attack scenarios

In the initial annex 1 of the project, the WP1 should be finished during the second period and all the deliverables were provided as scheduled before the end of the second period.
However, following a recommendation of the PO during the Second project review in september 2014, SNCF and Zanasi continued working during the 3nd period on risk assessment and threat analysis to obtain quantitative elements for the deliverables D6.4. which was added to the last project amendment.

**WP2 Static protection: topologic solutions to strengthen the railway infrastructure**

- Identify the most vulnerable paths and the susceptibility of the railway infrastructure devices to a potential act of EM terrorism.
- methodologies for testing the susceptibility of the various components of the infrastructure and,
- hardening rules aimed at increasing the network immunity **(prevention to EM attacks)**

Tasks to be delivered during the 3rd period

- D2.4 Hardening rules for infrastructure vulnerability reduction

During the third period, supplementary tests were performed in collaboration between ULG and Alstom in order to check and compare the vulnerability of wired track side equipment in relation to wireless equipment to EM attack signals.

**WP3 Intentional ElectroMagnetic Interference (IEMI) in Railway-why and how to sense them.**

- develop solutions to monitor the EM environment
- detect EM attacks on the railway infrastructure, able to disturb communication or signalling functions over the European territory and,,
- test and compare different detection principles

Tasks to be delivered during the 3rd period :

- D 3.4 "Assessment of the monitoring and detection solution: test report"

During the third period, several implementations, experimentations and demonstrations were performed in order to assess the cost and compare the performances of the different detection solutions. Demonstrations were performed with the partners of the WP4 in order to include the detection functions in the resilient architecture and to assess the interest of the detection to protect the communication transmission.

**WP4 Dynamic Protection: Detection System for Resilient Architecture**

- communication architecture specification
- requirements for interoperability
- heath.attack manegement module for EM attacks resilience
- acquisition system for detection sensors
- Multipath communication system for reconfiguration

Tasks to be delivered during the 3rd period :

- D4.4: implementation of the dynamic protection system
- D4.5: Validation of the implementation through use case

During the third period, several demonstrations (proofs of concept) were performed.

A demonstration was performed using an Alstom equipment permitting the reconfiguration and coupling it with the detection sensors and the acquisition system to identify the resilient communication configuration. A second demonstration was performed applying the whole SECRET resilient architecture (detection, acquisition system, heath/attack manager) including the Multipath Transmission Control Protocol (MP-TCP) permitting to adapt the communication link to the presence of attacks without time delay.
A third demonstration permitted to add the Central Heath/attack management module and to implement the transmission of the detection information to the control center.

### WP5 Recommendations for a resilient railway infrastructure to EM attacks

This activity started on Y2 of the project.

- develop proposals for TecRec (Technical Recommendations).
- develop recommendations on the way to design the infrastructure devices (methodologies, hardening rules...), on the EM attack management (detection, signature...) and design rules to ensure resilience of services.

Tasks to be delivered during the 3rd period :

- D5.2 Proposal for TecRec on preventive and recovery measures
- D5.3 Proposal for TecRec on static hardening rules
- D5.4 Proposal for TecRec on EM attack detection
- D5.5 Proposal for TecRec on redundancy for resilient architecture

The main recommendations of the different deliverables permitted to publish a white paper dedicated to SECRET results.

### WP6 Exploitation & dissemination

This WP is active throughout the whole life of the project.

Tasks to be delivered during the 3rd period:

- D6.1 Final Exploitation Plan.
- D6.4 on SECRET summary report ( this deliverable was added in the last amendment due to the 2nd review' PO recommendations of providing a deliverable to disseminate WP1 observations in the EC.

### WP7 Technical management

The deliverable has been achieved in month 3 (project quality plan) but the WP is active throughout the whole life of the project.

### WP8 Administrative and financial management

This WP is active throughout the whole life of the project.

Tasks to be delivered during the 3rd period:

- Submission of 2nd periodic report
- Submission of 2nd period FormC
- Submission of 3rd/Final report
- Submission of 3rd/Final Form C
- Amendments relating to the project duration extension and other issues linked with partners' updates

## 2 Work progress and achievements during the project period

### WP1 - THREAT ANALYSIS AND RISK ASSESSMENT OF ATTACKS EM SCENARIOS

Objectives :
- Identify the devices which can be easily obtained in the public domain and to characterise the EM interferences that they can produce in order to establish a list of the critical equipment and signals.
- Setting a risk assessment study to extract an inventory of typical EM attack scenarios which can involve critical or major events on the railway network.

**Task 1.1 - Identification of potential electromagnetic threats based on public-domain devices**

**Leader : Polito (M0 to M12)**
**Objectives**
Investigate, identify and classify electromagnetic devices and systems that can be used as potential source of threat to trains and to the rail infrastructure.

**Progress towards the objective**
An extensive research on potentially dangerous devices and systems was made.
Devices were listed according to relevant parameters as: Power, Size, Band coverage, Deployment framework, Cost, Availability, Expected effects on victim systems.
Wave shapes produced by different attacking devices are detailed.
Railway operating environment and potential victim systems are described.

**Clearly significant results**
Easily readable database of attacking devices ( D 1.1 )
Easily readable database of effects on victim systems ( D 1.1 )
Potentially harmful waveshapes expressed in graphs ( D 1.2 )
Potentially harmful waveshapes expressed in mathematical form ( D 1.3 )

**Deviations, impact and correction:**
none

**Impacts :**
This work represents the basis on which next activities will be built.

**Corrections:** none

**Task 1.2 - Analysis and consequences of EM attacks on the railway infrastructure and identification of countermeasures**

## Leader: IFSTTAR (M0 to M12)

**Objectives**
This task aims to identify and to classify the most likely scenarios, whose the causes are the potential threats related to EM aspects, by adapting tools and methods from risk assessment (e.g. Bowtie method). From this study, it will be necessary to determinate, in one hand, barriers/countermeasures (material or functional) to implementing in order to avoid reaching undesirable events that result from EM attacks, and in other hand, protective measures in order to reduce the spread of these events to catastrophic consequences. These works are an input for the WP5, which is a test case based on a scenario extracted from this task

**Progress towards the objective**
Rolling stock and railway infrastructures having different modes of operation in the European landscape, the study focuses on the next management generation of railway system ETCS/ERTMS, specifically on ETCS/ERTMS level 2, which uses widely radio communications tools, which are more sensitive to EM attacks. So the performed work describes methods and tools used to assess the vulnerabilities of GSM-R communication system faced with EM attacks with jamming devices. A User profile for these devices could be used to define a threat matrix that may be correlated to a bow tie chart in order to have a broader view of this type of threat.

**Clearly significant results**
First draft of results for this study highlights the weakness of radio communication subsystems in the railway area. Next steps of works are to detail other scenarios (especially consequences) and design the adequate barriers and countermeasures to the occurrence of threats.

**Deviations, impact an correction**

**Deviations:** During this first year, we noticed that it is really difficult to assess to all the railway information to deploy a full risk analysis. Moreover, the consortium reached the conclusion that it is necessary to combine three different approaches to classify the different attack scenarios: a generic Threat Matrix methodology, a Failure Mode and Effect Analysis (FMEA) approach and finally, a bow-tie risk analysis approach.

**Impacts:** the deliverable D1.4 details and arguments the 3 approaches, details the elements to consider for the definition of the scenario and illustrates the 3 approaches on one selected EM attack scenario.

**Corrections:** No specific correction

**Task 1.3 – Specification/experimentation of EM attack scenarios (M6-M20)**
**Leader : SNCF**

**Objectives**
Clarify the true threats and impacts of potential EM attacks on railway infrastructure
Definition and demonstration of EM attack scenarios

**Progress towards the objective**
In this task a specific scenario was define for the implementation of the proofs of concept performed by the partners of WP3 and 4. Moreover, other scenarios involving railway critical components (GSM-R, TETRA and Eurobalise) were defined and followed during specific experimentations performed by SNCF, Polito and IFSTTAR.

**Clearly significant results**
Deliverable D 1.4 EM attacks on Railway Networks: Consequences and Responses
Deliverable D 1.5 General definition of use case
Deliverable D 1.7 Demonstration EM attack scenarios : Description and results

**Deviations**
The realization of EM attack demonstrations on the railway infrastructure could not be carried out because we did not obtained the authorization to switch on jammers in the vicinity of the trains in operation due to the risks of disturbing the good operation of the trains. A possibility is still in discussion but we have to access to a site where the GSM-R is deployed but not employed.

**Impacts :** no tests on the whole railway infrastructure but tests were performed in employing real railway equipment (Network BTS and cab radio).

**Corrections:** We grouped all the main railway elements (access to an antenna of a BTS and on board cab radio) in a laboratory and we emulate the variations of the conditions regarding the characteristics of communication and jamming signals. The communication levels for which the communication link was lost were compared with the signal communication covering measurements performed along railway infrastructure in order to estimate the length of the railway sections which would be affected by the jamming.

**Statement on the use of resources**

IFSTTAR's personnel effort is then slightly lower than foreseen. But complementary risks analysis based on ontologies was carried out in WP4 to permit the assessment of the resilient architecture. A part of IFSTTAR personnel effort was forward to WP4

## WP 2 - STATIC PROTECTION: TOPOLOGIC SOLUTIONS TO STRENGTHEN THE RAILWAY INFRASTRUCTURE

**Objectives :** WP2 aims at identifying the most vulnerable paths and the susceptibility of the railway infrastructure devices to a potential act of EM terrorism. In addition, methodologies for testing the susceptibility of the various components of the infrastructure was developed and tested. Finally, hardening rules aiming at increasing the network immunity to EM attacks were identified.

### Task 2.1 Analysis of the infrastructure and identification of the coupling paths
**Leader : Polito (M1 to M12)**

**Objectives:** The main objective of this task is to perform a systematic analysis of the railway infrastructure and identify both “front door” and “back door” paths through which the EM interferences can agress the system.

**Progress towards the objective**

In the railway system ETCS/ERTMS several on board equipment were identified as sensitive to EM attacks due to the use of radio communications tools. An analysis of the coupling paths of EM threats is carried out on GSM-R, Eurobalise and TETRA communications systems.

The coupling between the train antennas and the fixed transmitting stations were estimated and compared to the coupling paths between jammers and train antennas, characterized through S-parameter measurements. A Signal-To-Noise ratio was defined in standard and worst cases to be used as reference during susceptibility assessments.

**Clearly significant results**

The identification of the coupling paths in GSM-R system is described in deliverable D 2.1, highlighting the wireless radio channel as the main path for EM attacks to railway infrastructures.

**Deviations:** Initially in the proposal, a sub-contracting budget was planned to the realization of the measurements because we did not know if we would be allowed to access to the railway equipment. The sub-contracting enveloped was based on an estimation given by RFF (Réseaux Ferrés de France) which recommended the intervention of a specific internal team. Finally, we could perform the measurements ourselves thanks to the help of the railway partners.

**Impacts:** Due to we carried out the measurement ourselves, Polito’s personnel effort and the travel costs are slightly higher than foreseen.

**Corrections:** In the amendment 5, we modified the Annex 1 (Description of Work) to translate the sub-contracting budget to the travel costs and MM.

**Task 2.2 Susceptibility analysis of critical infrastructure equipment to EM threats**

**Leader : Polito (M13 to M24)**

**Objectives:**
Investigate, identify and classify equipments of the rail infrastructure that result to be sensitive to potentially dangerous electromagnetic signals.

**Progress towards the objective**
In the railway system ETCS/ERTMS several onboard equipments were identified as sensitive to EM attacks due to the use of radio communications tools. A susceptibility analysis is carried out on GSM-R, Eurobalise and TETRA communications systems.
The transmitted/received functional signals were characterized according to power, bandwidth and BER. The interactions between specific jamming signals described in WP1 and the radio equipments were analyzed according to the coupling paths defined in task 2.1.

**Clearly significant results**
The results of the susceptibility analysis are described in deliverable D 2.2, highlighting the radio communications as the weak spot to EM threats in the railway area. This work represents the basis on which the next Task 2.4 (Definition of hardening strategies for infrastructures in order to reduce the electromagnetic vulnerability) will be carried out.

**Deviations:** Initially in the proposal, a sub-contracting budget was planned to the realization of the susceptibility tests because we did not know if we would be allowed to access to the railway equipment. The sub-contracting enveloped was based on an estimation of RFF (Réseau Ferrés de France) which recommended the intervention of a specific internal team. Finally, we could perform the tests ourselves thanks to the help of the Alstom and SNCF.

**Impacts:** Due to we carried out the susceptibility tests ourself, Polito's personnel effort and the travel costs are slightly higher than foreseen.

**Corrections:** In the amendment 5, we modified the Annex 1 (Description of Work) to translate the sub-contracting budget to the travel costs and MM.

**Task 2.3 – Assessment of adequacy of immunity standards to potential electromagnetic threats**

Leader: ULg

**Objectives**

The objective of this task is to analyse the currently employed EMC standards and measurement setups to significantly probe the railway system, and verify to what extent the bandwidth and energy levels in use are adequate to describe the EM attack threat.

The results of this task will demonstrate the possible deficiencies of current norms, and will provide an input for future revisions of European EMC standards, with the aim of extending their scope to cover also the potential risks of EM attacks.

**Progress towards the objective**

Regarding the potential threat identify in WP1, jamming, we have analyzed European Directives (EMC & RED), harmonized standards (product standards related to railway – CENELEC - and to communication systems –ETSI) and basic EMC standards (from TC77C of IEC, and SC77C for IEMN). In these standards, we have considered immunity test set-ups and performance criteria.

**Clearly significant results**

The main conclusion is that there is a gap in the present standardization: no basic EMC immunity standard considered jamming phenomena, ETSI EMC standard does not exist for GSM-R, the critical wave shapes identified in D1.3 (WP1) are not considered.

Even if SC77C is now considering jamming, we do not think that the study is mature enough to impact on basic standards, based also on the fact that jammers are illegal on the European market.

Nevertheless, we encourage manufacturers to add additional susceptibility tests on their communication systems (especially GSM-R and Tetra, but also LTE and further used technologies). These tests could help to compare the performances of these electronic subsystems regarding those threats.

Regarding the performance criteria, we have also suggest to use EVM parameter (IQ measurements) as this parameter could be also a real time monitoring of the quality of the communication, to include attack monitoring in each equipment or subsystem.

**Deviations, impact and correction**

There is no deviation regarding this task.

**Task 2.4 – Definition of hardening strategies for infrastructure in order to reduce its EM vulnerability to EM attacks**

Leader: Polito

**Objectives**

The objective of this task is to define rules capable of protecting the systems against intentional interferences. The most significant examples of rules concern the electromagnetic shielding for critical equipment, surge (transient) protection and the system monitoring to provide security alarms.

**Progress towards the objective**

The railway networks rely on Radio communications, both for traffic management and for security issues, and use GSM-R, TETRA, GNSS-GPS and Eurobalises technologies.

Attackers may disturb communications by interfering the expected flow of traffic or causing its disruption. Harmful devices have been identified and their possible neutralization has been studied.

The results of the previous tasks allow proposing a set of countermeasures meant to reduce the infrastructure vulnerability. A report summarizing this task provides a list of actions aimed at the improvement of various railways communication systems, their supposed cost, effect and applicability.

**Clearly significant results**

Hardening techniques for GSM, GPS, TETRA and EUROBALISES were identified and described.

Five main recommendations were provided and detailed. The values of the recommendations were discussed according to the attack scenarios.

**Deviations :** none

**Impacts :** This work represents the basis on which the next Task 5.3 (TecRec static hardening rules) was carried out.

**Corrections :** none

**Statement on the use of resources**

As previously communicated, Polito's personnel effort is slightly higher than foreseen.
In P2 the personnel resources has been used for a total of 18,2 m/m.
As previously stated, the cost of personnel was updated taking into account actual data and actual costs. Overall, the resources are being used as planned in Annex 1 (Description of Work).

## WP 3 - MONITORING THE EM ENVIRONMENT AND DETECTION OF EM ATTACKS

**Objectives :** The WP3 aims to develop solutions to monitor the EM environment and to detect EM attacks on the railway infrastructure, able to disturb communication or signalling functions over the European territory. WP3 concentrates on research of electromagnetic (EM) attack detection solution including sensors and processes to discriminate normal EM conditions and EM attack conditions. Output information data of the development of this WP3 will be serving the diagnostic system and dynamic protection in WP4.

### Task 3.1 - Electromagnetic and statistical characterisation of the railway environment in "normal" operation conditions

**Leader :IFSTTAR**

**Objectives**
The goal of Task 3.1 was to select the conditions (train station, train lines in urban and rural environments) and measurements methods to extract the "synthesis"' models of normal EM rail environment. From this model we will specify a test bed to generate in laboratory EM noise conditions that emulate the EM noise environment rail. This test bed will then be exploited for the implementation and the evaluation in the following tasks of this WP.

**Progress towards the objective**
Task 3.1 was active during the period M1 to M12. In this task, the ERTMS/ETCS critical systems and associated railway equipment to be considered were deduced from the previous "Secret" EM threats Tests strategy work (WP1). Using these results, we focused on the railway critical systems that are in the scope of this Secret WP3 activity. Then, we defined the corresponding frequency bands of interest to be investigated. Extended frequency bands centred on the GSM-R, TETRA, EUROBALISE and GNSS/GPS were selected. The methodology and the experimental conditions employed to collect reference noise conditions were studied. To define "normal" EM conditions, experimental results performed in European critical railway sites (stations, railway line) were recorded using a specifically developed portable test bed. Available jammers were also tested in order to upgrade an EMC test bed built to evaluate the impact of different radiofrequency jammers on a GSM-R link. Severe degradation of the radio link or total loss of communication was experienced during these laboratory tests. Therefore, during this period, "normal" EM conditions were measured and defined in order to constitute reference conditions for the development involved in WP3. Theoretical techniques to determine a normal electromagnetic environment were also identified and their evaluation has started in task 3.3.
Major T3.1 results were presented in the deliverable D3.1 and were focused on the evaluation of « normal » EM conditions in railway critical environments. Critical railway systems and sites have been identified and described. The methodology and the experimental conditions employed to collect reference noise conditions were studied and used. Significant experimental results performed in European critical railway sites were reported and evaluated. Theoretical techniques to determine a normal EM environment were presented and a preliminary analysis of the recorded experimental results was discussed. A WP3 contribution to the WP4 D4.1 deliverable was also prepared by Tasks 3.1/3.3.

**Deviations, impact and correction**
**Deviations**:
No deviations to the Description Of Work are reported for this task 3.1.
**Impacts:**
Task 3.1 is the basis for the work undertaken into WP3. It has considered the inputs coming from WP1 in terms of EM threats Tests strategy. Some inputs were also delivered to the system architecture performed in WP4.

**Task 3.2 – Specification of the acquisition system to access the quantities to recognize EM attack scenarios (M13-M24)**
**Leader: IFSTTAR**
**Objectives**
Task 3.2 concentrates on the specification of the acquisition system to access the quantities to recognize EM attack scenarios identified in WP1. It is divided in two sub tasks. Sub task 3.2-a evaluate quantities and sensors to monitor EM environment and detect EM attack signals. Sub task 3.2-b evaluates EM attack signatures on communication systems.
**Progress towards the objective**
Task 3.2 has been active during the period M13 to M24. The impact of the jammer location has been analysed and we concentrated on the GSM-R ground to train communication system. We considered jammers situated at different locations in trains and at ground, i.e. on a platform, close to a base transceiver station, and between two different base transceiver stations. Sub task 3.2- considered different simplified railway environments and corresponding propagation models. In the studied scenarios, the GSM-R link is broken by a jammer. Different physical layer mitigation techniques were envisaged i.e. switching front to back train equipment, higher power, directive antennas. But, the full benefit of the physical layer counter measures can only be obtained if the communication protocol evolves (work of WP4). To specify the detection acquisition system, we considered that one sensor is associated to each signalling receiver situated at ground or in the train and that it is working in parallel with the corresponding receiver. In task 3.2, we used the In phase and Quadrature phase (I/Q) information accessible in any digital transmission receiver. We exploited signals available at different stages of the receiver and noticed that the IQ constellation is significantly distorted when a jammer appears. The major advantage of this method is that it can detect a jamming signal very quickly, potentially during single bit transmission duration. A second analysis, based on the Error Vector Magnitude technique, was also developed. It provides a better discrimination between propagation effects and jammer impacts. This method necessitates a longer analyzing period, typically a burst length (156 bits in a GSM-R scenario). Finally, a last method based on the statistical analysis of the spectrum was studied. This last method permits to monitor several communication systems and it can be more adapted in train station. In sub task 3.2-b tasks simulations were carried out to model more accurately the impact of the jammer on the ETCS communication as a function of the position of the jammer and of its technical characteristics. The OPNET software was used. It is a leading commercial Discrete Event Simulator (DES). The modelled ERTMS architecture consists of three main components the train, the Radio Block Centre **(**RBC) and the GSM-R network that connect both devices. Extensive simulations have been performed.
**Clearly significant results**
Detection solutions permitting to detect a jamming signal very quickly have been identified.
The OPNET simulation showed that, in the case of a jammer located close to a BTS, the BTS is completely blocked due to the fact that this jammer also jams the uplink. Thus, the BTS is annulled. The only solution would be to have overlap BTS coverage areas to use an alternative BTSs. All the results are presented in deliverable **D3.2.**
**Deviations:** The requirement in term of detection being different according to the location (on board train or in train station), several detection methods were finally studied. A method permits us to monitor only one communication system but the time delay of detection is sufficiently brief to avoid an emergency braking. The other methods permit us to monitor several communication systems and are more adapted to the monitoring of the stations.
**Impacts:** Due to several detection solutions were studied and the number of measurement campaigns, IFSTTAR's personnel effort and the travel costs are higher than foreseen.

**Corrections:** in the proposal, a sub-contracting budget was planned to the realization of the measurement campaigns on the trains and along railway infrastructure because we did not know if we would be allowed to access to the railway environment. Finally, thanks to the help of SCNF, IFSTTAR personnel's could perform the measurements ourselves and we performed an amendment to redistribute the subcontracting budget in MM and travels.

**Task 3.3 - Representation space definition of the "normality" and the “non-normality” (M6-M18)**
**Leader: IFSTTAR**
**Objectives**
Task 3.3 concentrates on EM attack detection solution including sensors and processes to discriminate normal from attack EM conditions. Output data of the development of this WP3 serves the diagnostic and dynamic protection developed in WP4 and the demonstration phase of this WP3 is performed in task 3.5. Task 3.3 aims at defining how the railway EM environment is disturbed when an EM attack occurs. Its main objective is to characterize modification of the EM environment by defining an adequate representation space.
**Progress towards the objective**
Task 3.3 has been active during the period M6 to M18. The anomaly detection aims at finding something that is not consistent with what we expect of the behavior of a system or the behavior of one of its elements. The expected behavior of a system can be defined by its normal state; the occurrence of an anomaly can make the system switch to a degraded state. To reach this goal, we evaluated supervised mode techniques in laboratory, using the task 3.1 developed test bed and then, in situ, in railway environments. These supervised mode techniques necessitate a learning phase performed during “normal” and “attack” EM conditions. We have considered two different methods.
A first method, developed in task 3.2, collects the necessary data in the receiver, EM attack detection was evaluated at any railway receiver potentially jammed using the In phase and the Quadrature phase (I/Q) information currently accessible inside any digital transmission receiver. The Error Vector Magnitude technique, applied to the detection of jamming conditions, was then developed also in task 3.2. In task 3.3 our second selected method operates in the frequency domain. This method does not necessitate any information coming from the receiver or a direct physical link to it. However, it shares the same receiving antenna using for example a coupler or another close receiving antenna. This antenna requirement is needed for the detection equipment to sense the same useful and jamming signals as the railway receiver does. This separate acquisition equipment can be a real time spectrum or signal analyzer connected to the receiver antenna at the base transceiver station or mobile equipment. It can also be dedicated equipment composed of a software designed receiver associated to a specific signal processing. In task 3.3, such a dedicated signal processing was developed and evaluated. Spectral descriptors are created in a frequency range centered in the frequency band of interest. They cover a wider frequency range that the strictly occupied bandwidth. We used spectral power density. Classification detection is performed to detect and also to potentially recognize the jammer (see also task T3.4). A jammer is only recognizable if it has already been considered during the learning phase of the process. We concluded that this technique is very effective when a stable channel state is available over a sufficiently long period, typically several tens of milliseconds.
**Clearly significant results**
The last method developed in task 3.3, has the interesting potential to provide information about the jammer characteristics. The process of identifying these jammers was studied in task 3.4. Task 3.3 and task 3.4 results are presented in the available deliverable D3.3. This method will be now implemented in task 3.5.
**Deviations:** Like in the task T3.2, due to the requirements in terms of detection performances being different according to the location (on board train or in train station), several detection methods were studied. A method permits us to monitor only one communication system but the time delay of detection is enough brief to avoid an emergency braking. The other method permits us monitoring several communication systems and is more adapted to the monitoring of the stations.
**Impacts:** Due to several detection solutions being studied and the number of measurement campaigns, IFSTTAR’s personnel effort and travel costs are higher than foreseen.

**Corrections:** in the proposal, a sub-contracting budget was planned to the realization of the measurement campaigns on the trains and along railway infrastructure because we did not know if we would be allowed to access to the railway environment. Finally, thanks to the help of SNCF, IFSTTAR personnel’s could carry out the measurements ourselves.

**Task 3.4 – Specific modelling of sub-sets of EM attacks (M13-M39)**
**Leader: IFSTTAR**
**Objectives**
This task aims at identifying each electromagnetic (EM) attack to insure the efficient resilience of the railway system. Each EM attack has a specific representation in the frequency domain as defined in task 3.3. Task 3.4 studies how to cluster this frequency domain into several classes related to sub-sets of EM attacks with common properties.

**Progress towards the objective**
Task 3.4 has been active during the period M6 to M18. At this M24 reporting period, it is finished. As specified in task T3.3, the EM attack detections can be performed by a recognition system tuned for different types of EM attacks. The detection principle is based on supervised pattern recognition techniques. It uses power spectral densities (p.s.d., in dBm) obtained at the GSM-R receiver, or by using a dedicated secondary system. These p.s.d. are composed of M spectral channels sampled over a bandwidth defined by the frequency selectivity of the antenna, or by the configuration of acquisition system. The tested jammers use broad spectral bands affecting the uplink and downlink GSM and GSM-R. Although they are all type A, these jammers have different frequency characteristics (bandwidths, and spectral distributions of powers).
After analysis, we found that p.s.d. follow different distribution models with regards to the frequency channels and the type of the jammers. We considered the p.s.d. as a stochastic process defined by a multi variables statistical distribution of M uncorrelated components. In this case, the statistical distribution of the p.s.d. is expressed as the product of the marginal distributions of M frequency components. The first step is to estimate the generative statistical models for each state of the EM environment (clean state, jamming state with jammer 1, jammer 2...). For one spectral component, the model is defined by a multi Gaussians distribution being able to fit to its characteristics. To take into account the spectrum distortions of the jammer due to the EM complex environment, the model has been estimated with EM electromagnetic attacks "mixed" with EM noise of the EM environment that is potentially composed of communications signals.
Once the various classes K are learned (the B jammers to recognize and the clean condition), the detection is performed using a Bayesian classifier: The states being consider with equal probabilities, the class that obtains the maximum likelihood according to a new observation, determine the type of the jammer potentially used. A new observation is defined as a signal not used during the learning step.
**Significant result** Task 3.4 results are presented in the available deliverable D3.3. This method will be now implemented in task 3.5.
**Deviations:** Like in the task T3.2 and T3.3, several detection methods were studied. A method permits us to monitor only one communication system but the time delay of detection is enough brief to avoid an emergency braking. The other method permits us monitoring several communication systems and is more adapted to the monitoring of the stations.
**Impacts:** Due to several detection solutions being studied, the number of persons from IFSTTAR and the travel costs are higher than foreseen.
**Corrections:** in the proposal, a sub-contracting budget was planned to the realization of the measurement campaigns on the trains and along railway infrastructure because we did not know if we would be allowed to access to the railway environment. Finally, thanks to the help of SNCF, IFSTTAR personnel's could perform the measurements ourselves and in amendment 5, we redistributed the subcontracting budget in MM and travels.

**Task 3.5 Proof of concept, evaluation**

Leader IFSTTAR

**Objectives**

Task T3.5, was active between months 25 and 39 of the SECRET project. This task has concentrated on the proof of concept and evaluation of the jamming detection techniques which were developed in previous WP3 tasks. We used several state-of-the-art and low-cost hardware platforms to implement our techniques. The major objective of these implementations was to evaluate the jamming detection potential of the studied techniques in laboratory controlled environments. These jamming detection sensors were also developed to outperform an available commercial sensor whose latency time and too wide bandwidth were considered. A strong link was established with WP4 so that demonstrations could be performed to enable a common proof of concept of the global SECRET resilient radio architecture.

**Progress towards the objective**

Four different techniques were implemented to effectively build five different physical sensors. The first technique performs an analysis of the spectrum occupation, a supervised detection is used. This consists in learning the 'normal' electromagnetic environment and then recognizing any environment which does not belong to this 'normality'. The basic measured quantity is the energy inside a given resolution frequency bandwidth centred on a specific channel (power spectral density). This implementation was successful and especially effective when the electromagnetic environment remains unchanged. The second technique performed the detection by quadratic analysis of the received signal (I/Q) based on Error Vector Magnitude measurements. This implementation was also successful and could be implemented in receivers. The third technique evaluates an excess of energy provided by the jamming incoming energy in the observed bandwidth or in the allocated communication channels. This technique is easy to implement and was found quite effective. The fourth technique is indirect and evaluate, in case of jamming, the incapacity of a device to connect anymore to any network operating in the vicinity. Then, for the purpose of our proof of concept, we considered two generic cases of study for the demonstrations. Firstly, we selected the case of a video surveillance whose video signal is transmitted over radio up to a control centre. This case of study is derived from the monitoring systems that automatically trigger cellular phone communications in case of detection of abnormal situations like malicious or unauthorized intrusion. These systems can be inhibited using electromagnetic jammers. Secondly, we considered the case of a railway "netbox" equipment provided by Alstom. This product, designed for railway applications, provides wireless communication interface for all products embedded inside a rolling stock. During these demonstrations, the sensors have successfully provided the necessary input data to feed an Acquisition System (AS) connected to a Detection System (DS) so that the full system can decide if an electromagnetic attack really occurs and under which conditions.
**Deviations:** No deviations to the Description Of Work are reported for this task 3.5.
**Impacts:** Task 3.5 was an important step towards the proof of concept of the Secret resilient architecture. It has concentrated on the successful realization of the sensors needed by the AS/DS used in the demonstrations. The built sensors have proven to be more effective than the commercial build sensor and the overall system has been successfully demonstrated several times, including during the final SECRET conference. Such techniques could now be implemented on software defined radio platforms to provide reasonable cost jamming detection sensors widely available.

| **Statement on the use of resources** |
| --- |
| Slight increase in WP3 personal costs due to measurements performed by IFSTTAR personal (instead of initially forecasted subcontracting) and to the number of analysed detection techniques which was finally studied. |

## WP 4 - DYNAMIC PROTECTION: DETECTION SYSTEM FOR RESILIENT ARCHITECTURE

**Objectives :** This Work Package worked on a general communication architecture grouping requirements for interoperability and resilience to EM attacks. In order to dynamically cope with different EM attack conditions, the architecture integrates a health/attack management module (HAM), which is based on the inputs received from the acquisition systems defined in WP3. The HAM decides when an attack is taking place and how the communication architecture should adapt in order to face it.

### Task 4.1 Specification of the resilient architecture (M1-M11)
**Leader : EHU**

**Objectives**
The main objective of this task was to define an initial specification and design of a resilient architecture in terms of vulnerabilities to EM attacks. This initial specification will be later enhanced or amended as a consequence of the feedback obtained from the attack-centred evaluation carried out in T4.3. The final output is a resilient specification of the communication architecture.

**Progress towards the objective**
This task extends from M1 to M15 and so the main work of the task was carried out during the 1st period report. Deliverable D4.1 was finally finished during the 2nd period report. It was delivered for internal review in the M12 and was finally released in the M13 (in the 2nd period report) once applied the last contributions and required corrections. Then, from M14 on, the work in the WP4 was focused on the other tasks of WP4 in order to give a boost to them.

**Clearly significant results**
Deliverable D4.1 is the outcome of this task. This deliverable sets the design principles of the resilient communication system and so it was the basis for the rest of tasks of the WP4.

**Deviations, impact and correction**

**Deviations:**
As explained in 1st period report, D4.1 was originally scheduled to be delivered by M11 but it has been finally released by M13. This delay has been due to multiple discussions about the resilient architecture which has involved several audio conferences and face to face meetings.
**Impacts:** This delay may suppose a delay in other tasks that depend on D4.1, for example T4.2 and T4.3. However, on the one side, corrective actions were taken as explained later and on the other side task leaders are aware of the situation and the impact will be minimized.
**Corrections:** A solution to overcome the delay has been to increase the cooperation between tasks, to provide a higher level of parallelization between tasks and thus reduce the possible delays. Furthermore, T4.1 was finished before the M15, in M14, and the work capacity of WP4 was focused on other tasks, such as T4.3, to boost them. Thus, the impact of this delay in other tasks has been much contained.

**Task 4.2 Design of health/attack manager (M4-M15)**

**Leader : TRIALOG**

**Objectives**
The objective of this task is to design a dynamic protection system able to detect and dynamically cope with different EM attack conditions that may affect the communication among devices of the railway system. The deliverable D4.2 which is a result of this task is a refinement of the deliverable D4.1 (the result of T4.1) and is based on the outputs of WP3.

**Progress towards the objective**
The deliverable D4.2, the main result of this task specifies the dynamic protection system as two systems that are interconnected:

- The detection system which in turn is decomposed into two subsystems: the acquisition subsystem and the health/attack manager subsystem
- The multipath communication system which provides resilient communications between the onboard ERMTS and the on board heal/attack manager on one hand or between the RBC and the Central heal/attack manager on the other hand.

The annex of the deliverable describes an approach for the evaluation of the architecture. It will be used for the validation of the implementation through a use case, for example in D4.5. Recommendations have been identified for WP5.

**Clearly significant results**
The architecture of the dynamic protection system has been completely defined in the deliverable D42.
This deliverable has been submitted.
As mentioned in the previous periodic report, the delay of the deliverable was due to the delay of D4.1.

**Deviations, impact and correction**
Shift in deadlines but all the deliverables are provided.

**Task 4.3 Attack-centered assessment of the dynamic protection system**

**Leader Fraunhofer**

**Objectives**

The objective is to show that the attacks identified in the analysis carried out in the study phase of WP1 are effectively coped with at the dynamic protection level. In order to achieve this aim, a simulation based evaluation of the dynamic protection system (resilient communication architecture and health/attack manager) will be performed, using data farming in order to generate statistic data about the effectiveness of the dynamic protection system in different attack scenarios. Due to the iterative work methodology proposed within the SECRET project, this task will in fact consist of multiple repetitive phases.

The first phase is the assessment of the initial dynamic protection system as defined within Tasks 4.1 and 4.2. The result will be a refined, possibly amended architecture infrastructure, resilient compound network specification and health/attack manager specification.

Afterwards, the next phases will consist of the re-evaluation of the amended dynamic protection system in a closed loop. After each re-evaluation, the specification of the dynamic protection system might be accordingly modified. The final objective is to check that the attacks tried out on the implementation are effectively coped with at the dynamic protection level. An implementation specification will be provided.

**Progress towards the objective**

A comprehensive agent based model of the Secret domain was built-up: first, a generic model was created comprising generic descriptions of all involved technical systems with their physical, technical, and operational features. This includes the various health/attack managers investigated in Secret. In a second step, this generic model was instantiated in order to prepare the ground for concrete simulations. A concrete configuration of all relevant railway systems with fixed and moving components and systems including HAMs was built with their geo-spatial arrangements and operational characteristics.

**Clearly significant results**

A large number of different scenarios was investigated using concrete system configurations. Different attack modes, different temporal patterns and health/attack manager operations were simulated and analyzed. These models and simulations provided a very useful overall picture on the approach developed in Secret. It complemented the component view with its physical and technical characteristics by a system view bringing the interplay of all systems together.

The simulations of these models demonstrated that the Secret approach is fully adequate under a broad spectrum of physical, technical, and operational conditions.

**Deviations, impact and correction**

none

**Task 4.4 Implementation of the dynamic protection system (M12-M36)**

**Leader TRIALOG**

**Objectives**
The objective of this task is to implement the dynamic protection system specified in the task T4.2.

**Progress towards the objective**
This task has just begun. The D4.4, the main result of this task is due to M30.
The exact content of the demonstrator and of the risk analysis applied to the architecture will be finalized in September.

**Clearly significant results**
The platform, the development language and a repository (e.g. git svn) have been chosen.
The role of each partner has been defined.
The different steps of the development have been specified together with a calendar.

**Deviations, impact and correction**
N/A

**Task 4.5 Validation through Use Case**
Leader TRIALOG

**Objectives**
The objective of this task is to assess the effectiveness of the dynamic protection system from Task 4.4 to face EM attacks.

**Progress towards the objective**
During the 3rd period, Alstom developed a dynamic protection solution to test the resiliency of the communication between train and trackside in case of jamming of WiFi and 3G radio bearers.
Alstom engineers implemented two dedicated software components over one of its railway product “Netbox” : a Vertical Handoff algorithm (SEAMO) and a Mobile IP solution (open HIP) in order to manage the communication flows of an application running between the train and the ground.
The tests were performed in Alstom Charleroi together with the WP4 partners.
The test set-up and reports have been documented in “D4.5 Validation of the implementation through use case”

**Clearly significant results**
The test set-up proposed by Alstom allowed IFFSTAR to get additional results for the detection of 3G radio jammer. This allowed more results to be included in “D3.4 Assessment of the monitoring and detection solution: test report”.
The tests provided a second use case able to demonstrate the specific constraints of mixing WiFi with public mobile radio supplier, i.e. 3G. Generally, in this use case, we need to take into account the influence of the actual traffic load on the public 3G network in order to achieve acceptable performance of the dynamic protection. The algorithm needs to be configured accordingly and it is highly recommended to negotiate with the 3G operator an improved Quality of Service (QoS) user profile for railway application.

**Deviations, impact and correction**

Nothing to report

| **Statement on the use of resources** |
| --- |
| The efforts involved in this task have been mostly carried out by the University of the Basque Country, Trialog and Ifsttar with punctual collaboration of Alstom and SNCF.<br>No significant deviation for WP4 activities. |

## WP 5 - RECOMMENDATIONS FOR A RESILIENT RAILWAY INFRASTRUCTURE TO EM ATTACKS

**Objectives:** The WP5 aims to develop proposals for TecRec (Technical Recommendations). A TecRec is a UIC/UNIFE standard ( www.tecrec-rail.org ) designed to be used within the European region. In the case of SECRET, the TecRec will formalise the recommendations that individual companies may choose to mandate it through internal instructions/procedures or contract conditions.

### Task 5.1 Organisation of TecRec elaboration and synchronization activities (M1 to M16)

**Leader ALSTOM**

**Objectives :**
The WP5 aims to develop proposals for TecRec (Technical Recommendations). A TecRec is aUIC/UNIFE standard (www.tecrec-rail.org) designed to be used within the European region. In the case of SECRET, the TecRec will formalise the recommendations that individual companies may choose to mandate it through internal instructions/procedures or contract conditions. The task 5.1 consists in a process and a reference list of recommendations coming from the different WP and evoluting al along the project.

**Progress towards the objective**
With working with all involved WP's (1,2,3,4), preliminary list of potential recommendations have been identified and listed in an unique document. Next step is a formal review during steering committee to sort TecRec candidate to push toward UIC/UNIFE for deeper investigation and starting communication to those organism.
Contact with TecRec authorities to define way of working with consortium have been established

**Clearly significant results**A draft list of recommendations has been redacted; now ready to help UNIFE/UIC members to communicate with commissions.

**Deviations:**
The issue of jamming with respect to the rail system is studied for the first time through the SECRET project. This is a very recent issue and it is unlikely that UIC/UNIFE members quickly find an agreement to issue a recommendation. There is a risk of incompatibility with project duration.
**Impacts :**
UIC/UNIFE TecRec recommendation process is very long, major risk of incompatibility with project duration.
**Corrections:** Different standardisation bodies can be concerned by the recommendations issues from SECRET. In consequence, efforts are made to improve contact with standardisation bodies such as IEC (SC77C) to provoke evolution of standards regarding the immunity of civilian infrastructure against intentional electromagnetic interferences. The IEC SC77C accepted to take into account SECRET analysis and an annex on "jammers" will appear in a upcoming publication IEC 61000-4-36. We exchanges with the chairman of the IEC (SC77C) to contribute to the enrichment of this appendix.

**Task 5.2. TecRec preventive and recovery measures (M13-M36)**

**Leader ALSTOM**

**Objectives**

The objective is to define from the studies in WP1 a template of Security File that will be used as a generic guideline for a first understanding and management of security issues in a transportation system. The Security File will include a rationale for risk and threat analysis and a list of consequences and responses (preventive and recovery measures) to the EM attacks on railway networks SECRET will have analysed.Task 5.2, moving from the findings emerged in WP1, aims at defining a template of “Security File” that will be used as a generic guideline for a first understanding and management of security issues in a transportation system.

**Progress towards the objective**

D5.2 provided 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.

**Deviations, impact and correction**

N/A.

**Task 5.3. TecRec static hardening rules**

**Leader Polito**

**Objectives**

Regarding SECRET results to be proposed, we plan to develop recommendations on the way to design the infrastructure devices (methodologies, hardening rules...), on the EM attack management (detection, signature...) and design rules to ensure resilience of services.

The elaboration of Technical Recommendations (TecRec) will be made with a strong coordination with SECRET project members, ensuring the development of project results that will fit with of TecRec principles, and using the path offered by our partners, particularly UIC and its Security WG (involved in projects like ProtectRail and SECUR-ED).

**Progress towards the objective**

During the 3rd period, Polito collected, fulfilled and analyzed all technical recommendations issued from WP 2. The process and TecRec classification defined in D5.1 has been used.

Polito provided a deliverable D5.3 including five major recommendations and Alstom reviewed this deliverable. The recommendations were selected and organized to publish a white paper

Based on the results of WP2, and based on the analysis of standards, a TecRec was developed to specify the rules to be applied in the design (including the test phase), certification and deployment, up to the intervention during the maintenance and modification phases of critical equipment.

**Clearly significant results**

Five major recommendations to avoid and minimize the impact of jamming on the systems, and for the improvement of the network, and contributions to a white paper on recommendations.

**Deviations , impact and correction :**

**Deviations:**

The UIC TecRec process was not used during Secret project because the UIC TecRec process was not anymore alive. No other process has been identified.

**Impacts:** The WP6 Exploitation and dissemination refocused the way TecRec should be used. This work also produced recommendations for future practical implementations

**Corrections:** Finally, we decided to publish a white paper.

**Task 5.4. TecRec specification for EM attack detection**

**Leader Alstom**

**Objectives:**
Based on the results of WP3 (including the results of the test bed) the TecRec will define the situations and operational environments in which attacks can occur and by which EM attack detection devices can be detected. This proposal for TecRec will be issued to the UIC and UNIFE working groups.

**Progress towards the objective**

During the 3rd period, Alstom collected and analyzed all technical recommendations produced by WP 3. The process and TecRec classification defined in D5.1 has been used.

The WP3 recommendations were developed in "D5.4 Proposal for TecRec on EM attack detection".

**Clearly significant results**

Thirteen recommendations were extracted from the task 5.4. All these recommendations were compared to the recommendations issues from the other task of the WP5 to constitute a complete and coherent white paper on SECRET recommendations.

**Deviations, impact and correction**

**Deviations:**

The UIC TecRec process was not used during Secret project.The UIC TecRec process was not anymore alive. No other process has been identified.

**Impacts :** The WP6 Exploitation and dissemination refocus the way TecRec should be used.

**Corrections:**

Finally, we decided to publish a white paper.

**Task 5.5. TecRec specification for EM attack detection**

**Leader Trialog**

**Objectives:**

Regarding SECRET results to be proposed, we plan to develop recommendations on the way to design the infrastructure devices (methodologies, hardening rules...), on the EM attack management (detection, signature...) and design rules to ensure resilience of services.

The elaboration of Technical Recommendations (TecRec) will be made with a strong coordination with SECRET project members, ensuring the development of project results that will fit with of TecRec principles, and using the path offered by our partners, particularly UIC and its Security WG (involved in projects like ProtectRail and SECUR-ED).

The objective of this task is to deliver a TecRec specifying the typical architecture that offers qualities like resilience, but also traditional qualities like authentication, confidentiality, integrity… Thanks to the high level of standardization in the railway domain the deployment of such architecture will be facilitated.

**Progress towards the objective**

During the 3rd period, Alstom collected and analyzed all technical recommendations produced by WP 1 to 4. The process and TecRec classification defined in D5.1 has been used.

The WP1 recommendations were developed in “D5.2 Proposal for TecRec on preventive and recovery measures” and the WP3 recommendations were developed in “D5.4 Proposal for TecRec on EM attack detection”.

Alstom also reviewed “D5.3 Proposal for TecRec on static hardening rules” and “D5.5 Proposal for TecRec on redundancy for resilient architecture” respectively established by Polito and Trialog.

**Clearly significant results**

The WP5 work provided an exhaustive collection of TecRec established by all Secret project WPs which will be used in WP6 Exploitation and dissemination.

**Deviations, impact and correction**

**Deviations:**

The UIC TecRec process was not used during Secret project because the UIC TecRec process was not anymore alive.

**Impacts :** The WP6 Exploitation and dissemination will refocus the way TecRec should be used.

**Corrections:**

Finally, we decided to publish a white paper.

| **Statement on the use of resources** |
|---|
| Slight underspending in task 5.1. |

# WP 6 EXPLOITATION & DISSEMINATION

**Objectives :** The main goal of this WP is the dissemination and exploitation of the results via cross-fertilization between Security and Railway stakeholders and end users. The expected dissemination of the results will take place at three levels:

- Dissemination and discussion of the initial results among the Advisory Board inside the project;
- Technology and business transfer to the end user community outside the project;
- Dissemination to the scientific community.

**Task 6.1 Setting up of Dissemination tools M1-M40**

**Leader UIC**

**Objectives**

The objective is to set up the various tools to ensure a continuous dissemination of the project activity and results in and out the consortium

**Progress towards the objective**

The main tools for raising awareness on the project and for communication have been implemented during the first period. Information was regularly updated in the public and private website during the third period.

**Clearly significant results**

- Maintenance and update of the SECRET website
  - *http://www.secret-project.eu/*
- Maintenance and update of the SECRET workspace (*http://extranet.uic.org*)
  - Management of users.
  - Addition of documents: official and working documents.
  - Update of the calendar of meetings.
- Maintenance and update of the 3 existing mailing lists and creation of a new one for WP4
- Regular information on SECRET was given in UIC enews (UIC electronic letter on projects and activities with more than 5000 addressees)
- Press release for the final conference
- Production of 3 rollups for the final conference

**Deviations, impact and correction**

No deviation

**I**

**Exploitation and Dissemination**

**Task 6.2. Exploitation and Dissemination of Results M1-40**

**Leader UIC, ZANASI**

**Objectives**

Task 6.2 is dedicated to the exploitation/dissemination of the results produced throughout the project, to be carried out by means of several initiatives: publications, conferences, workshops, press releases, relations with local authorities, etc. ZANASI, specifically, is in charge of disseminating amongst security stakeholders.

**Progress towards the objectives**

Deliverable D6.1 on Final exploitation plan

Deliverable D6.4 on SECRET summary report

**A White paper**

2 events organized :

- 28 January 2015, in Paris, UIC HQ : workshop on "How to protect signalling system against cybercrime" : Focus on the SECRET and UIC Argus project
- 28 October 2015, in Lille, IFSTTAR, France: Final conference

Presentation of the project in various seminars and conferences gathering together end users and/or security experts and/or researchers

- 14-15 September 2014, in Vancouver: 6th IEEE International Symposium on Wireless Vehicular Communications (WIVEC2014)
- 24-26 November 2014, in Rennes, France : C&ESAR 2014 : Détection et réaction face aux attaques informatiques
- 26-28 November 2014 in Lisbonne, Portugal : UIC world security congress
- 18-25 May 2015, Gran, Canaria, Spain: URSI Mid-Atlantic Meeting 2015
- 06 May 2015, Sousse, Tunisia : Nets4trains 2015 : International Workshop on Communication Technologies for Vehicles
- 16-22 August 2015 in Dresden, Germany: EMC 2015: Joint IEEE International symposium on electromagnetic compatibility and EMC Europe
- 15-16 September 2015 in Paris, UIC HQ : 2nd UIC World GSM-R Conference
- 15-18 September 2015, in Las Palmas de Gran Canaria, Spain: IEEE - ITSC 2015 - Smart Mobility for Safety and Sustainability
- 14-16 October 2015 in Palma de Mallorca, Spain : JITEL 2015 Conference
- 09-13 November 2015, Barcelona, Spain : 2nd International Workshop on Management of SDN and NFV Systems

We also produced a supplementary D6.4 deliverable which was included in the last amendment. This DL is a summary report of the whole SECRET project, which comprises of a short and easily understandable description of the equipment and technologies investigated during the project, the risks that have emerged (including the methodology used for estimating them) and the recommendations for their mitigation. Contributions to D6.4 have also been provided by POLITO and SNCF.

**Clearly significant results**

D6.4 immediately addresses a need expressed by the Commission services during a project meeting in September 2014. The Commission services asked for a clear and concise

summary report, which could help them, as well as the security stakeholders, in benefiting the most from the results of the project..

Publications : around 20 scientific publications or articles in conferences

A white paper grouping all the SECRET recommendations

**Deviations, impact and correction**

No deviations compared to what specified in the Grant Agreement following the latest amendment (Grant agreement version date: 2015-07-10).

**Task 6.3 Targeted transmission for Co-Restreint UE deliverables (M6-M40)**

**Leader UIC**

**Objectives**

The objective is to manage the production and the transmission of the confidential or restreint UE deliverables

The concerned deliverables are D1.1, D1.2, D1.4, D1.5, D1.7, D2.1, D2.2 and D2.4.

**Progress towards the objective**

The rules defined within M6.18 were applied.

**Clearly significant results**

All the Co- restreint UE deliverables were provided to the commission in respecting the SECRET process for protection of the information.

**Deviations, impact and correction**

No deviation

# WP 7 – TECHNICAL MANAGEMENT

**Objectives :** The objective of this Work Package is to ensure that the project is able to achieve high quality results and to guarantee the systematic scientific monitoring of activities throughout the project. To support the scientific coordination, quality assessment will be implemented

## Task 7.1 Technical management (M1 to 40)

**Leader Ifsttar**

**Objectives**

The technical management task aims:

- to ensure the scientific actions of management and coordination of the activities among the WPs,
- to ensure the inter-relation of the Work between the different WPs,
- to take charge of the scientific monitoring actions,
- to take care of the scientific quality of both the work done and the deliverables.
- to take care of the management of the Advisory Committee

**Progress towards the objective**

The project manager ensured the project coordination taking into account the recommendations issued from the project review and all inputs received from the partners.

During the 3rd period, 5 technical meetings took placed to coordinate the technical actions and three experimentation weeks involving several partners were planned to carry out complementary measurements, demonstrations and results assessments.

**Clearly significant results**

Thanks to the technical coordination, real-time demonstrations were held in front of the participants during the final conference of the project. Four different demonstrations were presented to the participants during the final conference of the project: demonstrations about jamming impact, jamming detection, immunity test bench to intentional interferences and resilient communication solution in presence of EM attack. The possible implementations were also presented and how to cope with the effect of the jammer. In the afternoon, participants were shown an example of resilient architecture for a dynamic protection system to EM interferences for railway applications.

**Deviations:**

No deviation

**Impacts**

No impact

**Corrections:**

No need for corrective actions

**Task 7.2 Quality assessment (M1 to 40)**

**Leader Ifsttar**

**Objectives**
The objective is to support the actions of the administrative manager and of the technical manager through some quality processes such as peer review processes

**Progress towards the objective**
The reviewing process was applied for each deliverable in order to control the quality of the production.

**Clearly significant results**

All the deliverables were provided in time in respecting the quality review process.

**Deviations:**
No deviation

**Impacts**
No impact

**Corrections:**
No need for corrective actions

## WP 8 – ADMINISTRATIVE AND FINANCIAL MANAGEMENT

The workpackage is in charge of the project organisation and the management of the project activities.

The main objective is to lead the SECRET project, co-ordinate the work of the different work packages and ensure work progress according to the plan. It will ensure that the project is able to achieve high quality results and guarantee the systematic monitoring of activities throughout the project

**Task 8.1 Administrative and financial management (M1-M40)**

**Leader ERT/Ifsttar**

**Objectives**

The aim of the administrative management is to coordinate and to ensure a continuous monitoring of the project, in accordance with the grant agreement and its annexes, and to prepare the periodical and final reports using the inputs of the work package leaders.

**Progress towards the objective**

We had to face major changes for SECRET's administrative coordination, as the relating partner ERT merged with Ifsttar on 1rst January 2014 and from project administrative coordinator on September 2014.

Our Project officer also changed on April 2015.

Nevertheless, 12 consortium meetings were organized, including the General Assembly in Brussel on Sept. 2014 and the final conference in Villeneuve d'Ascq on October 2015.

1rst, 2nd and final periodic reports have been completed and submitted. According to discussion with our Project Officer, 3rd and final periodic reports have been merged in a same document.

**Clearly significant results**

- 5 amendments have been implemented during the project duration
- 3 project reviews
- 3 meetings with the advisory committee

**Deviations:**

- Project duration has been extended from 36 to 40 months
- 5th amendment allowed to update SECRET's DoW and some important changes, such as the introduction of ALSTOM Transport (France) as ALSTOM Belgium 3rd party, budget transfers between ERT as former partner and Ifsttar,…

**Impacts**

No impact

**Corrections:**

No need for corrective actions

**Task 8.2 security management (M1-M40)**

**Leader ERT/Ifsttar**

**Objectives**
- setting up and monitoring the rules dedicated to the management of the security aspects of the project.
- implementing a process to ensure the respect the level of confidentiality needed for the sensitive data (clearance level, restricted readers, data transmission rules)

**Progress towards the objective**
Management of sensitive material security :
The “confidential” mention has been put on any material linked with this list and presented inside the consortium. This provision applied also to any information out the perimeter of a documents’ list for information judged confidential by any partner.

A group of referent persons (security board) has been set and any dissemination outside the consortium involving sensitive information linked with this list must be approved by each of those referent persons.

**Clearly significant results**
- Use of encryption tools for sensitive information
- Secured transmissions between partners

**Deviations:**
No deviation reported

**Impacts**
No impact

**Corrections:**
No need for corrective actions

| **Statement on the use of resources** |
|---|
| No deviation. |

# 3 Project management during the period

## 3.1 Contractual and financial management

Upon the 5 amendments which have been implemented during SECRET's duration, two amendments were issued and finalized during the last period

- Amendment n° 4 (Change of project manager –Ifsttar-, change of legal representative - Alstom)
- Amendment n°5 (update of SECRET's DoW, taking into account budget readjustment for some partners, task share between Alstom Belgium and Alstom Transport (France) created as 3rd party, and budget transfer from former partner ERT to Ifsttar)

## 3.2 Management tasks and achievements

**Consortium meeting arrangements:**
During the project duration, the two days format meeting used for the consortium meetings enabling at least two sub-group technical works (WP meetings) and plenary sessions.

**Advisory Committees**

**SECRET** management kept constantly in touch with its Advisory Committee whose members have been informed on the Project results and invited to join meetings and activities.

The 2nd Advisory Committee was formally held on September 16th, 2014 in Brussels (ECTRI premises).
A list of Scientific and end user representatives was built during previous consortium meetings. They were chosen *intuitu personae* for their experience and specific added value in the field.
The four participating members for this 2nd meeting were:

- Mr Albert FERNANDES, Disruptive Technologies, QinetiQ
- Mr Jose Manual NEVES, REFER
- Mr Alfonso DIEZ PEREZ, Director de Telecomunicaciones - ADIF
- Mr Max SCHUBERT, Head of I.NVT 342 Technologymanagement for Level Crossings, Signals, UPS
-

The scope, results, next actions of active tasks for each WP were presented (for non classified subjects).

Discussion took place in relation to end user specific situations and scientific aspects.

Despite of gathering a 3rd Advisory Committee during the project Final Conference on October, the 29th, 2015, we invited the members to join and share their questions and point of vue.
Were present in Lille :

- Albert FERNANDES
- Richard HOAD
- Alexei OZEROV
- Dominique SERAFIN
- Chaouki KASMI

## 3.3 Problems which have occurred and how they were solved or envisaged solutions

**The problems met during the 3rd period were more relating to financial and administrative issues and did not impact the scientific agenda.**

Day-to-day collaboration between researchers and industrials (ALSTOM, SNCF and Trialog) can be considered as very good.

Some difficulties occurred in finding available and relevant trains to perform measurement campaigns; this induced little additional delays.

After the merge of ERT into IFSTTAR (UTRO), the change of coordinator contact occurred minor administrative delays.

All the partners were very constructive to propose, validate and adopt operational procedures meeting the specific needs of the project regarding the management of sensitive information (dual use). The security management plan is well understood and applied by each partner. The deployment of the encryption for sensitive documents has been globally well handled by relevant partners. Alternative solutions were found to be more adequate in some cases (3 envelopes with SNCF).

The only change of partner structure occurred in ALSTOM organization. An amendment was forecasted to consider ALSTOM France identified in the consortium as a third party for ALSTOM Belgium.

## 3.4 List of project meetings, dates and venues (3rd period)

**3nd technical review**
The 3nd technical review took place in Villeneuve d'Ascq on Oct 30th 2015, with most deliverables submitted and status for all relevant activities presented. A representative of each partner was present.

The project meetings were attended by all partners during the last period.

**MT8 (UIC) in Paris, January 27th, 2015.**

Progress of WP1, WP 2, WP3, WP4, WP6, WP7, and WP8 was reviewed. A joint workshop with ARGUS project and partners has been organized in UIC premises on January the 28th 2015.

**MT9 (Ifsttar) in Villeneuve d'Ascq, April, 17th, 2015.**

Progress of WP1, WP 2, WP3, WP4, WP5, WP6, WP7, and WP8 was reviewed. All partners discussed the amendment 5 issues and proposed a meeting with EC Project Officer.

**Meeting with SECRET's new Project Officer, Brussels, June 10th, 2015**
Mr Chenard as new PO requested information on SECRET's last issues. Efforts and difficulties met during the first months of the project were presented by Ifsttar and Alstom Belgium. Mr Chenard gave his agreement to extend the project until November, the 30th, 2015.

**Meeting with SECRET's financial officer (and PO), Brussels, June 39th, 2015**
Ifsttar requested this "technical" meeting for the 5th amendment preparation.

**MT10 (Ifsttar) in Villeneuve d'Ascq, July 2nd and 3rd, 2015.**

Progress of WP1, WP 2, WP3, WP4, WP5, WP6, WP7, and WP8 was reviewed. All partners were informed on discussions with the new PO and prepared the final conference.

**2nd Advisory Committee**
The 2nd Advisory Committee was held on September 16th, 2014 in Brussels (ECTRI premises)

**Scientific workshop & final conference preparation**
SECRET's partners were present at Ifsttar Villeneuve d'Ascq from October, the 26th to the 28th to improve the scientific tests to be shown during the Final Conference.

**Final Conference & project review**
The final conference and the project review where held in Villeneuve d'Ascq on October the 29th, 2015.
The final conference gathered 85 participants.

## 3.5 Project planning and status

There is no significant deviation from the planning for scientific activities.

## 3.6 Impact of possible deviations from the planned milestones and deliverables

The late issue of D4.2 had no impact to check on the planned deliverables since these documents were presented and discussed quite early in the project course.

## 3.7 Changes to the legal status of any of the beneficiaries, in particular non-profit public

ERT merged into IFSTTAR as of 1/1/2014 (UTRO procedure).
ALSTOM Transport has been introduced as 3rd party for ALSTOM Belgium during the 3rd period.

## 3.8 Definitions and acronyms

| Acronym | Meaning |
|---|---|
| BTS | Base Transceiver Station |
| CENELEC | Comité européen de normalisation en électronique et en électrotechnique |
| DES | Discrete Event Simulator |
| EIRENE | European Integrated Railway Radio Enhanced Network |
| EM | ElectroMagnetic |
| EMC | ElectroMagnetic |
| EN | European Standard |
| ERTMS | European Railways Traffic Management System |
| ETCS | European Train Control System |
| ETSI | European Telecommunications Standards Institute |
| EVM | Error Vector Magnitude |
| FMEA | Failure Mode and Effect Analysis |
| GSM | Global System for Mobile communications |
| GSM-R | Global System for Mobile communications - Railways |
| HSL | High Speed Line |
| IEC | International Electrotechnical Commission |
| IEMI | Intentional Electromagnetic Interference |
| LGV | Ligne à Grande Vitesse (HSL) |
| MM | Men Month |
| p.s.d | Power spectral density |
| RBC | Radio Block Centre |
| RF | Radiofrequency |
| RFF | Réseaux Ferrés de France |
| SC | Subcommittee |
| SNR | Signal-to-Noise Ratio |
| TC | Technical Committee |
| TecRec | Technical Recommendation |
| TETRA | Terrestrial Trunked Radio |
| TGV | Train à Grande Vitesse |
| UIC | Union internationale des chemins de fer |
| UNIFE | Union des Industries Ferroviaires Européennes |
| WP | Workpackage |