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 4.1

Preliminary specification of the dynamic protection system

Submission date: 30/08/2013

Deliverable on Dynamic Protection System
Date: 30/08/2013
Distribution: All partners
Manager: EHU

Document details:

Title	Preliminary specification of the dynamic protection system
Work package	WP4
Date	30/08/2013
Author(s)	E Jacob (EHU), M Higuero (EHU), C Pinedo (EHU), C Gransart (IFSTTAR), M Heddebaut (IFSTTAR), A Kung (TRIALOG), M Sall (TRIALOG)
Responsible Partner	EHU
Document Code	SEC-D4.1-C-082013-Preliminary specification of the dynamic protection system-EHU
Version	C
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
1.1	27/08/2013	EHU IFSTTAR TRIALOG	Internal review of the document by Alstom and corrections by the authors of the document.
1.0	24/07/2013	EHU	Version for internal review. Minor changes. EHU.
0.9	23/07/2013	EHU IFSTTAR TRIALOG	- Review and changes in section 3.1. EHU. - Section 3.2. EHU. - Section 3.3. EHU. - Initial version of section 4, Approach to justify SECRET resilient architecture. TRIALOG and comments of EHU. - Second version of the Acquisition System. IFSTTAR & EHU.
0.5	03/07/2013	EHU IFSTTAR TRIALOG	- Initial version of section 3.1, State of the art of ERTMS. IFSTTAR. - Initial version of section 4, Approach to justify SECRET resilient architecture. TRIALOG. - Enhanced version of section 5, Architecture for resiliency. EHU. - Initial version of the Acquisition System. IFSTTAR.
0.2.1	17/06/2013	EHU	- Initial version of section 5, Architecture for resiliency. EHU.

Table of content

1 Executive summary

The objective of the dynamic protection system is to detect and dynamically cope with different EM attack conditions that may affect the communication among devices of the railway system. In this deliverable a preliminary view of this dynamic protection system is presented.

2 Introduction

2.1 Purpose of the document

The purpose of the Deliverable 4.1 is to present a preliminary view of the resilient architecture in order to face EM attacks. After analysing the main subsystems that take part in the rail network operation and the communications among them, an initial resilient railway communication architecture in terms of vulnerability to EM attacks is described in this deliverable. This deliverable will be the basis for the specification of the resilient architecture that will be developed along the remaining work of the Work Package 4.

The document consists of 3 main sections. One first section consisting of the state of the art regarding ERTMS that presents not only important concepts of the signalling system but also some resiliency issues and the possible evolution of the ERTMS beyond the current version of the standard.

The second section is focused on presenting a risk management methodology that will be applied to the SECRET resilient architecture in order to assure that the resiliency objectives are covered with the proposed architecture.

Finally, the last and most important section of the document is the preliminary presentation of the resilient architecture. This section firstly provides the general ideas and concepts the architecture is based on and the application scenarios covered. Then, the two systems the architecture consists of are explained separately.

2.2 Definitions and acronyms

	Meaning
API	Application Programming Interface
AS	Acquisition System
BSC	Base Station Controller
BTS	Base Transceiver Station
CHAM	Central Health/Attack Manager
DS	Detection System
DSS	Detection SubSystem
EDGE	Enhanced Data Rates for GSM Evolution
EM	Electromagnetic
ERTMS	European Railway Traffic Management System
ETCS	European Train Control System
ETML	European Traffic Management Layer
EVC	European Vital Computer
FMEA	Failure Mode and Effect Analysis
GSM	Global System for Mobile communications
GSM-R	Global System for Mobile communications - Railway
GPRS	General Packet Radio Service
HAM	Health/Attack Manager
HIP	Host Identity Protocol
HSPA	High-Speed Packet Access
ICT	Information and Communications Technology

IP	Internet Protocol
LEU	Lineside Electronic Unit
LTE	Long Term Evolution
MCS	Multipath Communication System
MIP	Mobile IP
MPTCP	Multipath TCP
MSC	Mobile Switching Centre
OHAM	On-board Health/Attack Manager
PDU	Packet Data Unit
RBC	Radio Block Centre
RIU	Radio In-fill Unit
RMS	Railway Management System
TETRA	TErrestrial Trunked RAdio
TCP	Transmission Control Protocol
THAM	Trackside Health/Attack Manager
TVRA	Threat and Vulnerability Risk Assessment
UMTS	Universal Mobile Telecommunications System
WiMAX	Worldwide Interoperability for Microwave Access
WP	Work Package

3 State of the art

3.1 European Railway Traffic Management System (ERTMS)

European Railway Traffic Management System (ERTMS) is the signalling and management system for the railway sector driven by the European Union whose initial and main objective is to ease the interoperability of railway infrastructures between countries that are member of the European Union. One of the several reasons of the lack of interoperability in the railway sector was the existence of more than 20 signalling and management systems for the railway traffic management inside the European Union. ERTMS was the proposal of the European Union to replace them and homogenize the signalling system of the European railway network.

This section provides a brief introduction to the main characteristics of ERTMS and it is written base on the publically available documentation about ERTMS (1) (2) (3).

3.1.1 Architecture

The ERTMS consists of 3 main components, as it is shown in the Figure 1.

- The GSM-R component manages the communications.
  The aim of this component is to provide voice and data communications between the railway staff, which may be a mobile item (the most representative perhaps is one train), and the Railway Control Centre (RBC), which is a fixed point. It is based on the GSM standard and it has been designed to support high speeds (up to 500 km/h). In Europe, it uses a specific frequency band to avoid disturbances due to other services:
  - Uplink: 876 – 880 MHz
  - Downlink: 921 – 925 MHz

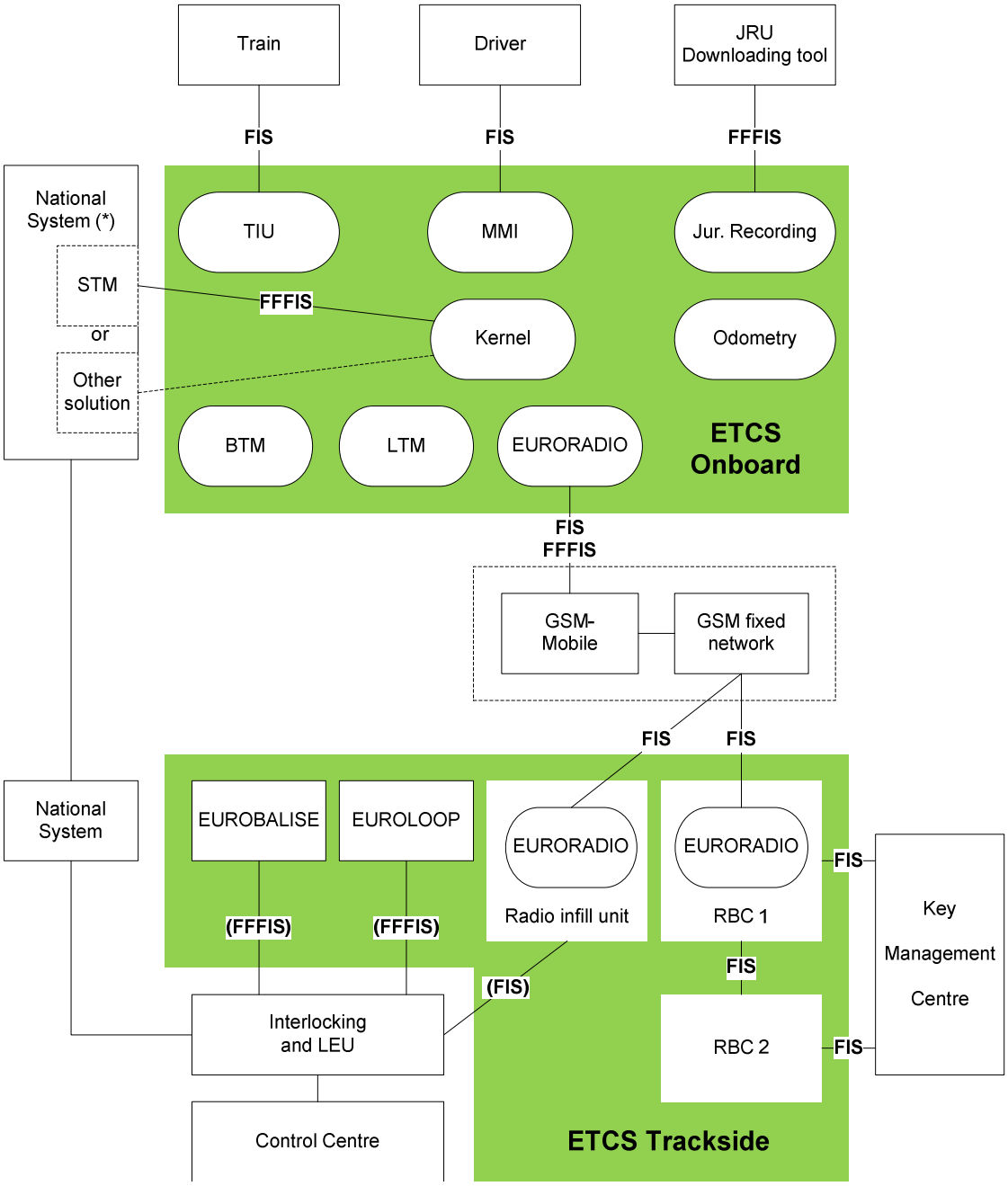
- The ETCS component manages the protocol between the train and trackside equipment including the Radio Block Centre (RBC).
  ETCS is the signalling protocol of the ERTMS architecture. It was designed to replace many incompatible signalling systems that were being used in Europe and it was especially designed for supporting high-speed lines.

- The ETML (European Traffic Management Layer) component is a high level component outside of the scope of this deliverable.
  This component should optimise train movements thanks to the intelligent interpretation of timetables and train running data.

Figure 1: Main components of ERTMS.

ERTMS architecture consists of two subsystems, the on-board subsystem located in the train and the track

subsystem. The communication between both subsystems may be based on different wireless communication technologies, one of them may be GSM-R, but the specific wireless technology used will depend on the ERTMS Level deployed in the track.



(*) Depending on its functionality and the desired configuration, the national system can be addressed either via an STM using the standard interface or via another national solution

Figure 2: ERTMS/ETCS architecture.

The main components of the on-board ERTMS command/control subsystem are:

- The on-board computer-based system, the *European Vital Computer* (EVC), which elaborates the information about the train circulation and the movement authority.
- *GSM-R mobile unit* for the bidirectional radio communication between ERTMS train borne system and *Radio Control Block* (RBC) trackside communication.

- *Odometry*, which provides information about train position, speed and driving direction to the EVC.
- *Driver Machine Interface*, which interfaces the driver with the EVC displaying vital information for the train circulation.
- *Balise Transmission Module* and *Train Transmission Module,* which pick up the information from Eurobalises and Euroloop.

The main components of the trackside ERTMS command/control subsystem are the following ones:

- *Eurobalise.*
- *Euroloop.*
- *Lineside Electronic Unit* (LEU), the encoder that connect Eurobalises and Euroloop to the signalling system.
- *Radio In-fill Unit* (RIU), which is used in ERTMS Level 1.
- Trackside radio communication equipment distributed along the railway line.
- *Radio Block Centre* (RBC), which is a computer-based system that sends information to the on-board system taking into account the data received by the interlocking and ERTMS itself.

In relation to GSM-R communication, in the following figure, Figure 2, it is presented a simplified diagram of the interfaces and relations between the components of the ERTMS involved in a GSM-R communication between trackside and on-board equipment.

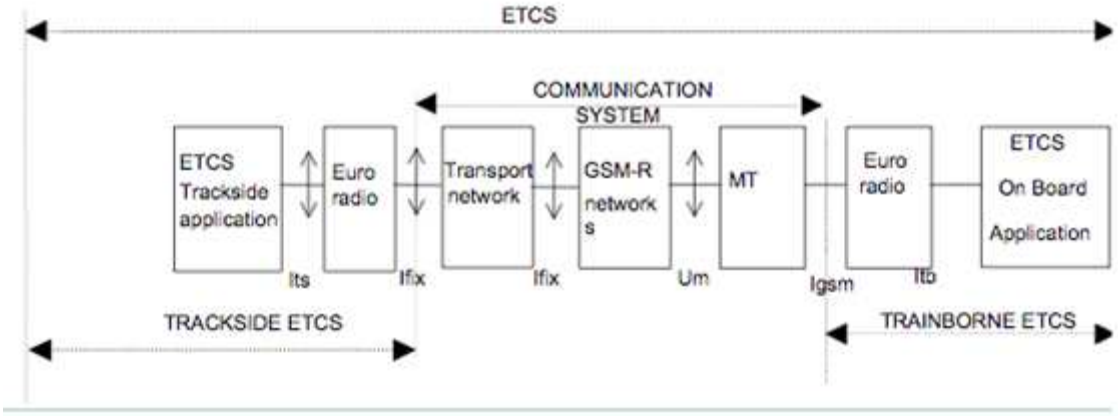


Figure 3: ETCS scope (trackside and train borne).

In Figure 4, once again in the case of using GSM-R, the relations between the different protocols are shown. The diagram shows two protocol stacks for each device, one protocol stack for the circuit management and another one for data transmission once the circuit has been established. For the circuit management, GSM and digital telephone signalling protocols are used. For data transmission (transmission of ETCS messages), standard protocols like X.224 and T.70 are used whereas the Euroradio layer (identified in Figure 4 as “Safety Layer + KM”) offers an end to end secure communication and the application layer is composed of ETCS messages.

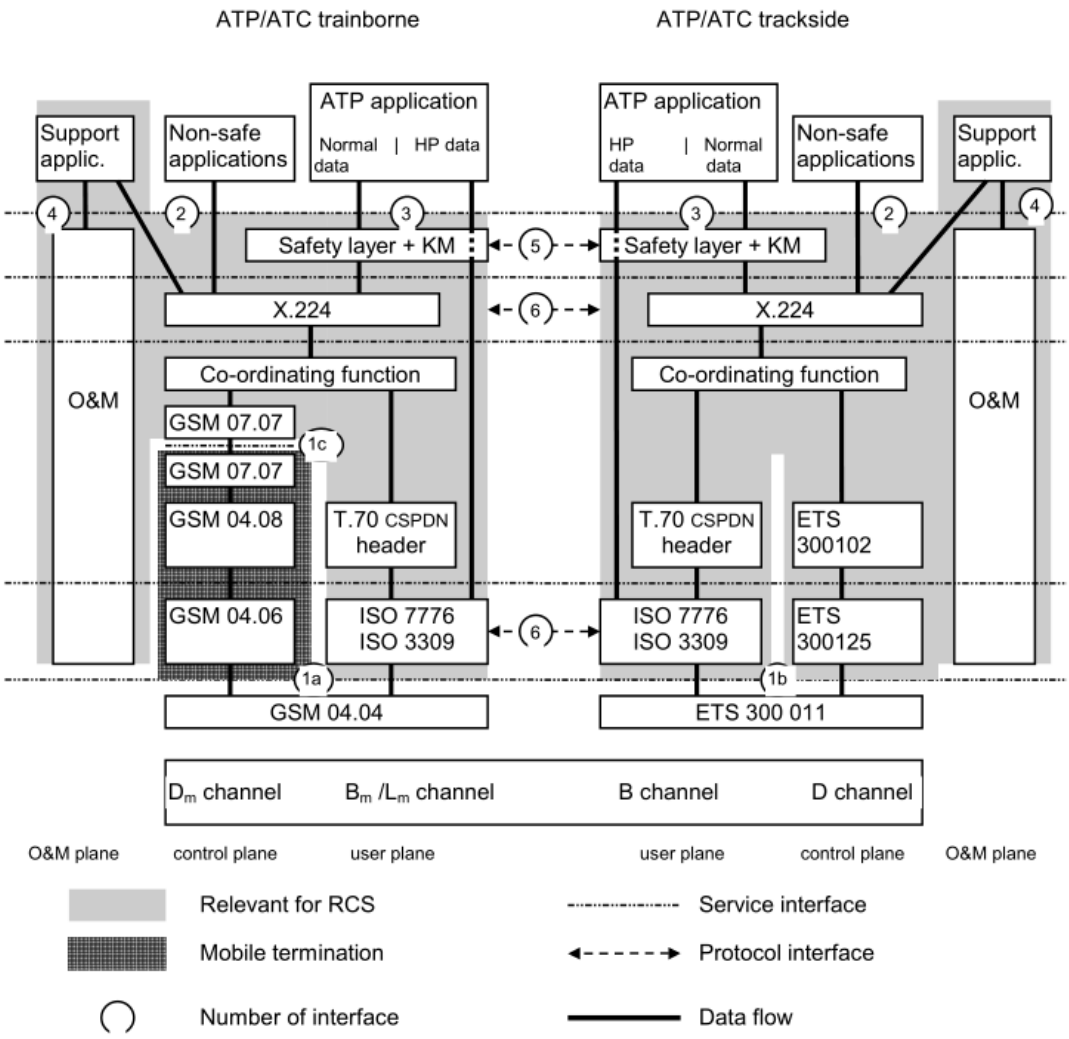


Figure 4: Protocol stack.

3.1.2Levels of ERTMS

There are several levels of ERTMS, which require different kind of technologies and are designed to offer different grades of rail line capacities. This section describes briefly these levels.

3.1.2.1 ERTMS Level 0

Level 0 covers operation of ETCS equipped trains on lines not equipped with ETCS or national systems or on lines where trackside ERTMS/ETCS infrastructure and/or national systems may exist but operation under their supervision is currently not possible (e.g. commissioning or on-board/trackside failed components).

In Level 0 it is authorized to operate trains without any train control system and therefore line side optical signals or other means of signalling are used to give movement authorities to the driver.

3.1.2.2 ERTMS Level STM/NTC

This level is called STM (Specific Transmission Module) in ERTMS specification 2.3 and NTC (National Train Control) in the specification 3.3.

Level NTC is used to run ERTMS/ETCS equipped trains on lines equipped with national train control and

speed supervision systems.

Train control information generated trackside by the national train control system is transmitted to the train via the communication channels of the underlying national system. Lineside optical signals might be necessary or not, depending on the performance and functionality of the underlying systems.

The achievable level of supervision is similar to the one provided by the underlying national systems.

3.1.2.3 ERTMS Level 1

Level 1 system relies on balises embedded in the track to provide updates to the train borne system about its authority to proceed.

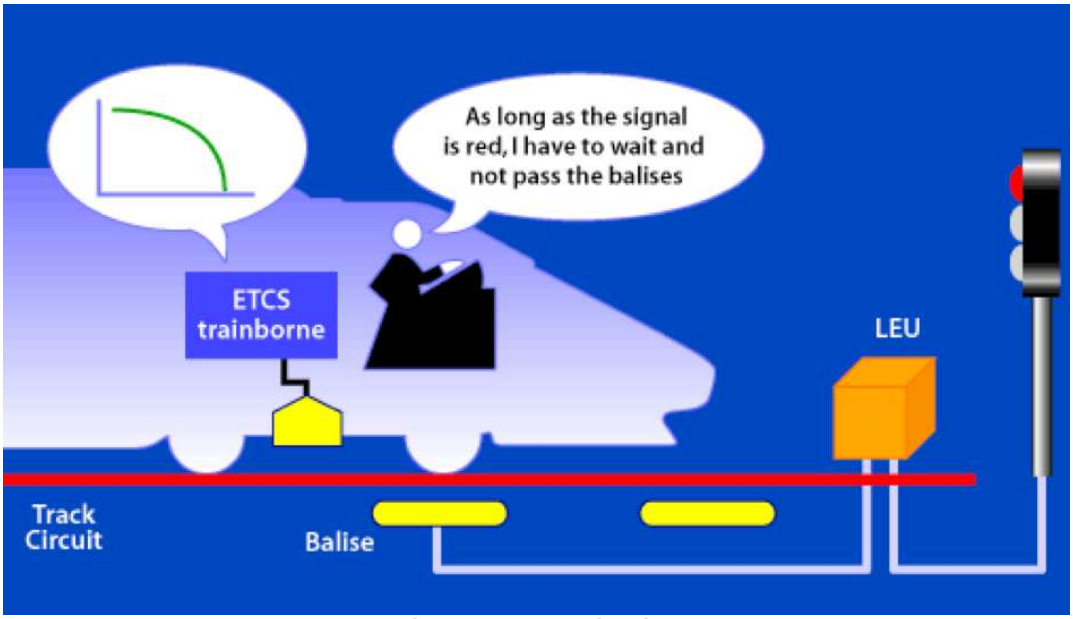


Figure 5: ERTMS level 1.

ERTMS level 1 is designed as an add-on to or overlays a conventional line already equipped with lineside signals and train detectors. Communication between the tracks and the train are ensured by dedicated balises (known as “Eurobalises®”) located usually on the trackside adjacent to the lineside signals at required intervals, and connected to the train control centre. Receiving the movement authority through Eurobalises, the ETCS on-board equipment automatically calculates the maximum speed of the train and the next braking point if needed, taking into account the train braking characteristics and the track description data. This information is displayed to the driver through a dedicated screen in the cabin. The speed of the train is continuously supervised by the ETCS on-board equipment.

The main benefits brought by ERTMS Level 1 are interoperability (between projects and countries) and safety, since the train will automatically brake if exceeding the maximum speed allowed under the movement authority.

3.1.2.4 ERTMS Level 2

Level 2 systems use a radio-link to provide updated authorities to the train on a near-continuous basis. The system relies on balises to update the train position with balises demarking positions and track circuits tracking train location for the interlocking.

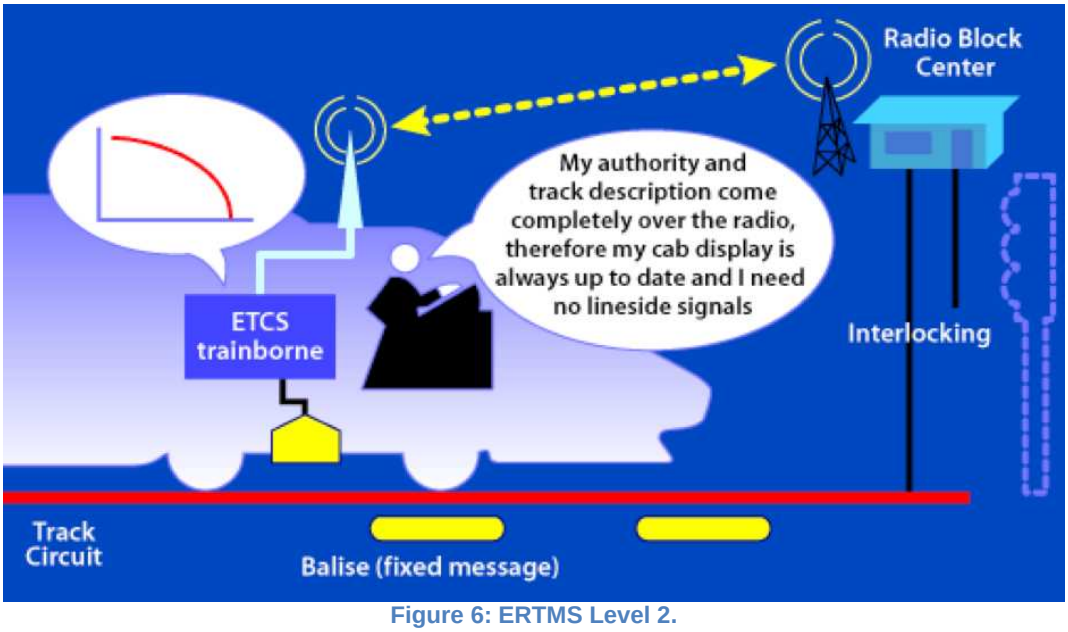


Figure 6: ERTMS Level 2.

As opposed to level 1, ERTMS level 2 does not require lineside signals. The movement authority is communicated directly from a Radio Block Centre (RBC) to the on-board unit using GSM-R. The balises are only used to transmit “fix messages” such as location, gradient, speed limit, etc. A continuous stream of data informs the driver of line-specific data and signals status on the route ahead, allowing the train to reach its maximum or optimal speed but still maintaining a safe braking distance factor.

Whilst enabling greatly reduced maintenance costs through the removal of lineside signals, ERTMS Level 2 also presents the possibility for substantial line capacity increase by enabling higher operational speeds and offering reduced headways: more capacity means more trains moving, thus more benefits.

3.1.2.5 ERTMS level 3

Level 3 is a moving block system with the train integrity on board. The train relies on balises to update position only, transmitting position and integrity data back to the interlocking via GSM-R link. This level is in a conceptual phase.

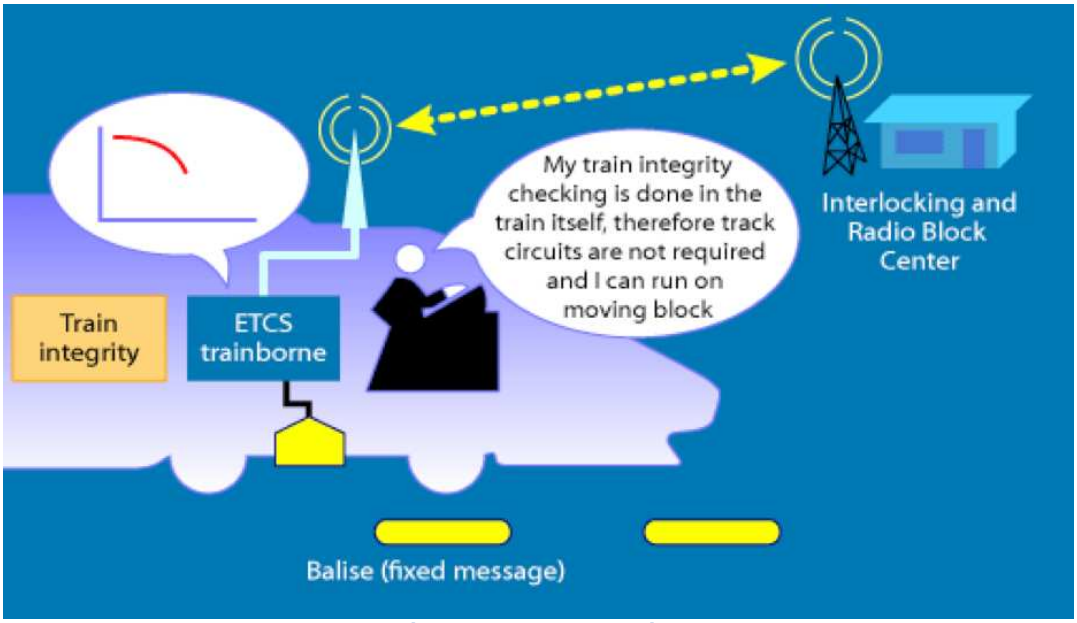


Figure 7: ERTMS Level 3.

ERTMS Level 3, still in its test phase, allows for the introduction of a “moving block” technology. Under ERTMS level 1 and 2, movement authorities are determined using “fixed blocks” - section of tracks between two fixed points which cannot be used by two trains at the same time. With ERTMS level 3, accurate and continuous position data is supplied to the control centre directly by the train, rather than by track based detection equipment. As the train continuously monitors its own position, there is no need for “fixed blocks” – rather the train itself will be considered as a moving block.

3.1.3 Current implementation of ERTMS

Currently there are two version of the ERTMS specification: The set of specifications number 1, whose System Requirement Specification version is the 2.3.0 (1), and the set of specifications number 2, whose System Requirement Specification version is the 3.3.0 (2).

Some lines are equipped with equipment following the release 2.3. New lines should use release 3.3. Some guidelines are provided by ERA to achieve the migration between 2.3 and 3.3.

3.1.4Examples of deployment

Following, some maps with information about deployments of ERTMS in the countries of the partners of this project are presented. This information has been gathered from ERTMS official web page (4).

Figure 11: ERTMS deployments in Spain.

Figure 10: ERTMS deployments in France.

Figure 9: ERTMS deployments in Belgium.

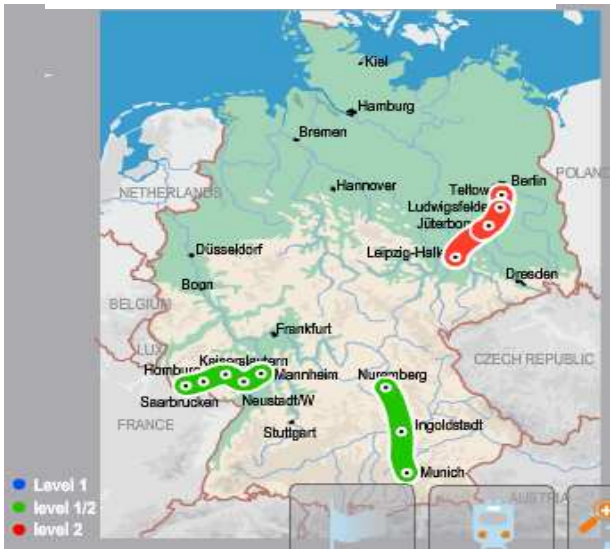


Figure 8: ERTMS deployments in Germany.

Figure 12: ERTMS deployments in Italy.

In conclusion, there are a similar number of ERTMS Level 1 and Level 2 track lines deployed. This is due to the fact that in the last few years there have been an increasing number of ERTMS Level 2 deployments.

3.2 Resiliency in ERTMS

In the current specification of ERTMS no resilient architecture is proposed. Thus, resilient architectures are implementation dependant, mostly proprietary solutions of railway operators and train manufacturers which are not published. However, GSM-R Industry Group has proposed different advices for the GSM-R deployment, in order to increase the capacity and reliability. Although resiliency and reliability are not the same issue, both are related to some extent and thus, these advices for reliability can also be applied for increasing the resiliency of the system. In this section we will present different coverage architectures presented in the ERTMS Conference of 2003 (5).

The wireless link between the BTS and the train is a key point for the ERTMS because it allows keeping in contact the RBC and the train in movement. However, this part of the network is the weaker one due to its exposition to external perturbations (unintentional interferences, attacks, etc.). Therefore, redundancy is aimed at improving availability of the system to cope with any of these perturbations. In order to reach this coverage redundancy, three possible architectures are proposed: single coverage with high cell overlap, double coverage with in co-located sites and double coverage in interleaved sites.

3.2.1 Single coverage with high cell overlap

This proposal is based on using a single coverage infrastructure with a share BSCs and MSCs. In order to obtain coverage redundancy, BTSs are set to a distance equal to the cell coverage radius so that there is a coverage overlap in all places along the railroad.

This alternative to get redundancy involves setting up more number of BTS, which involves higher number of site acquisition. All these BTS share the rest of Base Station Subsystem elements reducing the cost comparing to other alternatives. However, in case of failure of any shared elements, all system is affected.

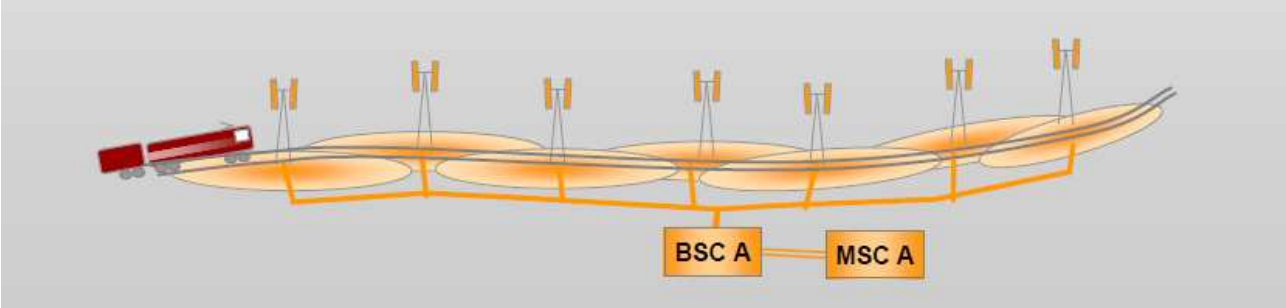


Figure 13: Single coverage with high cell overlap.

3.2.2Double coverage with in co-located sites

The second alternative proposed is focused not only in the resiliency of the wireless network, but also in the rest of the Base Station Subsystem, that is the BSCs and MSCs. This way, if any component of the network fails, there is another available access network to provide service to train. This proposal duplicates the number of BTS, BSC and MSC increasing the network deployment cost. However, BTSs of both networks are placed in common places, so the site acquisition is equal as single-coverage case.

This proposal permits to use different frequency range for the same area so it provides system resiliency in case of interferences focused on a particular frequency band. However in case of external perturbations originated close to the BTS that affects both used frequencies, this architecture does not provide any kind of resiliency because both BTS are placed at the same distance from the perturbation so the effect in both equipment would be equal.

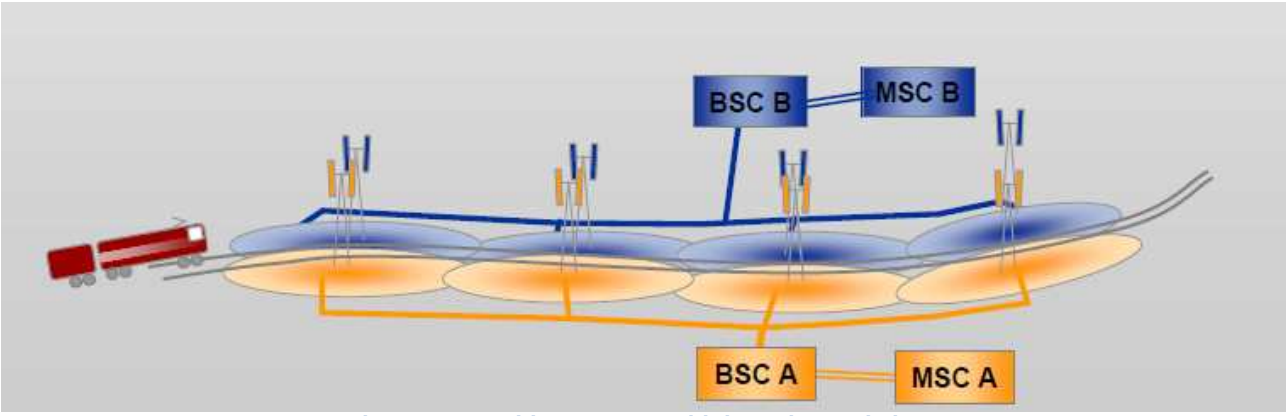


Figure 14: Double coverage with in co-located sites.

3.2.3Double coverage in interleaved sites

The last proposal is a duplicated access network with BTSs of each network placed in its own site. The distribution of BTS along the railroad is shown in the Figure 15. As we can see the BTSs of the network B are placed between two BTS of the network A. This way, the architecture does not only protect against perturbations for a particular frequency, providing two access network working on different frequencies, but it also provides resiliency against perturbations originated close to a BTS that affect multiple frequencies. In this architecture scheme, if a BTS of network A is attacked with a directional EM jammer, the train would be still able to communicate throughout the network B.

This architecture involves the highest cost of proposed alternatives, due to duplication of equipment and double site acquisition, but it also provides the highest failure tolerance and resiliency level.

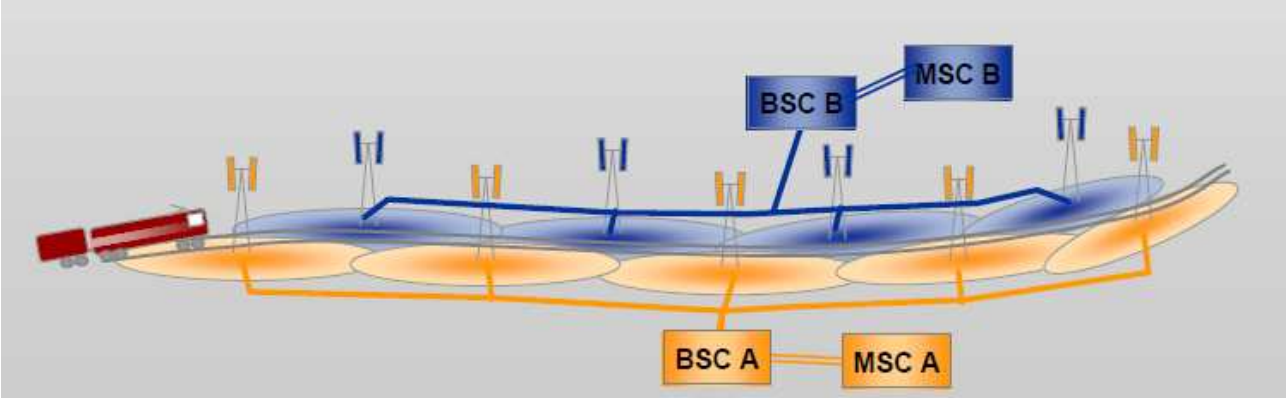


Figure 15: Double coverage in interleaved sites.

3.3 Evolution of ERTMS towards IP

Nowadays, the underlying protocols used to transmit ETCS messages between the RBC and the train are not based on the IP protocol stack as it was shown in the Figure 4 in the page 9 of the document. However, current ERTMS specification is not absolutely unaware of the IP protocol stack family. In fact, the communication among RBCs, detailed in the "RBC-RBC Safe Communication Interface" document (6), is performed over the IP protocol.

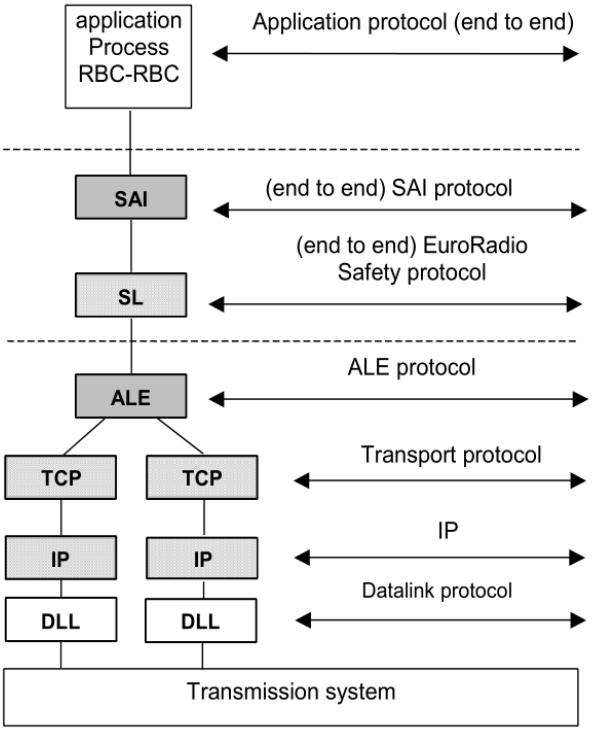


Figure 16: Protocol Stack for RBC-RBC communication.

EuroRadio Packet Data Units (PDUs) are inserted inside TCP segments thanks to the Adaptation Layer that performs actions like address mapping and connection establishment. One or multiple TCP connections may be used for each logical connection, in order to satisfy all availability requirements. This idea of increasing the availability of the connection by using multiple connections will be proposed afterwards in the document for the resilient architecture.

Returning to ETCS signalling, ERTMS Level 2 and Level 3 are completely related to GSM-R. However, the use of GSM-R implies several limitations. In the article "An Overview of GSM-R technology and its

shortcomings" (7), most important issues are pointed out. Perhaps the most important issue today to justify the improvement or replacement of the GSM-R technology is the limited number of channels because only 19 channels of 200 KHz are available to establish communication circuits. Each channel provides 8 timeslot but only 7 are available to establish communications. A GSM-R cell can use only few of the channels, because the same channel cannot be reused by neighbouring cells due to interference. This is not a limitation for voice communications because they are limited in time. However, in ERTMS Level 2 and beyond each train must establish and maintain a permanent circuit with the remote RBC and this may suppose a problem for GSM-R cells located in heavy loaded rail sections. Other drawbacks related to GSM-R are the limited capabilities to offer new services, for example, video surveillance or Internet access for users, and the fact that is an outdated technology that doesn't benefit from improvements that could be also beneficial for the railways such as an improved spectral efficiency, higher bitrates or a cost-efficient architecture.

Due to these limitations, the research community proposed the logical evolution of GSM-R towards GPRS or towards a custom implementation of GPRS for railway, which we will call GPRS-R. There are several research papers, i.e. "The European Switch: A Packet Switched Approach to a Train Control System" (8), that present GPRS as an alternative mainly to improve the capacity of the GSM-R cells thanks to the packet switching technology and its more efficient resource usage compared with circuit switching. There are also research projects, for example, one of the main objectives of the project "Facilitating and speeding up ERTMS deployment" (9) funded by the European Commission is to "*improve the performance and the interoperability (IOP) features of the telecommunication link, including the development of packet switching/GPRS and GSM-R compatibility testing".*

However, GPRS is not only a proposal of the research community but also the industry is testing it. The International Union of Railways (UIC) carried out a project called "GSM-R Network Management, Frequency Management" (10) from 2010 to 2012 whose main work was related to GRPS:

> *"The European Train Control System (ETCS) at Level 2 should replace lineside signalling, and should provide a full automatic train protection including train supervision. In order to achieve these goals, there is a need of a data service, which will help to overcome future restrictions especially in dense area. Following this line, A-GSMR will assess the readiness of IP-based solutions (e.g. GPRS) to be available for ETCS level 2 to overcome future restrictions especially in dense areas. A-GSMR will also gather and manage the frequency needs for railways, related to all frequencies and the common needs. The A-GSMR will act as an interface between railways and European frequency authorities and as the centre of competence in the field of telecommunication for railways."*

UNISIG, the consortium that is responsible of publishing the ERTMS/ETCS standards, is also studying the GRPS integration in ERTMS and is working on several alternatives to achieve it. In the Figure 16, it is presented the protocol stack of the main alternative (Alternative 1) (11) to use ETCS over GRPS. This alternative is based on the use of TCP/IP protocols and a wrapper layer for being able to interact with the EuroRadio layer without requiring modifying it. In fact, this proposal for integrating GRPS in ERTMS is quite similar to the protocol stack already used for the RBC-RBC interface that was presented in the Figure 16.

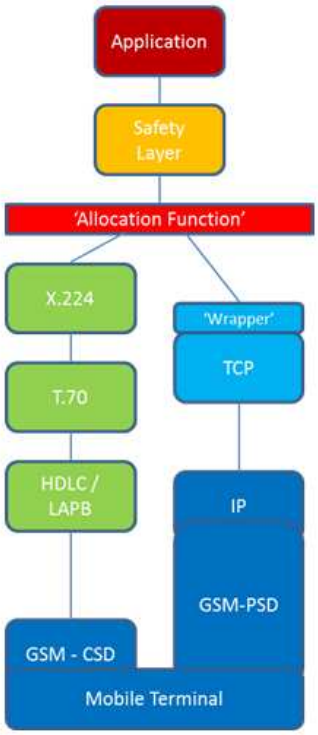


Figure 17: Protocol stack alternative for ERTMS over GPRS (Figure from (11)).

Standardization of ETCS over GPRS will bring IP to the RBC-Train communications and with it the advantages and disadvantages of the use of. Perhaps, one of the main advantages will be the simplification of the protocol stack and a greater independence of the wireless technology used because once IP has been introduced, any IP-capable wireless technology could be considered to be used for signalling between the train and RBC.

Furthermore, the research community and the industry are looking beyond GPRS and are taking into account other wireless technologies, especially LTE, that will suppose a great technological improvement of ERTMS passing from GSM-R, a 2G technology, to LTE, a 4G technology, without passing through other intermediate technologies like EDGE, UMTS or HSPA. In events specialized in telecommunications in railway, such as Railway Telecommunications 2012 in Malaga (Spain), multiple of the presentations and networking events were focused on discussing the convenience of LTE as a replacement for GSM-R.

In conclusion, nowadays it seems that there is clearly a trend of evaluating GSM-R and considering other technologies for the communication between train and ground due to its drawbacks. Perhaps it is early to evaluate which wireless technology will replace GSM-R but what is almost certain is that the new technology will be based on IP because the main candidates to replace GSM-R, GPRS and LTE, are IP technologies and other major alternative technologies (UMTS, WiMAX …) are also IP.

4 Approach to justify SECRET Resilient Architecture

4.1 Introduction

The objective of this section is to carry out an overall threat and vulnerability analysis that will help justify the design of the SECRET resilient architecture.

The first subsection (methodology used) describes the typical methodologies used by various stakeholders:

- Risk management methodologies used at critical infrastructure levels. We use as a typical example the BowTie risk analysis (12). This methodology could be used in the threat and vulnerability analysis of the SECRET railways critical infrastructure (WP1).

- Risk management methodologies used at ICT infrastructure levels. We use as a typical example the TVRA (13) analysis. This methodology could be used in the threat and vulnerability analysis of the SECRET ICT architecture (WP4).

- Architecture design methodology used at ICT infrastructure levels. We use as a typical example the Carnegie Mellon software architecture methodology (14).

The second subsection (methodology used) explains the relationships between the methodologies. The last sections (applying the methodologies in SECRET and security analysis at ICT level) include the analysis that will help justify the decisions of the SECRET architecture.

4.2 Methodologies Used

4.2.1 Risk Management Methodologies

Risk management is about the assessment of risks and the application of measures to minimize, monitor and control threats. Risk management can be applied to any systems (e.g. financial markets, power plant, electricity grid, space station, vehicles). The ISO 31000 family of standards provide a set of principles and guidelines for risk management.

One widely used method is the BowTie methodology. In a nutshell, the BowTie methodology is organised around four main concepts: hazards (i.e. a source of danger), top events (i.e. an event that causes the hazard), causes (of a top event) and impact (of the occurrence of a top event).

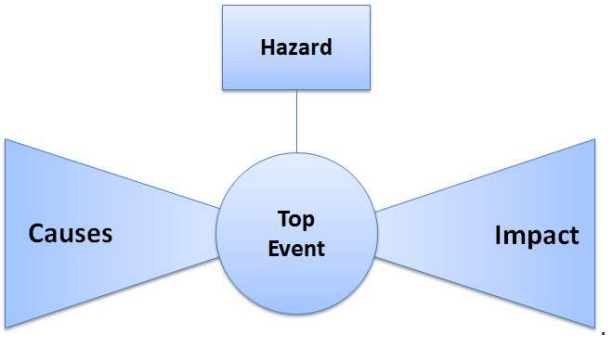


Figure 18: Bow-Tie Diagram.

Figure 18 shows how the concepts are displayed in a diagram. The shape of the diagram is the reason for the name of the methodology. An example of hazard could be "*train collision*". An example of top event could be "*train can no longer be stopped*".

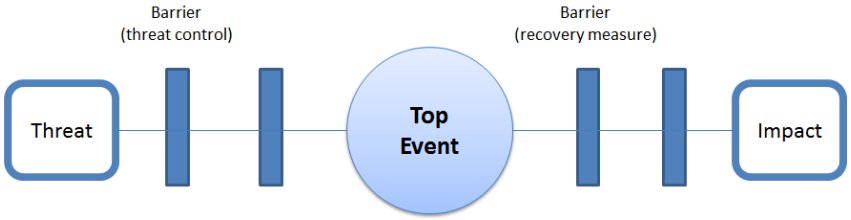


Figure 19: Threats and Barriers.

In a Bow-tie diagram, causes consist of threats and barriers. A threat is a factor that could cause a top event. There might be multiple threats that could cause a top event. Barriers are measures to control a threat and prevent, or delay the occurrence of a top event. Barriers can also be recovery measures that take place after the occurrence of a top event. An example of threat could be "*loss of distance information with train ahead*". An example of barrier could be "*stop the train*". Figure 19 shows how threats and barriers are visually displayed in a diagram.

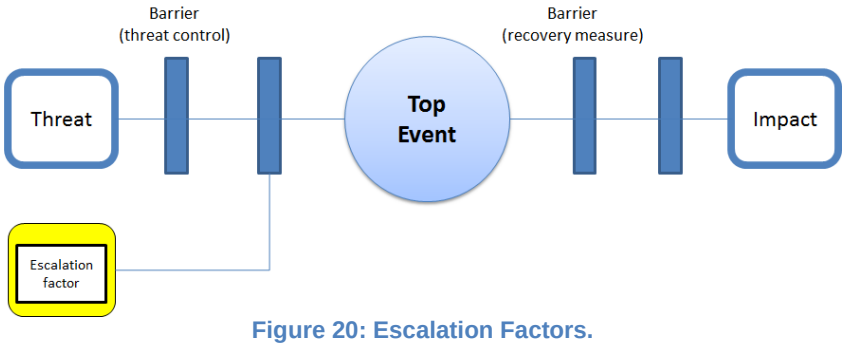


Figure 20: Escalation Factors.

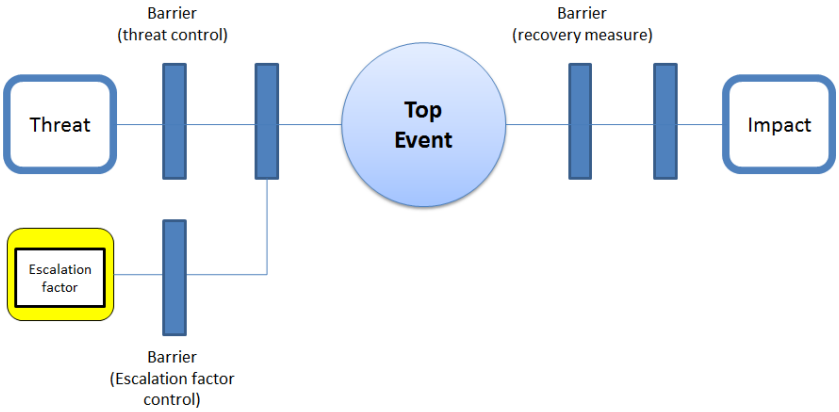


Figure 21: Barriers for Escalation Factors.

Escalation factors can be considered as specific threats created to prevent the operation of a barrier. An example of escalation factor could be an "*attack on the train braking system*" that would prevent the effectiveness of the "*stop the train*" barrier. Figure 20 shows the display of escalation factors in a Bow-tie diagram. Escalation factors also are threats. They can therefore be controlled by other barriers as showed in Figure 21.

The risk management methodology approach is to define as many bow-tie diagrams as top events. This involves the identification of barriers and escalation factors.

Risk management methodologies often include a risk measure approach. One widely used approach is the Failure Mode and Effect Analysis (FMEA) sometimes called FMECA to indicate criticality analysis. In this approach, each failure mode is associated with the following parameters.

- A failure probability level, The MIL–STD–882 standard defines 5 levels: frequent, probable, occasional, remote, improbable.
- A severity level. The MIL–STD–882 standard defines 4 levels: catastrophic, crucial, marginal, negligible

Figure 22 shows an example of criticality matrix where the overall criticality is the results of multiplying the failure probability level by the severity level: C = P x S.

		Severity			
		Negligible	**Marginal**	**Critical**	**Catastrophic**
Failure probability	**Frequent**	High (not desirable)	Unacceptable	Unacceptable	Unacceptable
	Probable	Moderate (acceptable)	High	Unacceptable	Unacceptable
	Occasional	Moderate	High	High	Unacceptable
	Remote	Low (negligible)	Moderate	High	High
	Improbable	Low	Low	Moderate	Moderate

Figure 22: Example of Criticality Matrix.

In some cases a third parameter is added, detectability. For instance the following 5 levels can be used: high degree, good, likely to detect, fair, low or no detectability. The resulting criticality is the result of multiplying the probability by the severity and by the detectability. There are calculation schemes where each parameter is associated with a valued ranging from 1 to 10. The resulting risk, often called RPN (Risk Priority Number) is a value ranging between 1 to 1000.

4.2.2Risk Management for ICT Infrastructures

ICT infrastructure could also be analysed using the Bow-tie methodology associated with a FMEA risk measure. This however is not usual practice. Instead, a security methodology such as TVRA is typically used. There is a wealth of templates and security analysis documents based on TVRA. In a nutshell, the purpose of TVRA is to improve the security of an ICT based system by (1) providing an understanding of the security threats to a system and (2) specifying possible countermeasures where these are determined to be necessary.

TVRA includes 10 steps:

- Identification of Target or Evaluation (TOE)
- Identification of Objectives
- Identification of Functional Security Requirements
- Systematic Inventory of Assets
- Systematic identification of Vulnerabilities
- Calculation of the likelihood of the attack and its impact
- Establishment of Risks
- Security Countermeasure identification
- Countermeasure Cost-benefit analysis
- Specification of Detailed Requirements

One of the major benefits of the TVRA method is that there are calculations of impact, likelihood and risk, based on the following principle equations:

- The impact of a threat is calculated is a function of asset impact (i.e. impact of attacking a given asset) and of attack intensity (e.g. isolate single attack vs. massive multiple attacks:

```
Overall Impact = Asset Impact + Attack Intensity
```

- The likelihood of a threat is a function of practicality factors such as

```
Likelihood =    f(System knowledge) +
                f(Time) +
                f(Expertise) +
                f(Opportunity) +
                f(Equipment)
```

- The risk of a threat is a function of likelihood and impact. Risk result is a value ranging from 1 to 9, with three categories: *minor, major, critical.* Critical and possibly major risks must be solved through countermeasures

```
Risk =      Occurrence Likelihood X Overall Impact
```

- Once threats and risk values have been identified, the cost benefit of countermeasures can be defined. The cost benefit is defined as the difference between the overall risk before and the overall risk after the introduction of a countermeasure

```
Overall Risk Before = Sum of Risk Values for all threats Before
Counter Measure
Overall Risk After = Sum of Risk Values for all threats After
Counter Measure
```

The calculations proposed are not based on formal background. Rather they correspond to heuristics proposed by security experts. The main advantage of the approach is that they allow various stakeholders in an organisation to interpret in a consistent way the results of an analysis. In other words, the managers, the applications developers and the security experts use a common “language” or tool to understand each other.

The risk management methodology approach is to define as many threats as possible and then identify the countermeasures.

Note that TVRA and FMEA are very close. The table below shows the equivalent concepts

TVRA	FMEA
Threat	Failure Mode
Asset Impact	Severity
Likelihood	Probability
No equivalent concept but could be integrated in Likelihood	Detection
Risk	Risk

Table 1: TVRA and FMEA comparison table.

4.2.3 Architecture Design Methodology

A typical architecture design methodology is the software architecture methodology from Carnegie Mellon which is the result of a nearly 15-year research work. Extensive literature is available including widely used text books (15). In particular specific work has been carried out in the area of security and survivability (16).

The CMU software architecture methodology is organised around the concept of quality attributes (often called non-functional requirements). Here is a list of quality attributes:

- Execution qualities: security, usability, dependability, predictability
- Evolution qualities: testability, maintainability, scalability

The approach is to specify *scenarios*, which are structured means to state attribute requirements. A scenario includes the following elements:

- *Source* At security level, the source is typically an attacker
- *Stimulus*. At security level, the stimulus is typically an attack e.g. an EM attack
- The stimulated *Artefact*. At security level, the stimulated artefact is typically the system being attacked.
- The *Environment* or the conditions under which a stimulus occurs (e.g. normal train operation)
- The *Response* to the stimulus. The response is influenced by architecture techniques called *Architecture tactics* (e.g. switch to manual mode operation)
- The *Response Measure*. This measure is needed in the design process in order to validate the architecture design (e.g. train still in operation at 200 km/h)

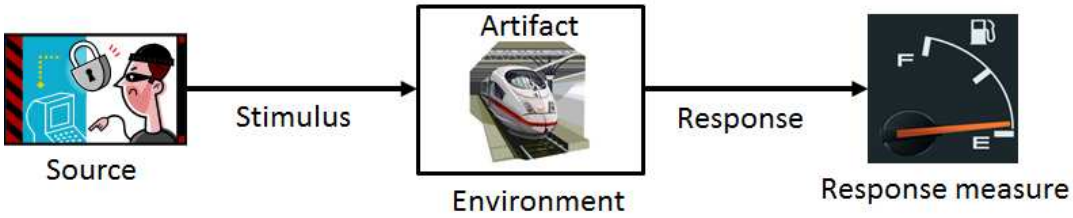


Figure 23: Scenario Model.

Figure 23 shows the resulting scenario model. The whole design process can be described as involving three steps:

- Identification of scenarios.
- Influencing the responses by selecting appropriate architecture techniques called in CMU jargon *architecture tactics*.
- Measuring the responses in order to validate the design decisions

The last step (*response measure*) is particularly important. Each quality attribute has to be associated with a body of theoretical knowledge allowing the designer to assess the impact of an architecture decision. To this end the following is needed:

- The body of theoretical knowledge or the *quality attribute reasoning framework*. There can be as many reasoning frameworks as quality attribute. The security quality attributes is typically based on risk management methods.
- Functions to predict the response measure given a stimulus for a particular architecture. Such functions are called *quality attribute models*. Reasoning frameworks allow the use of quality attribute models.
- Methods to evaluate the functions. Such methods are called *quality attribute evaluators*

Reasoning frameworks are often associated with a set of existing architecture tactics. Examples of architecture tactics identified by Carnegie-Mellon (16) are:

- Redundancy
- Diversity
- Deception: artifice aimed at inducing enemy behaviours that may be exploited

- Authentication
- Intrusion detection
- Recovery/adaptation
- Physical, logical, cryptographic and temporal isolation
- Personnel management

4.3 Applying the Methodologies in SECRET

The relationship between a Bowtie diagram used to describe the handling of a given hazard (critical infrastructure level) and a TVRA analysis (ICT infrastructure level) is the following:

- A BowTie diagram contains barriers which result from architecture decisions (i.e. SECRET resilient architecture)
- A TVRA threat is an escalation factor. Barriers to control escalation factors are countermeasures of the analysis. They result from architecture decisions (i.e. SECRET resilient architecture)

Figure 24 shows an example of SECRET threat.

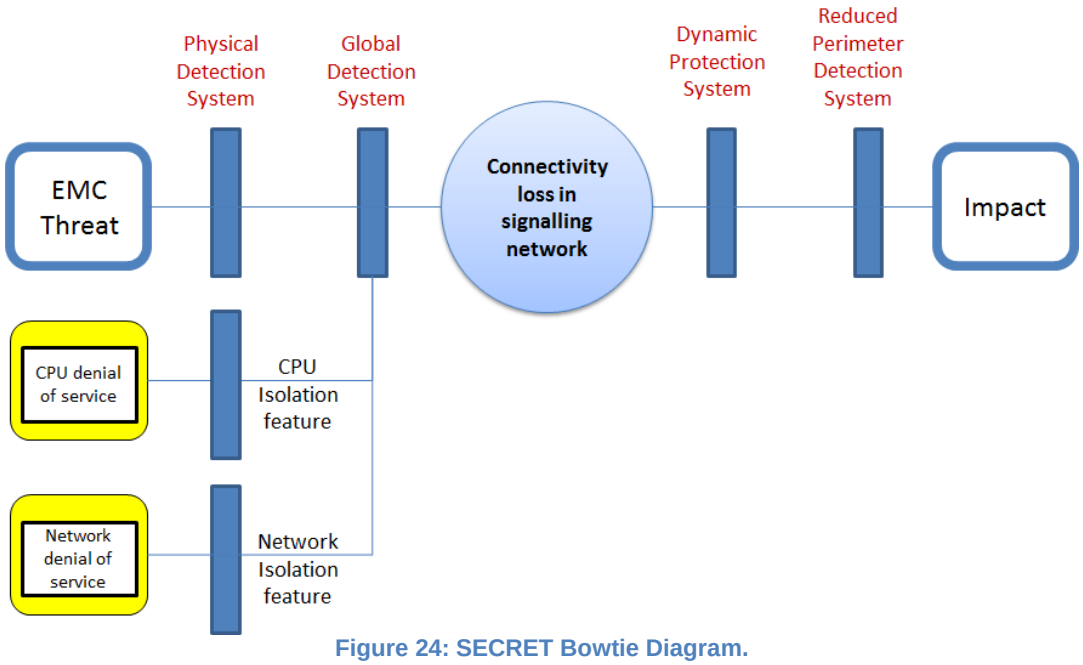


Figure 24: SECRET Bowtie Diagram.

The relationship between the Bowtie diagrams and TVRA threats and a software architecture scenario is the following:

- A threat or escalation factor in a Bowtie diagram is a stimulus in a scenario
- Barriers of a Bowtie diagram are part of the response in a scenario

Figure 25 shows two examples of scenarios relevant to SECRET.

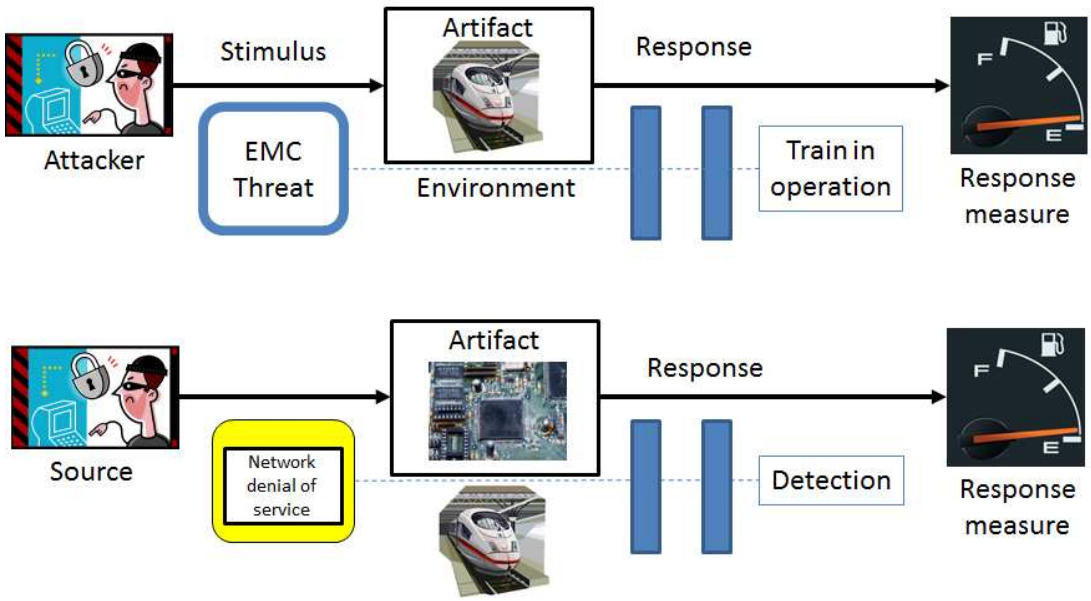


Figure 25: Scenarios for Architecture Tactics.

Finally, risk calculation between a FMEA and TVRA are based on similar approaches (but different terminology).

4.4 Security Analysis at ICT level

In this section the characteristics a system must have in order to be qualified as Resilient System are described. First a definition of resilience is given and then the different components of a resilient system are reviewed.

The term resilience has many definitions depending on the context and application. For example, Paulo Veríssimo (Univ. of Lisboa Faculty of Sciences) gives the following definition of Resilience: “The ability to recover from or adjust easily to misfortune or change”. Concerning computing the University of Kansas’s ResiliNets Project (17) defines Resilience as: “Resilience is the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation”. More generally, the target system must be able to automatically operate through faults and attacks in a seamless manner. This project specifies a certain number of principles that must be followed for a resilient system. Eighteen principles are detailed in (17). A brief definition of each of them is presented in annex. Among these principles are the followings:

- Service requirements: Of course the first principle is to specify the service requirements which determine the resilience level the system under construction must achieve.
- Normal behaviour: A second principle is that the normal behaviour of the system must be well understood and easily verified through monitoring. This will allow the system to detect adverse attacks or abnormal conditions.
- Threat models: The objective of a model is to ignore, mask, or abstract unimportant or unnecessary details, thereby highlighting the details of interest. It promotes consistency when the analysis is performed by different actors. Threats models are mandatory for the system to be able to detect attacks and be able to defend itself against them.
- Metrics: They can be defined as consistent standards of measurement. They are a mean to better understand and control a system. In the context of the SECRET project, they allow to better defend against threats (18). As such, they are requested for analysing and evaluating system resilience.

4.4.1Threat Models

In (19) a list of the most common threats that can attack GSM networks is given. Each of them is evaluated using a risk assessment methodology called DREAD presented in (20). As our project deals with EM Attack, this deliverable will focus on threads that can be achieved through EM Attack of Jamming. The restricted list together with the evaluations will be used as a first input to our proper risk analysis using the TVRA methodology. The result of this analysis will be shown in the next version of this document.

The GSM network will potentially face different types of jamming techniques like:

- Spot Jamming. It is the most common method in which the attacker uses all its transmitting power on a single frequency. While it is a powerful method, it suffices for the network to use another frequency.
- Sweep Jamming. In contrast to the previous technique, the attacker is able to rapidly shift from one frequency to another. It causes a considerable packet loss but is very power consuming.
- Barrage Jamming. Several frequencies are jammed at the same time. As above, it is very power consuming and its effect is reduced when the number of frequencies is high.
- Base Jamming. It is like barrage jamming but here an antenna is jammed as its source at all frequencies.
- Deceptive Jamming. With this technique, the network is flooded with fake data such that the attacker deceives the defensive mechanism of the network without leaving any traces. This type of attack is difficult to detect.

Several jamming attack models are possible (the list below is not exhaustive):

- Continuous-Wave jammer is an electronic jammer that emits an electromagnetic wave of constant amplitude and frequency. Early jammers belong to this category. This type a jammer is discussed in (21).
- Constant jammer is a jammer that emits continuously a radio signal with random bits. It therefore prevents legitimate traffic sources to access the network for sending packets.
- Deceptive jammer is a jammer that injects regular packets on the network without any gap between packets.
- Random jammer is a jammer that emits a radio signal during an interval of time and is quiet during another interval of time. Both intervals are either random or fixed. When it is emitting, it can behave as a constant jammer or as a deceptive jammer
- Reactive jammer is quiet when the network is idle and emits a radio signal when it detects activity on the network. When it is emitting, it can behave as a constant jammer or as a deceptive jammer. Again, this kind of jammer is hard to detect.

4.4.2Assets potentially subject to attack

The different assets that are potential target to EM attacks are described in the deliverable D3.1.

4.4.3Initial impact analysis

In this section the TVRA methodology is used to analyse the impact of an attack on assets. We provide here a first simplified analysis that will be refined in a subsequent version of this deliverable. It is based on informal discussions with other work package participants. We will call this analysis v1. A subsequent version v2 will be provided when more detailed information will be provided by other work packages. The following three threats are identified:

- Simple EM attack which does not prevent communication (see Figure 26 and Figure 27). The asset being attacked is a local device in charge of ERMTS function. The attack has not effect, but the EM

manipulation is detected. The tactics used is detection. The local health/attack manager sends an alert to the global manager which logs the info.

Source	Stimulus					Artifact
Threat	Attack					Asset
	Factor	Range	Value	Resistance to attack	Likelihood	
EMC attack in a train level does not prevent communication	Time	<= 1 day	0	Basic	Likely	Local train device in charge of a European Rail Traffic Management System (ERTMS) function.
	Expertise	Layman	0			
	Knowledge	Public	0			
	Opportunity	Unnecessary	0			
	Equipment	Specialized	3			
	Asset Impact	Medium	2			
	Intensity	Single instance	0			
	Time	<= 1 day	0	Basic	Likely	
	Expertise	Layman	0			
	Knowledge	Public	0			
	Opportunity	Unnecessary	0			
	Equipment	Specialized	3			
	Asset Impact	Low	1			
	Intensity	Single instance	0			

Figure 26: EM Attack does not prevent communication (Part 1).

Response			Impact	Response Measure		
Countermesure			Impact	Risk assessment		
Tactics	Mechanism	Behavior		Level	Value	Gain
-	-	no detection	Medium	Critical	6	3
Local detection	local EMC attack/health manager detect intrusion	local manager sends a message to global manager which logs info	Low	Major	3	

Figure 27: EM Attack does not prevent communication (Part 2).

- The EM attack is stronger and it would provoke lack of communication at the channel level. (See Figure 28 and Figure 29). The effect of the attack is the loss of communication, which causes the train to be stopped. The countermeasure is multipath communication. The attack is however detected and therefore a higher level alert is sent to the global health/attack manager.

Source	Stimulus					Artifact
Threat	Attack					Asset
	Factor	Range	Value	Resistance to attack	Likelihood	
EMC attack in a train level which prevent channel communication	Time	<= 1 day	0	Basic	Likely	Local train device in charge of a European Rail Traffic Management System (ERTMS) function.
	Expertise	Layman	0			
	Knowledge	Public	0			
	Opportunity	Unnecessary	0			
	Equipment	Specialized	3			
	Asset Impact	High	3			
	Intensity	Single instance	0			
	Time	<= 1 day	0	Basic	Likely	
	Expertise	Layman	0			
	Knowledge	Public	0			
	Opportunity	Unnecessary	0			
	Equipment	Specialized	3			
	Asset Impact	Low	1			
	Intensity	Single instance	0			

Figure 28: EM Attack prevents channel communication (Part 1).

Response			Impact	Response Measure		
Countermesure			Impact	Risk assessment		
Tactics	Mechanism	Behavior		Level	Value	Gain
Local detection	local EMC attack/health manager detect intrusion	No communication possible. Train stopped	High	Critical	9	6
Local detection and Redundancy	local EMC attack/health manager detect intrusion and multipath communication	local manager sends a message to global manager which activates real-time supervision measure	Low	Major	3	

Figure 29: EM Attack prevents channel communication (Part 2).

- EM attack is very strong and it prevents communication (see Figure 30 and Figure 31). The effect of the attack is a train stop. The attack is detected at the train level (and causes the train to stop) and at the global level (and this cases traffic management measures).

Source	Stimulus					Artifact
Threat	Attack					Asset
	Factor	Range	Value	Resistance to attack	Likelihood	
EMC attack in a train level which prevent channel communication	Time	<= 1 day	0	Basic	Likely	Local train device in charge of a European Rail Traffic Management System (ERTMS) function.
	Expertise	Layman	0			
	Knowledge	Public	0			
	Opportunity	Unnecessary	0			
	Equipment	Specialized	3			
	Asset Impact	High	3			
	Intensity	Single instance	0			
	Time	<= 1 day	0	Basic	Likely	
	Expertise	Layman	0			
	Knowledge	Public	0			
	Opportunity	Unnecessary	0			
	Equipment	Specialized	3			
	Asset Impact	Low	1			
	Intensity	Single instance	0			

Figure 30: EM attack prevents communication (Part 1).

Response			Impact	Response Measure		
Countermesure			Impact	Risk assessment		
Tactics	Mechanism	Behavior		Level	Value	Gain
Local detection	local EMC attack/health manager detect intrusion	No communication possible. Train stopped	High	Critical	9	3
Global detection	Global EMC attack/health manager detect problem	Global alert level 3 (traffic management measures)	Medium	Critical	6	

Figure 31: EM attack prevents communication (Part 2).

5 Architecture for resiliency

5.1 Objectives and specifications

5.1.1 Objectives

The main objective of the resilient architecture, as it was defined in the DoW, is to offer an **improved resilience against EM attacks** in order to protect principally wireless communications between trackside and trains. The architecture should provide a dynamic protection solution combining resilient communication architecture with a resilient health and attack management subsystem.

Other minor objectives that should be covered by the future resilient architecture are listed below:

- The resilient architecture should be also adapted to the **interoperability** needs associated with the current harmonization process of the European railway network.

- The resilient architecture should keep in mind **new trends** of development in the European railway network to guarantee its viability in future specifications and deployments.

- The resilient architecture should be **flexible** enough in order to provide the communications with different levels of protection that could be implemented depending on the security requirements of the items to be guarded.

- The resilient architecture should **efficiently manage resources**, especially resources like radio that might be limited.

- The resilient architecture should **not suppose a significantly loose of performance** in the **trackside-train communications**. Although it is inevitable that the resilient architecture will increase the computation and communication requirements, the overload and latency introduced by the resilient architecture should not be high.

5.1.2 Specifications

The list of specifications considered for the design of the resilient architecture is listed below:

- Resilient architecture should be focused on protecting the signalling systems between trackside and train.

  Railway sector is a complex environment where multiple communication systems are used to cover different communication necessities. For example, in a specific track section there may be deployed communication systems to perform command and control tasks of the trains, allow the communication with the deployed staff, allow the communication in emergency situations, … The resilient architecture should be focused on protecting the command and control communications between trackside and train, although the design principles of the resilient architecture may be probably useful to protect other communication systems with requirements of resiliency.

- Resilient architecture should be focused on protecting ERTMS signalling system.

  There is a huge amount of signalling systems for the command of trains. ERTMS is the standard backed by the European Union to homogenize and replace in a future all the different national railway command and control systems in Europe. Consequently, ERTMS has been defined as the main communication system that should be protected by the resilient architecture.

- The resilient architecture should protect the more critical and vulnerable wireless links of ERTMS.

As it was stated in the state of the art, the wireless technologies used by ERTMS depend on the ERTMS Level deployed in the track. The most important technologies are Eurobalise for ERTMS Level 1 and GSM-R for ERTMS Level 2 and 3, although there are other less important wireless technologies like Euroloop and Radio-in-fill. The sensitivity to jamming of Eurobalise and GSM-R are quite different. In GSM-R the distance between the train and the BTS are much longer and thus the power of the receiving signal is weaker. This causes more easiness to disturb the GSM-R signal than the Eurobalise signal. Furthermore, even in case of disturbing the signal of one Eurobalise, it seems that Eurobalises are not so strategic for the traffic management as GSM-R. In conclusion, the resilient architecture should be able to protect the most critical and sensitive technologies of ERTMS against EM attacks. Thanks to the feedback received from other WPs of the project, GSM-R has been identified as the most important technology to consider in the current specification of ERTMS.

- The design of the architecture for resiliency should be a valid solution for current specifications and deployments of ERTMS.

  A disruptive proposal, which may suppose a meaningful change of the current ERTMS specifications, although interesting from a theoretical or researching point of view, would lack of applicability. The railway environment, as other sectors with huge security concerns, is a conservative sector with high degrees of standardization. New approaches are discarded and implementations are based on technologies that have proved their trust and reliability for years or even decades. Although new approaches could come to be standardized, it would require of several years and quite more years to get first deployments. Thus, the architecture should be focused to offer some degree of resiliency to current ERTMS deployments without requiring great modifications of the current standards.

- The architecture for resiliency should cover the considered evolution of ERTMS.

  As it was shown in the state of the art, several test beds and proposals are being performed to evolve ERTMS towards IP. So, the architecture should be flexible enough to be able to be useful in future evolution of ERTMS.

5.2 General overview of the architecture for resiliency

ERTMS Level 2 and 3 requires a permanent communication path between trackside and the train so that the RBC can signal the train. All the possible communication paths between the trackside and the train rely, at least in a certain section of the communication path, on wireless communication technologies. Current ERTMS specifications uses GSM-R and future specifications will depend on GPRS-R or other packet-switched technologies like LTE. But wireless communication technologies are more sensitive against EM attacks than wired ones. Indeed, there are wired technologies, for instance, the optical fibre, that are immune to electromagnetic interference and even in general it is quite easier to shield sensitive wired technologies against electromagnetic interference. However, the usage of wireless communication technologies in ERTMS is absolutely necessary to connect the fixed endpoint (the RBC) and the mobile one (the train).

Up to four wireless technologies are defined in the current specifications of ERTMS: GSM-R, Eurobalise, Euroloop and Radio In-fill. The usage and importance of the previous technologies depends on the ERTMS Level deployed in the track.

Facing the impossibility to absolutely guarantee wireless communication between trackside and the train against EM attacks, the aim of the proposed resilient architecture is to provide a flexible architecture that will provide multiples way to harden trackside-train communications depending on, on one side, the ERTMS deployment and, on other side, the security level that want to implement the management staff.

The architecture is based in two main concepts: detection of EM attacks and a hardened wireless communication path. These two main concepts are the basis of the resilient architecture that consists indeed of two subsystems: the Detection System (DS) and the Multipath Communication System (MCS).

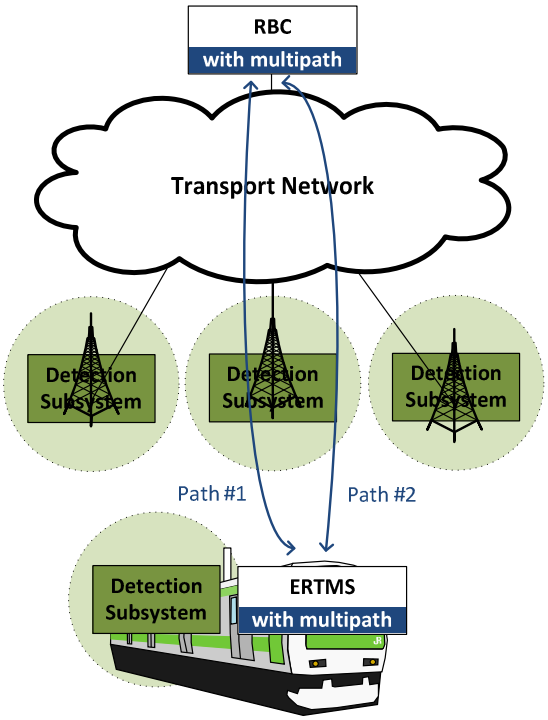


Figure 32: Subsystems of the Detection System (DS) and Multipath Communication System (MCS) for the resilient architecture.

Firstly, the DS allows the detection in real-time of the EM attacks that occur in the railway infrastructure. Thus, the management staff can be provided with accurate information, which allows to anticipate loose of connectivity in certain sections of the trackside exposed to an EM attack or, in the worst case, resolve quickly if the loose of communication with a train is due to an EM attack or due to a different reason (lack of power, hardware failure, …).

The availability of this information for the railway management staff is crucial to perform the suitable actions in order to restore communications and normal operation. Given the information, management staff could deploy manual reactive actions or even, depending on the railway management system, automatic reactive actions.

Secondly, the MCS aims to provide multiple paths of communication between the RBC and the train in order to maintain the ETCS session of ERTMS Level 2 or Level 3 even if one or several paths fail. This implies the requirement of deploying a multipath protocol between the RBC and the on-board ERTMS located in the train. In order to get it, two alternatives are available. The first alternative is to include the multipath protocol on the operative system of the RBC and the on-board ERTMS in the train. The second alternative is to deploy middle boxes between both endpoints to translate current protocols to multipath protocols. Both solutions have their advantages and drawbacks, but both provide multipath communications for the ETCS signalling between the RBC and train. Furthermore, one additional advantage is that the multipath and resiliency is obtained at an underlying layer and thus the ETCS application, which may be more complex to test and validate, doesn't need modifying.

One important requirement to be able to implement the MCS is that endpoints of the multipath communication must use Internet Protocol (IP). Consequently, this subsystem can't be directly deployed in traditional ERTMS based on GSM-R because there is no IP in the protocol stack of the communication RBC-Train. However, as it has been shown in the state of the art, it seems that the great majority of new proposals of ETCS over new technologies will use IP and thus this proposal should be of very applicability on all of those scenarios. Furthermore, other alternative is the use of middle boxes between the train and RBC that allow the translation of the circuit switching technology of legacy ERTMS to packet switching technology with support of multipath.

In order to take full advantage of MCS, trains needs to be multihomed or in other words trains needs to have two or more IP interfaces. It is important to remark that the MCS is unaware of the wireless technologies

used, which provides a great flexibility (Wi-Fi, WiMAX, LTE, TETRA …). The only requirement is that interfaces must be IP with at least one IP address and there should be two or more IP interfaces per train in order to be able to establish two or more paths between the RBC and the train. Indeed, there will be as many different RBC-train paths as IP interfaces the train has. Depending on the number and type of interfaces the communication will be more reliable against EM attacks. Indeed, in order to provide a better resilience against EM attacks it would be advisable to deploy multiple interfaces using different technologies that ideally use different range of frequencies.

Another advantage of this MCS not related to resiliency is the fact that it would ease the coexistence and migration of wireless communication technologies used for ETCS signalling. If a train supports several wireless communication technologies (GPRS-R, Wi-Fi, WiMAX, LTE, TETRA, …), the MCS could provide smooth inter-technology handover mechanism maintaining the ETCS session in the process, for example, if a section of the track only supports WiMAX and another section only supports LTE.

Finally, deploying together the DS with the MCS would be of great interest because both subsystems complement one another. On one hand, the DS might provide useful information to the MCS in order to change the active interface in case an attack that affects the current active interface is being performed. Thus, the MCS might change the communication paths based on the information provided by the DS. In the other hand, the DS could profit from the hardened communication provided by the MCS to harden the communication between the trackside detection subsystem and the on-board detection subsystem located in the train.

5.2.1 Application scenarios

This section covers the application scenarios of the resilient architecture attending to the deployed ERTMS. As it is shown in the Table 1, there are two main application scenarios depending if the communication between the train and the RBC is based on IP or not.

		ETCS over non-IP (GSM-R)	ETCS over IP (GPRS-R, LTE, …)
Detection System	**(On the track)**	Yes	Yes
	(On the train)	Yes (but inefficient)	Yes
Multipath Communication System		No (IP needed)[1]	Yes

Table 1: System availability per application scenario.

5.2.1.1 ETCS over non-IP (current ERTMS specification)

This use case is related to the current specifications of ERTMS. ERTMS Level 1 uses a unidirectional communication path from trackside to train based on Eurobalise, whereas ERTMS Level 2 and 3 is based on a bidirectional communication protocol between track and train over GSM-R and Eurobalises are only used for positioning purposes.

Regardless of the use of Eurobalise or GSM-R, the communication between the RBC and train is not IP-aware, so the MCS can't be implemented in this scenario.

Technically it would be possible to deploy the MCS to provide resiliency for legacy ERTMS based on GSM-R and circuit switching. It would be necessary to have an IP transport network and, one or several IP wireless access networks like Wi-Fi, WiMAX, LTE or TETRA. In this case, it would be possible to deploy several middle boxes in the communication path between the train and the RBC so as to perform the translation between circuits and packets (with support of multipath communications). However, as it has been shown in the state of the art, today it is considering evolving ERTMS towards IP communications schemes due to the shortcomings associated to the circuit-switching technology.

Another solution for providing multipath communications on legacy ERTMS would consist on avoiding the use of IP and managing multiple GSM-R circuits established between the same train and the same RBC,

[1] See detailed explanation in 5.2.1.1.

which should be managed by the ETCS application. This requires a great change in the logic of the current RBC deployments that could be proposed but difficult to implement or come to a successful end. Furthermore, this would be more to solve the problem deploying a more robust application instead of providing a more resilient architecture to be used by upper layer protocols or applications.

In conclusion, the resilient architecture for current ERTMS deployments is reduced to the DS as it can be seen in the Figure 33.

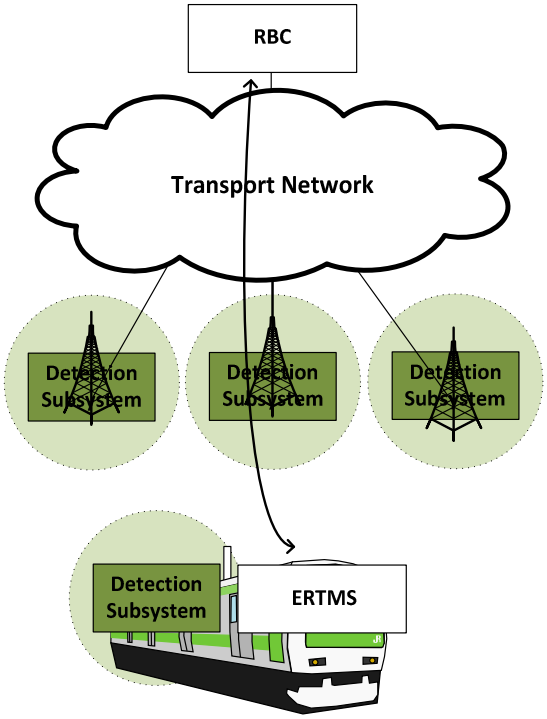


Figure 33: Resilient architecture for ETCS over Eurobalise/GSM-R.

Other point to be considered is the DSS (Detection Subsystem) located on the train (on-board DSS) and the reporting of the information from this on-board DSS to the trackside DSS.

In the case of using ERMTS L2 or L3, GSM-R may also be used to report the information of the Detection System in addition to allowing ETCS signalling between RBC and train. However, as GSM-R is a circuit-switching technology two circuits should be required, one for ETCS signalling between RBC and train, and another circuit for the communication between the on-board DSS and the trackside DSS. This increased number of circuits used per train may be a problem in some GSM-R cells where there is high density of trains.

In the case of using ETCS over Eurobalise (ERTMS L1) is even more complicated because there is a need of communication between train and trackside and Eurobalise cannot be used for this purpose. Although Eurobalise is a bidirectional communication technology, currently it is exclusively used as a unidirectional communication technology from trackside to train. Thus, in order to be able to use the on-board Detection System in ERTMS L1 another suitable wireless access network should be available to be used or if not available on-board DSS could not be deployed.

5.2.1.2 ETCS over IP (GPRS-R, LTE …)

As it has been presented in previous sections, new research on wireless technologies for ERTMS is heavily focused on IP-aware technologies like GPRS. Nowadays, GPRS research is of great interest because it provides a better resource usage and an increased number of manageable trains per cell than GSM-R for a reduced cost of upgrade from the current GSM-R infrastructure. Furthermore, evolution towards LTE or other wireless technologies is constantly considered on research forums focused on railway communications. All of these new proposed wireless technologies for ERTMS are packet-switching technologies, instead of circuit-

switching like GSM-R, and are based on the protocol stack of Internet by using Internet Protocol (IP).

The use case of the ETCS protocol over Internet Protocol (IP) allows the deployment of the DS and the MCS. In this use case, the resilient architecture may be deployed in three ways adapting to the requisites of the railway management authority:

- Only the DS
- Only the MCS
- DS and MCS

The first possibility, only the DS, is a very similar case to the resilient architecture for ETCS over GSM-R with some considerations.

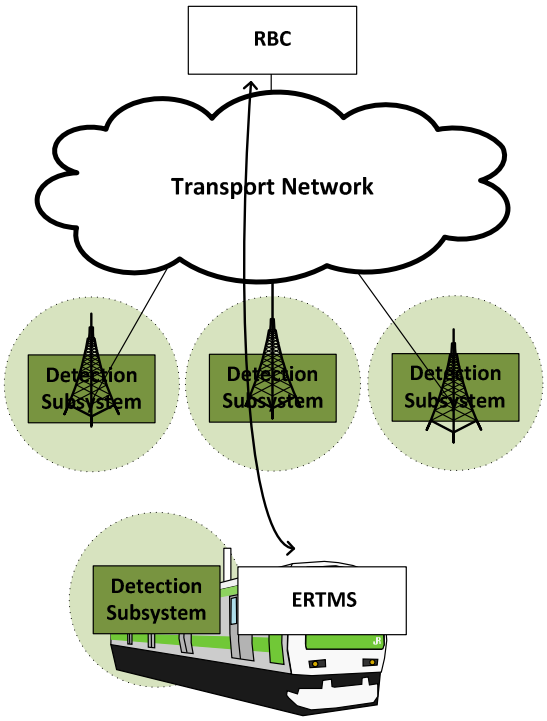


Figure 34: Resilient architecture for ETCS over IP: only Detection System.

The main difference with ETCS over GSM-R is that a packet-switching technology is used in ETCS over IP. Thus, the same transceiver of the train could be used to multiplex the information exchange of the ETCS signalling and the DS. Even in case two different transceivers are used, one for the on-board DSS and another for the on-board ERTMS, the packet-switching technology provides a better usage of the radio resources than the circuit-switching technology.

The second option would be to implement only the MCS. In this scenario, all the redundant paths will transmit the same information and so, ETCS commands would be received duplicated by the endpoint. However, EM attacks can't be detected in this scenario and thus a more dynamic traffic management policy cannot be implemented depending on the attacks. Only a traffic mirroring policy would be implemented, that is, replicating signalling messages through all available interfaces at the same time.

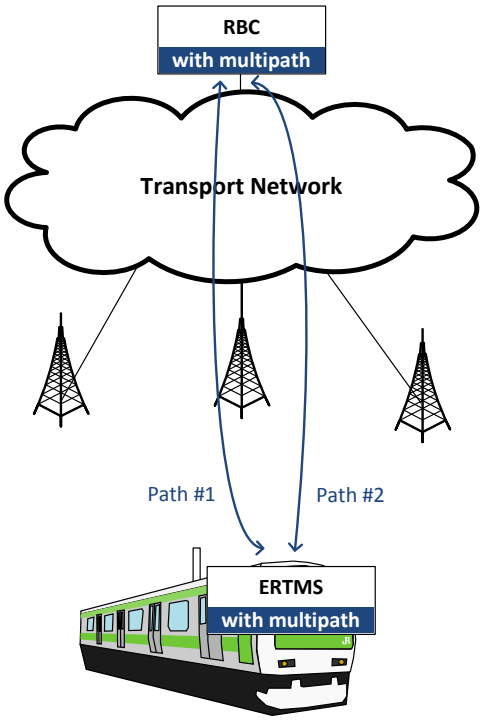


Figure 35: Resilient architecture for ETCS over IP: only Multipath Communication System.

Finally, the third and most completed scenario consists on the deployment of the DS and the MCS to provide a better resiliency against EM attacks.

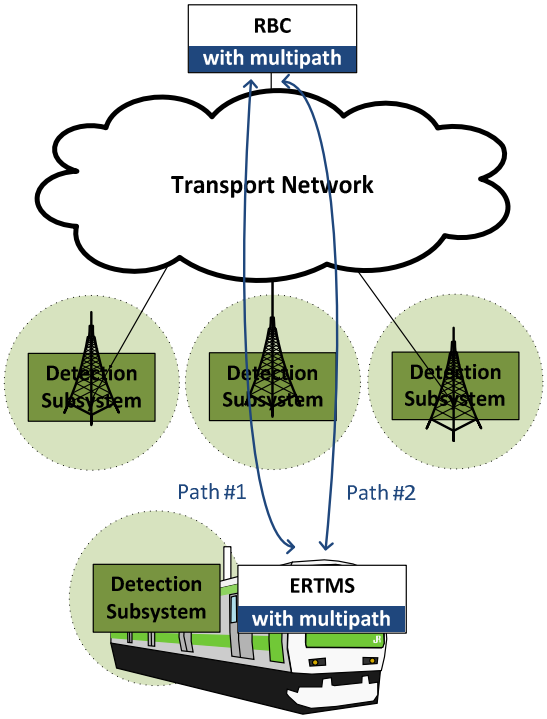


Figure 36: Resilient architecture for ETCS over IP: Detection and Multipath Communication Systems.

This resilient architecture has a DS to detect in real-time EM attacks and a hardened communication between the RBC and the train provided by the MCS. In addition, these subsystems benefit each other. The on-board DSS may provide information to the on-board MCS so that more intelligent traffic policies than always-mirroring can be implemented (for example, only one active interface and only in case of an attack disturbing the active interface, the active interface would be changed or all the interfaces would be

activated). In addition, the on-board DSS could also benefit from a hardened communication between the train and trackside thanks to the MCS and thus reporting from the on-board DSS to trackside DSS could be hardened also against EM attacks.

Although there are three possible scenarios for the ETCS over IP use case, the recommended resilient architecture is the third one because it provides a complete solution that boots two subsystems to face more reliably against EM attacks.

5.3 Architecture of the Detection System

The main aim of the Detection System (DS) is to detect EM attacks that are performed in the protected infrastructure and thus be able to react to overcome them.

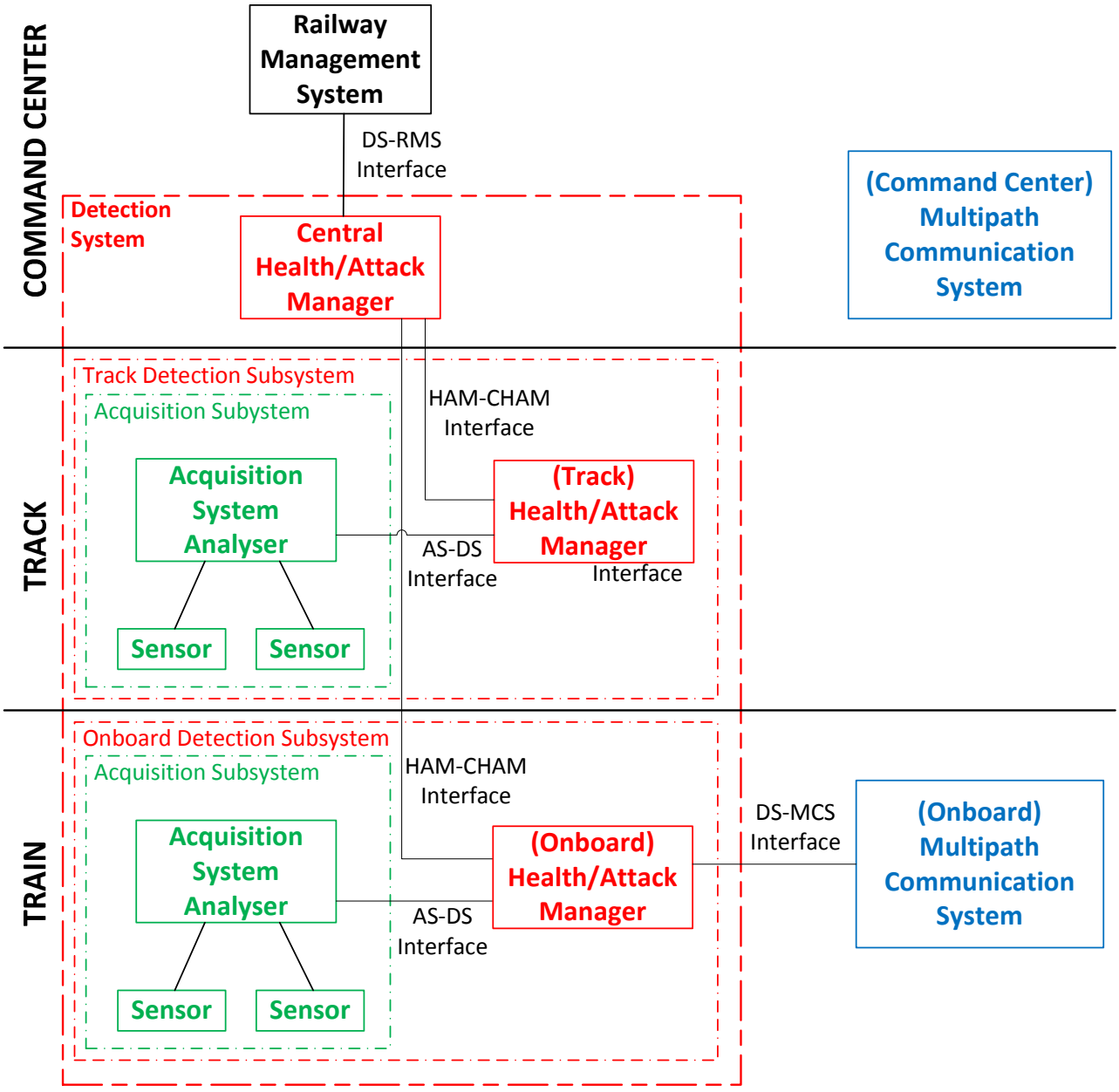


Figure 37: Logical Architecture of the detection system.

The DS presents a geographically distributed architecture composed of one Central Health/Attack Manager

(CHAM), which would be generally located at the command centre, and multiple detection subsystems distributed along the track and inside trains.

On the one hand, the CHAM is the main element of the DS. It consolidates the information provided by each detection subsystem with regards to EM attacks and thus it provides a complete view of the EM state of the railway infrastructure protected by detection subsystems. The CHAM also provides the interaction facilities with the DS via program interfaces for human beings or APIs for external programs.

On the other hand, the detection subsystems are autonomous systems responsible for the detection of EM attacks in a specific geographical area and for carrying out the pertinent actions when EM attacks are detected. The management of the location of the geographical area covered by the detection subsystem is quite easy to manage for detection subsystems deployed in the track because they are static but it could be quite more complex in case of a detection subsystems deployed inside a train. Regarding the actions performed when an EM attack is discovered, they may depend on the current configuration of the detection subsystem:

- Discard the report of the EM attack.
- Report the information about the EM attack to the CHAM or even to other interfaces, for instance, to notify the driver of a train about the attack.
- In case of availability of a Multipath Communication System (MCS), change the communications configuration of the MCS to adapt communications to the on-going EM attack.

Although it is needed at least one detection subsystem to protect the track, the covering of the static areas may be carried out by multiple subsystems if it is advisable, for example, so as to balance the load in various detection subsystems. However, it is required one independent detection subsystem per train.

Each detection subsystem is composed of one Health/Attack Manager (HAM) and one acquisition subsystem. On the other hand, one acquisition subsystem consists of several sensors and one Acquisition System Analyser. Sensors provide the information that must be processed by the Acquisition System Analyser to determine the presence or lack of an EM attack. The aim of the Acquisition System Analyser is to manage the sensors, analyse the output of sensors and set whether an EM attack is happening or not. The Acquisition System Analyser will provide the HAM with normalized information about the on-going EM attack. On the other hand, the HAM receives the information about the EM attack detected by the acquisition system and must process it and take the actions according to the current configuration of the HAM. The HAMs deployed in the track are generally called Trackside Health/Attack Managers (THAMs) whereas HAMs deployed inside trains are generally called On-board Health/Attack Managers (OHAMs).

In the following subsections the components and the interfaces of the detection system are going to be explained in more detail.

5.3.1Components

Following, the main components of the DS are listed and it is shown their relation to the work packages and tasks of the SECRET Project.

Component	Design	Proof of concept implementation
Acquisition System Sensor	WP3: T3.2 & T3.3	WP3: T3.4 & T3.5
Acquisition System Analyser	WP3: T3.2 & T3.3	WP3: T3.2 & T3.3
(Trackside/On-board) Health/Attack Manager	WP4: T4.1 & T4.2	WP4: T4.4
Central Health/Attack Manager	WP4: T4.1 & T4.2	WP4: T4.4

Table 2: Components of the DS and their relation to WPs and Ts of the SECRET Project.

5.3.1.1 Acquisition System Sensors

The sensors of the acquisition system provide input information to be processed by the Acquisition System Analyser. The information provided by sensors will vary depending on the kind of sensor and, for example, it

may be the radio frequency signal received by an EM sensor or even information from upper layers like the latency, bit error rate or number of retransmissions. This raw information will be received and processed by the Acquisition System Analyser to detect the presence of EM attacks.

The Work Package 3 is mainly working on the processing of radiofrequency signals to detect EM attacks and currently two main kind of sensors or approaches to get the required information are considered.

Firstly, a sensor or input source that provides access to information inside the GSM-R receiver at different stages along the receiving chain. This allows collecting information before/after different filters in the GSM-R receiver. This approach requires the modification of the existing equipment in order to collect the necessary analogue data.

Secondly, in order to observer the same radiofrequency signals than the ones effectively received by the railway equipment, the EM signal received by the same antenna is equally shared between the acquisition system and to the communication system located in the train, in the station or at ground. In this case, the sensor consists of the shared communication antenna and the acquisition system. The following Figure 38 represents this situation in the case of a GSM-R railway communication system.

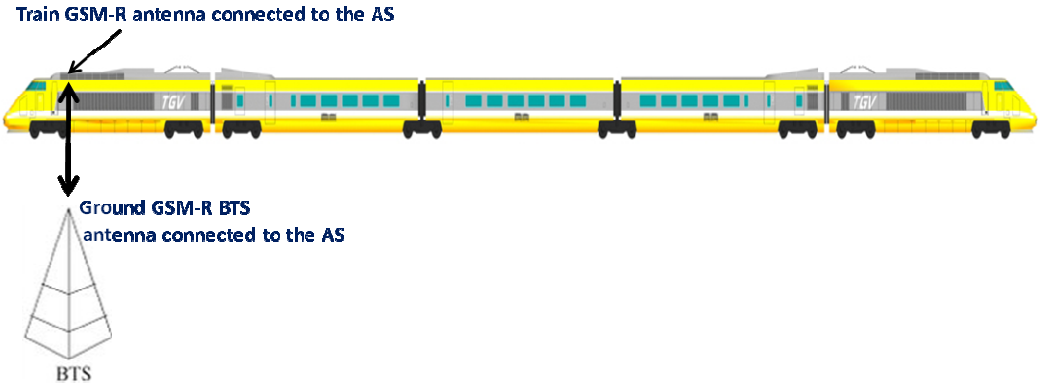


Figure 38: Sensors of the acquisition system connected to the railway system antennas.

Apart from these approaches, other sensors may be developed. For instance, it would be possible to deploy a sensor that gathers and provides to the Acquisition System Analyser information about the performance of protocols of the upper layers that may be meaningful for the detection of EM attacks. The sensor could gather the data performing active checks in the network or requesting the information to the MIB of network devices.

5.3.1.2 Acquisition System Analyser

The Acquisition System Analyser is mainly responsible for processing the information provided by sensors to detect the presence of EM attacks. It must also control sensors and establish the communication with the Health/Attack Manager (HAM) to inform about changes detected in the state of the EM environment detected.

Depending on the kind of sensors deployed, the Acquisition System Analyser must perform different kind of computational tasks to detect the presence of EM attacks. Currently, as it was presented in the section 5.3.1.1, two kinds of sensors to work with radiofrequency signals are considered in the Work Package 3.

The first approach is based in having access to the radiofrequency signal before/after different filters in the GSM-R receiver. The signals provided by this sensor will be processed in Acquisition System Analyser by a model of quadratic detection based on the I/Q (In phase / Quadrature of phase). This approach, as it was previously pointed out, would require the modification of the existing equipment in order to collect the necessary analogue data, which could be not realistic.

The second approach is a bit different. It is conducted completely in parallel with the existing receiving chain, without any direct information collected in the existing receiver itself. However, as in the first approach, we use the existing train or ground antenna to feed the detection equipment built in a separate sensor and

signal processing box. Therefore, the same antenna signal is shared between the existing receiver and this add-on equipment. We perform the detection of attacks by an adapted time or frequency analysis based of the previous knowledge of the normal electromagnetic environments corresponding to the system in use. This second approach enables more flexibility in terms of signal processing. Moreover, since it doesn't require modifying the existing equipment, this second solution could present an advantage for its real implementation.

The Acquisition System Analyser will have to implement other algorithms in order to be able to support other kind of sensors.

Based on the analysis performed to the input provided by each sensor, the Acquisition System Analyser will establish if one EM attack is being carried out and will notify the Health/Attack Manager (HAM).

5.3.1.3 Health/Attack Manager (HAM)

The main purpose of the HAM is to collect the EM attack reported by the acquisition system and process them according to the configuration set by the CHAM.

Whenever possible HAMs must establish and keep a session with the CHAM. As mentioned previously, the communications between CHAM and HAMs are based on the IP protocol; however, there are several options regarding the networking modules depending on the kind of HAM or application scenario. If the HAM is deployed statically in the track, the HAM is required to have a communication interface to establish a connection with the CHAM. However, if the HAM is deployed in a train, there are several alternatives. One option is to deploy the on-board Detection Subsystem (DSS) without the multipath communication system, in this case the HAM and the ETCS systems would have a wireless communication transceiver each one of them, for example, a GSM-R module each one of them. The second option is to deploy the on-board DSS with the multipath communication system, in this cases the communication modules would be installed in the MCS, for instance, only one LTE module, and the DSS and the ETCS system would have only a wired connection towards the MCS.

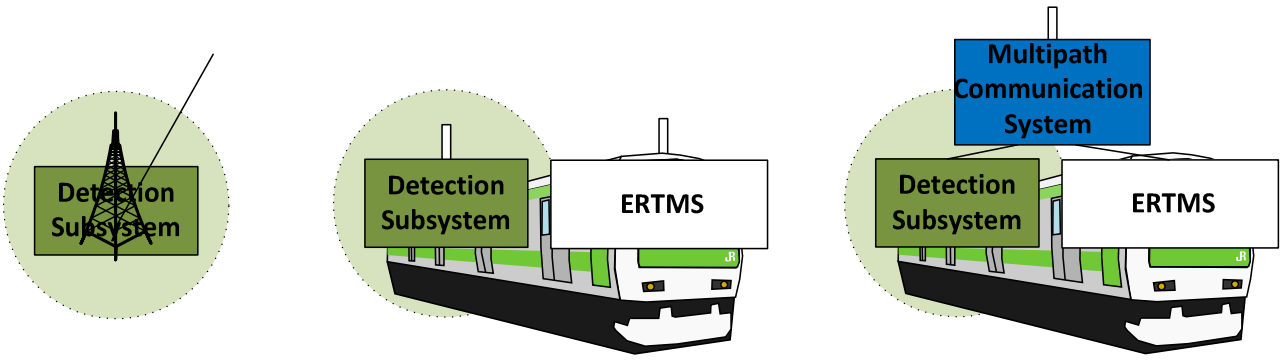


Figure 39: Detection Subsystems: DSS on the track with one wired connection, DSS on the train with one own wireless communication transceiver and DSS on the train with connectivity through the MCS.

A simplified status machine for the HAM is presented in the next figure.

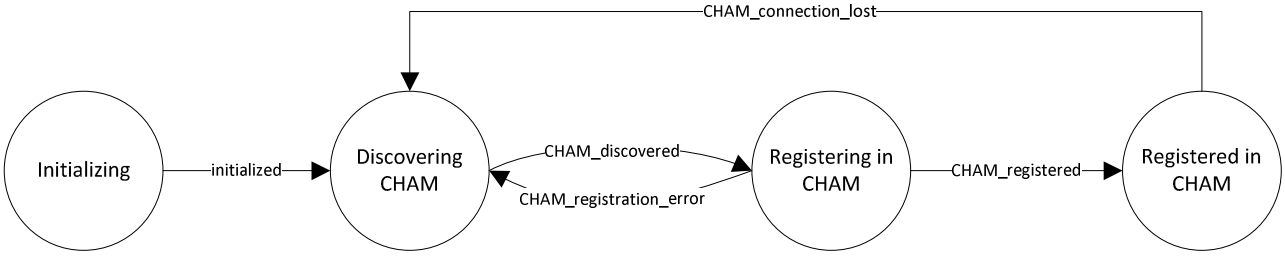


Figure 40: Simplified state diagram of a HAM (RHAM or THAM) w/o MCS.

When the HAM is registered in the CHAM, it is fully operational and it can report EM attacks to the CHAM and accepts commands from the CHAM.

However, if the HAM is deployed in a train with the multipath communication system, the HAM must register not only in the CHAM but also in the multipath communication system to be able to modify the communications path of the MCS depending on the attacks reported by the acquisition system. Because when the HAM is registered in the multipath communication system, the last one delegates the management of the wireless communication modules (GPRS-R, LTE …) to the HAM.

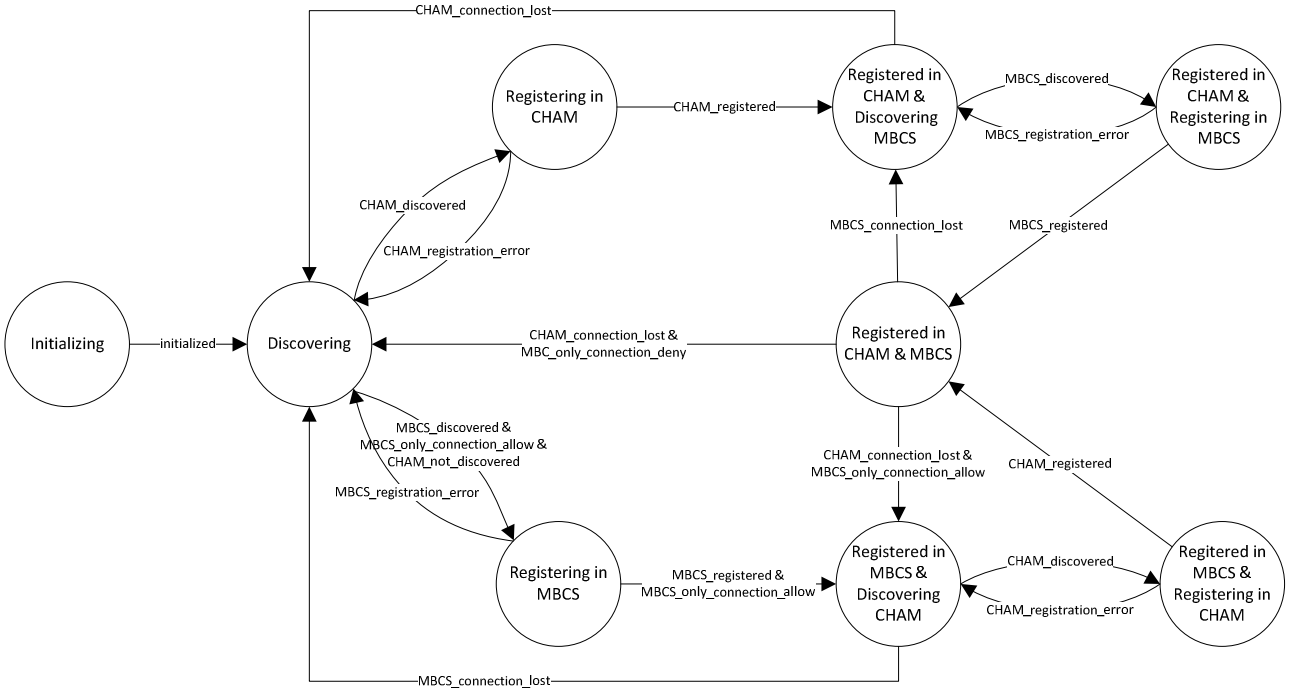


Figure 41: Generic state diagram for a distributed HAM.

The information about on-going EM attacks is received from the interface with the acquisition system. The EM attack reports from the acquisition system would be processed depending on the HAM configuration, which was established by the CHAM.

5.3.1.1 Central Health/Attack Manager (CHAM)

The Central Health/Attack Manager (CHAM) has two well-differentiated functions that must accomplish. Firstly, it must perform the orchestration of detection subsystems to allow the reception of reports of attack and to improve the detection capabilities of isolated detection subsystems. Secondly, it must provide an interface to allow the management and operation tasks on the detection system.

As regard as the orchestration of detection subsystems is concerned, it is required that the CHAM and HAMs of the detection subsystems must be capable of establishing an IP communication. Furthermore, the CHAM must know which detection subsystems are active and thus the HAM must register in the CHAM as soon as possible. To do that, the HAM must know the address of the CHAM or, at least, it should be able to find it by using a service discovering protocol. In addition, the CHAM must implement a method to verify the continuous availability of a previously registered HAM (*keepalives*, periodical registration …). Consequently, the CHAM is capable of knowing the detection subsystems the DS is composed of over time.

Measures to guarantee the communications between CHAM and HAMs must be taken in order to avoid security attacks. Thus, CHAM should verify the identity of HAMs before proceeding to their registration and then all the communications between CHAM and registered HAMs must be secured against modification attacks and optionally against sniffing attacks.

Once a HAM has registered in the CHAM, it is considered fully operational and it passes to take part of the DS. Then, the HAM can begin to process EM attacks according to its current configuration. The EM attacks that are reported from the HAM to the CHAM would be notified to the management staff and the CHAM would also analyse them to take into account the location of the detection subsystem. Thus, it is possible to connect an EM attack report from one detection subsystem with attack reports from neighbouring detection subsystems or even the CHAM might take the decision of informing a detection subsystem about an attack that is being performed close to it. This last case would be interesting, for example, so as to inform a train about an attack when it is bringing closer to an attacked area.

When the HAM has been registered in the CHAM, the HAM can also be configured by the CHAM indicating how it should process the EM attacks reported by its acquisition system.

Finally, the CHAM must log all the operations received and carried out to allow a posterior analysis of the EM attack and the behaviour of the detection system.

Regarding the interface with the management staff, the CHAM is the component of the detection system that allows the customization of the behaviour of all the detection system and it also provides centrally all the information about attacks gathered from remote detection subsystems. Thus, the CHAM must also provide a management and an operational interface. The management interface must allow the configuration of basic parameters regarding the behaviour against attacks detected by the acquisition system. On the other hand, the operational system must allow displaying in real-time the EM state of the guarded infrastructure and should also allow the search of historical data so as to allow a posterior analysis.

5.3.2Interfaces

In the following table the main interfaces of the DS are listed and it is detailed their relation to the work packages and tasks of the SECRET Project.

Interface	Design
AS-DS Interface	WP4: T4.1 & T4.2; WP3: T3.2
HAM-CHAM Interface	WP4: T4.1 & T4.2
DS-MSC Interface	WP4: T4.1 & T4.2
DS-RMS Interface	WP4: T4.1 & T4.2

Table 3: Interfaces of the DS and their relation to WPs and Ts of the SECRET Project.

Following, the interfaces of the detection system are described and listed their main requirements.

5.3.2.1 AS-DS Interface

This interface is the interface between the Acquisition System (AS) and the Detection System (DS), or more precisely, the interface between the Acquisition System Analyser and the Health/Attack Manager (HAM). This interface will have to be defined together with the WP3 and the WP4 of the SECRET Project.

The main objective of this interface is to report the EM attacks detected by the AS to the DS. It is required to define the format of an EM attack report message. At least that report message should include the following information:

- Information about the EM attack
- Information about the location of the attack

Furthermore, the AS should supply continuous EM attack report messages so as to inform about the temporary evolution of the EM attack.

The interface should include the following functionalities:

- A registration and keepalive procedure so that the HAM can entrust that the AS is alive and will

supply EM attack reports when one attack is detected.

- In case of detection of presence of a jammer superimposed on the useful information, the Acquisition System Analyser must notify it to the HAM.

- In case the Acquisition System detects a jamming signal,
  - The Acquisition System Analyser will try to recognize this particular jammer by observing its occupied bandwidth, used waveform... If this recognition is successful, the Acquisition System Manager will inform the HAM about the type of jammer detected among an existing list; otherwise, it will deliver an “unknown” jammer message.
  - The Acquisition System Analyser will provide the HAM with a rough localization of the jammer i.e. at ground, in train. To build this information, the acquisition system will study the jamming signal time evolution through its sensors.
  - The Acquisition System Analyser will deliver the expected level of jamming i.e. low impact on the communication path, degradation of bit error rate, loss of connection according to the existing jammer signal ratio (JSR) scale.

- In case of the detection of a new jamming signal, some information related to this new, not yet referenced jammer, could also be delivered to the HAM/CHAM to be shared among all the acquisition systems. This new information could be exchanged through a message updating the version of the jammer knowledge database.

5.3.2.2 HAM-CHAM Interface

This interface is the interface between the Central Health/Attack Manager (CHAM) and the remotes Health/Attack Managers (HAMs). It is an internal interface of the Detection System (DS) and thus would be specified by the WP4 but it would be conditioned by the EM attack report specification and other requirements of the AS-DS Interface.

This interface should include the following functionalities:

- Verification of the integrity of the communication between the CHAM and the HAM so that the CHAM can entrust that every HAM is alive and that it will receive EM attack reports when one attack is detected.

- EM attack report messages from HAMs to the CHAM. The reception of these messages must be acknowledged by the CHAM.

- Report of capabilities and configuration of the HAMs by the CHAM.

5.3.2.3 DS-MCS Interface

This interface is the interface between the Detection System (DS) and the Multipath Communication System (MCS), or more precisely, between the Health/Attack Manager (HAM) and the Multipath Communication System (MCS) of a train. It is an external interface of the DS and would be designed and developed in the WP4.

The aim of this interface is to establish an association between both systems, so that the detection system can manage the behaviour of the Multipath Communication System according to the detected EM attacks.

This interface should include the following functionalities:

- Verification that the MCS can entrust that the HAM is alive and thus can delegate the control of the multipath protocol to it.

- Report of capabilities and configuration of the MCS by the CHAM.

5.3.2.4 DS-RMS Interface

This interface is the management interface of the Detection System (DS).

This interface could be a human oriented interface or an API for integrating the DS with external applications. However, in order to test the platform it is going to be developed a human interface that must provide access to the operational and management functionalities of the detection system.

- This interface must inform about the state of the detection network providing information about the detection subsystems of which it is composed. Any change in the state of the detection subsystems should also be notified.

- This interface must inform immediately the management staff about the characteristics of any attack detected that is currently active.

- The interface must inform as soon as possible of the result of an attack that cannot be reported during its lifetime because of a lack of communication between the reporter and the CHAM due to the attack itself or to another reason.

- The CHAM should store any detected attack and this interface should permit a posterior search of suffered EM attacks for analysis purposes.

- The DS must allow the configuration of the active detection subsystems.

5.4 Architecture of the Multipath Communication System

The aim of the Multipath Communication System (MCS) is to offer redundant communication paths between the Radio Block Centre (RBC) and the train. To implement the MCS, ERTMS must support IP communications between the train and the RBC. Thanks to the MCS, the ETCS application of the RBC and train are unaware of the multiple paths since underlying networking protocols manage them transparently to offer a more robust and efficient data transport service to the uppers layers of the OSI stack. This a great advantage because no change in the ETCS application protocol is required.

Multipath communication protocols have emerged in IP to improve the communication between end devices that have multiple interfaces and consequently IP addresses. Perhaps nowadays the most representative devices of this kind are mobile devices. When Internet was initially developed one host had one unique IP address, whilst nowadays it is quite usual to have end devices, for example, mobile devices, that have multiple interfaces and thus can also have multiple IP addresses. However, traditional IP protocol only allows using one IP address/interface to establish a communication with the IP address of a remote device. Multipath communication protocols overcome this limitation allowing the use of all the IP addresses/interfaces a device has so as to establish multiple paths with the IP addresses/interfaces of the remote device. The maximum number of available paths is the result of the multiplication of sender's IP addresses by the receiver's IP addresses. These paths are used to implement different traffic policies. The most usual, and sometimes the unique currently implemented, is the load balancing policy that is based on balancing packets through all available paths to increase the throughput. This traffic policy is usually known as "Concurrent Multipath Transport". However, it is supposed that other traffic policies will be developed in the future like for example an active-passive policy.

Regarding resiliency in RBC-train communications, multipath communication protocols may provide a better resiliency against EM attacks but it will depend on the physical characteristics of the paths rather than the number of paths. In other words, to use multipath communication protocols, the ERTMS devices in the RBC and train must implement the multipath protocol. Furthermore, the train should have multiple wireless interfaces that ideally should use different technologies and frequencies. Following this premise, there will be multiple paths whose wireless links will be completely different and so it would be more difficult to disturb all the available paths between the RBC and train. In contrast, a mayor number of IP addresses in the RBC increases the number of paths although it doesn't improve substantially the resiliency against EM attacks because the kind of wireless links would be the same.

On other hand, as IP protocol provide an abstraction of the underlying technology (GPRS-R, WiMAX, LTE, TETRA …), multipath protocols also provide an abstraction between the end device and its interfaces or IP addresses. Thus, multipath protocols, and by extension the MCS, provide a solution for heterogeneous or migration scenarios. For example, if one section of the track supports only one kind of wireless technology and another section of the track supports another different one, the train supporting both technologies and using multipath communication protocols would maintain the RBC-train session without requiring the intervention of the application and performing transparently the vertical handover by the multipath protocol.

The proposal of architecture for the MCS is based on the use of Multipath Communication Managers that translate traditional IP communications to multipath communications. This middle box provides hardened communications to the ERTMS but it also can provide hardened communications to other critical services like the Detection System (DS). The architecture is presented in the Figure 42.

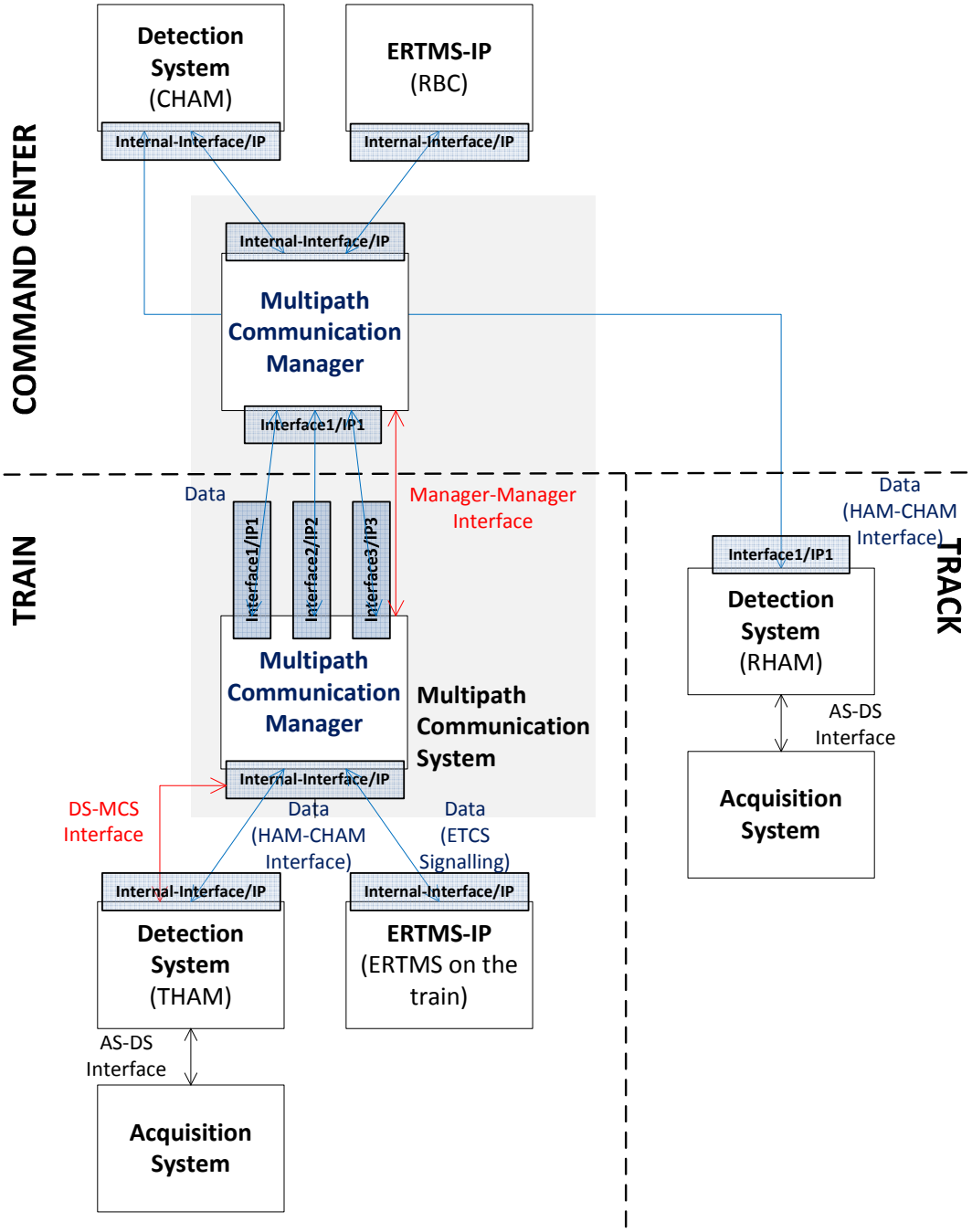


Figure 42: Architecture of the Multipath Communication System (MCS) and optional integration with the DS.

The use of a multipath communication manager has many advantages. Firstly, the integration of the ERTMS is much fairer and a smaller number of changes must be performed in the ERTMS in comparison with the changes required in case of implementing the multipath protocols inside the ERTMS. The main change is related to the communication module of the on-board ERTMS. Instead of using an integrated GSM-R module as legacy on-board ERTMSs, the new on-board ERTMS based on IP is required to be directly connected through a wired connection to the MCS and thus to delegate the communication management to the MCS. In this case the on-board ERTMS manages neither the wireless interfaces nor the multipath protocol nor the information exchange with the DS.

Secondly, apart from the on-board ERTMS, other critical systems may benefit from the resiliency of the communications provided by the multipath communication manager. For example, the THAM may be directly connected to the MCS using a cable to share the available wireless interfaces of the MCS with the ERTMS and to harden the communications with the CHAM thanks to the multipath protocol instead of using their own transceivers. This may suppose a reduction of the wireless transceivers required in a train.

Finally, it is important to remark that a preliminary architecture has been presented in the Figure 42 and that depending on the multipath protocol selected some changes may be required.

In the following subsections the main components and interfaces of the MCS are going to be described in more detail.

5.4.1Components

In the following table, the components of the MCS are listed and it is pointed out their relation to the work packages and tasks of the SECRET Project.

Component	Design	Proof of concept implementation
Multipath Communication Manager	WP4: T4.1 & T4.2	WP4: T4.4

Table 4: Components of the MCS and their relation to WPs and Ts of the SECRET Project.

5.4.1.1 Multipath Communication Manager

The Multipath Communication Manager provides the on-board ERTMS and the RBC with support for multipath protocols in order to harden communications between both elements against EM attacks and without requiring the implementation of the multipath protocol on the elements of the ERTMS.

This component may be composed of two main elements: the control module and the translation module. The translation module performs the translation between traditional IP protocols and multipath protocols, whereas the control module instructs the translation module how to perform the translation.

Indeed, the control module is responsible for applying the adequate traffic policy. It will depend on the presence or lack of the Detection System (DS):

- Lack of input from the DS.

  Due to the lack of information about EM attacks, the control module must implement a default mirroring traffic, which will mirror any packet through all the available interfaces and paths in the manager.

- Multipath Communication Manager governed by the Detection System (DS).

  The DS will instruct the Multipath Communication Manager how to manage its available interfaces depending on the detected EM attacks. Thus, a more efficient and dynamic traffic policies may be implemented. In general, only one interface or path will be used but depending on the EM attacks the active interface can be switched or even multiple interfaces may be used simultaneously mirroring

the data but only when it is strictly needed.

Due to the low bandwidth required by the ETCS application, load balancing traffic policies used in the standard multipath protocols could be unneeded for the current project. The multipath communication manager must be able to switch between networks interfaces maintaining without resetting the established connections and in the case of using simultaneously several interfaces, the traffic should be mirrored instead of load balanced between the active network interfaces. These are aspects that will be considered in the election of the multipath protocol.

5.4.2 Interfaces

Bellow, the main interfaces of the MCS are listed and it is detailed their relation to the work packages and tasks of the SECRET Project.

Interface	Design
DS-MSC Interface	WP4: T4.1 & T4.2
Manager-Manager Interface	WP4: T4.1 & T4.2

Table 5: Interfaces of the MCS and their relation to WPs and Ts of the SECRET Project.

5.4.2.1 DS-MSC interface

This interface is the interface between the Detection System (DS) and the Multipath Communication System (MCS), or more precisely, between the Health/Attack Manager (HAM) and the Multipath Communication System (MCS) of a train.

This interface has been detailed previously in the section 5.3.2.3 of this document.

5.4.2.2 Manager-Manager Interface

The interface between two multipath proxies will consist on the multipath protocol selected in order to strengthen the communication between the track and the train. This protocol should meet the next requirements:

- The multipath protocol must be aware of the multiple IP interfaces an end device has, so it must support multihomed end devices.
- The multipath protocol must manage the mobility and provide a solution for horizontal and vertical handovers.
- The multipath protocol should support different traffic policies for the paths, or at least, it should be easily modifiable to implement the desired traffic policies.
- The multipath protocol must suit to the current proposals of ETCS over IP.
- The multipath protocol should adapt to the deployment based on the use of Multipath Communication Manager, and thus it should adapt to the initial architecture proposed in the Figure 42.

Currently, at the time of writing this deliverable, Host Identity Protocol (HIP) (22) and Multipath TCP (MPTCP) (23) are considered to be the most adequate multipath protocols to be used in the MCS. Another third approach, due to the basic traffic policy required by the system, basically consisting on duplicating packets in the origin and discarding duplicated packets in the receiver, may be considered

Another third approach could be the use of Mobile IP (MIP) (24) with multiple Care of Addresses (multiple CoAs) (25), advanced routing or even Software Define Networking (SDN) to solve the mobility problem and

implement a simplified multipath system based on duplicating packets in the origin manager and on removing duplicated packets on the received manager.

References

1. **Alcatel; Alstom; Ansaldo Signal; Bombardier; Invensys Rail; Siemens;.** *ERTMS/ETCS System Requirement Specification.* s.l. : UNISIG, 2010. Mandatory Specification. 2.3.0.
2. —. *ERTMS/ETCS System Requirement Specification.* s.l. : UNISIG, 2013. Mandatory Specification. 3.3.0.
3. **Unife.** From Trucks To Trains, how ERTMS helps amking rail freight more competitive. [En ligne] 2012. http://www.unife.org/uploads/2012_ERTMS_Facts_sheets_1_-_18.pdf.
4. ERTMS Web Page. [En ligne] http://www.ertms.net.
5. *Radio bearer capacity and planning for ETCS, Solutions for BSS redundancy.* **Sauthier, Eric et Poutas, Laurent.** 2003. ERTMS Conference.
6. **Alstom; Ansaldo; Bombardier; Invensys; Siemens; Thales.** *ERTMS/ETCS RBC-RBC Safe Communication Interface.* UNISIG. s.l. : UNISIG, 2012. Mandatory Specification. 3.0.0.
7. *An overview of GSM-R technology and its shortcomings.* **Sniady, A. et Soler, J.** 11 2012, 12th International Conference on ITS Telecommunications (ITST), pp. 626,629.
8. *The European Switch: A Packet-Switched Approach to a Train Control System.* **Ruesche, S., Steuer, J. et Jobmann, K.** 3, 2008, IEEE vehicular technology magazine, pp. 37-46.
9. Project "Facilitating and speeding up ERTMS deployement" 2011-EU-60013-S. [En ligne] 20011. http://tentea.ec.europa.eu/en/ten-t_projects/ten-t_projects_by_country/multi_country/2011-eu-60013-s.htm.
10. Project "GSM-R Network Management, Frequency Management". [En ligne] http://www.uic.org/spip.php?article429.
11. *ERTMS/ETCS Protocol Stack main Alternative 1.* UNISIG. s.l. : UNISIG, 2013. Working document. 07.
12. BowTie risk analysis. [En ligne] http://www.governors.nl/bowtieexp.html.
13. **ETSI.** *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis.* s.l. : ETSI, 2011. Technical Specification. V4.2.3.
14. Carnegie Mellon software architecture methodology. [En ligne] http://www.sei.cmu.edu/architecture/.
15. **Bass, Len, Clementz, Paul et Kazman, Rick.** *Software Architecture in Practice (3rd Edition).* s.l. : Addison-Wesley, 2012.
16. **Ellison, Robert J., et al., et al.** *Security and Survivability Reasoning Frameworks and Architectural Design Tactics.* s.l. : Carnegie Mellon University, 2004.
17. ResiliNets Principles. [En ligne] https://wiki.ittc.ku.edu/resilinets_wiki/index.php?title=ResiliNets_Principles.
18. **Mateski, Mark, et al., et al.** *Cyber Threat Metrics .* s.l. : Sandia National Laboratories, 2012.
19. *Threats and Countermeasures in GSM Networks.* **Babu, K. Vsn Raghu et Ravi, T.** 2, 12 2012, International Journal of Engineering and Advanced Technology (IJEAT), Vol. 2. ISSN: 2249 – 8958,.
20. **Howard, Michael et LeBlanc, David.** *Writing Secure Code, Second Edition.* s.l. : Microsoft Press, 2003.
21. **Kraus, Thomas.** Low Budget GNSS Jammer. Munich, Germany : Institute of Space Technology and Space Applications University FAF.
22. **Moskowitz, R., et al., et al.** *RFC 5201 Host Identity Protocol.* s.l. : IETF, 2008.
23. **Ford, A., et al., et al.** *RFC 6182 Architectural Guidelines for Multipath TCP Development.* s.l. : IETF, 2011.
24. **Perkins, C.** *RFC 5944 IP Mobility Support for IPv4.* s.l. : IETF, 2010.
25. **R. Wakikawa, Ed., et al., et al.** *RFC 5648 Multiple Care-of Addresses Registration.* s.l. : IETF, 2009.

Annex 1: Principles of ResiliNets

The definitions of the eighteen principles below come from the presentation “Towards a resilient networking architecture”, Marcus Schöller, James Sterbenz and David Hutchison.

P1. ***Service Requirements*** determine the need for network resilience
P2. ***Normal Behaviour*** must be specified, verified, and refined through monitoring to understand normal operations
P3. ***Threat and Challenge Models*** are essential to understanding and detecting potential adverse events and conditions
P4. ***Metrics*** are needed to measure and engineer network resilience
P5. ***Resource Tradeoffs*** determine the deployment of resilience mechanisms
P6. ***Complexity*** of the network in general, and resilience in particular, must be reduced to maximize overall resilience
P7. ***Multilevel Resilience*** is needed with respect to protocol layer, protocol plane, and hierarchical network organization
P8. ***Translucency*** is needed to control the degree of abstraction vs. the visibility between levels
P9. ***Heterogeneity in Mechanism, Trust, and Policy*** among different network realms is a reality of emerging multiprovider networks
P10. ***Redundancy*** in space and time increases resilience against faults and some challenges
P11. ***Diversity*** in space, time, medium, and mechanism increases resilience against challenges to particular choices
P12. ***Autonomic*** behaviour is necessary for network resilience that is highly reactive with minimal human intervention
P13. ***Security and Self-Protection*** is an essential property of entities to defend against challenges in a resilient network
P14. ***State Management*** is an essential aspect of networks in general, and resilience mechanisms in particular; the alternatives of how to distribute and manage this state are critical to resilience
P15. ***Connectivity and Association*** among communicating entities should be maintained when possible, but information flow should still take place even when a stable end-to-end path does not exit
P16. ***Context Awareness*** is necessary for network components to operate autonomously to detect challenges
P17. ***Adaptability*** to the network environment is essential for a node in a resilient network to detect, remediate, and recover from challenges
P18. ***Evolvability*** is needed to refine future behaviour to improve the response to challenges, as well as for the network architecture and protocols to respond to emerging threats and application demands