Project details	
Project acronym	**PROTECTRAIL**
Project full title	The Railway-Industry Partnership for Integrated Security of Rail Transport
Grant Agreement no.	242270
Call ID and Topic	FP7-SEC-2009-1, topic SEC-2009.2.2.1

D01.14 – FINAL REPORT

Dissemination status	
Version of the document	1.03
Responsible partner	ASTS
Reviewing partner(s)	-
Date of the last version	19/11/2014
Dissemination level	PU

Approval status		
Author(s)	**Reviewed by**	**Authorised by**
SP leaders and co-leaders	C. Dambra, ASTS, F. Papa, ASTS	V. Siciliano, ASTS
14/11/2014	19/11/2014	19/11/2014

TABLE OF CONTENTS

1 Introduction....5
2 SP1 Dissemination and exploitation of results....7
2.1 Objective of the SP1....7
2.2 Main results of SP1....7
2.2.1 Dissemination....7
2.2.2 Exploitation....8
3 SP2 Functional and Technical Railway Security Specifications....10
3.1 Objective of the SP2....10
3.2 Main challenge....10
3.3 Main findings....10
3.4 Main benefits to end-users and industry....11
4 SP3 Integration Sub-Missions (Physical & Operational Assets)....12
4.1 Objective of the SP3....12
4.2 The SP3 WPs results....12
4.2.1 Stations and buildings....12
4.2.2 Structures....14
4.2.3 Tracks....15
4.2.4 Signalling & power distribution....15
4.2.5 Communications and information systems....17
4.2.6 Rolling stock clearance....17
4.2.7 Staff clearance and access right management....18
5 SP4 Integration Sub-Missions (Transported Assets)....20
5.1 Objective of the SP4....20
5.2 The SP4 WPs results....20
5.2.1 Passenger clearance control....20
5.2.2 Luggage clearance control....22
5.2.3 Freight clearance control....23
5.2.4 Special tunnel and fast tracks security....24
6 SP5 Global Integration....25
6.1 The PROTECTRAIL integration framework....25
6.2 Demonstration Run in Zmigrod/Poland....27
6.2.1 Demo site characteristics....27
6.3 On-Board and way-side equipment installation....28
6.3.1 The Video Monitoring System....28
6.3.2 The Platform....29
6.3.3 The Container....31
6.3.4 The Gantry....32

6.3.5 The Fence....33
6.3.6 Loco and Cars....33
6.3.7 The Zmigrod Architecture....35
6.3.8 Scenario Description....35
6.4 The Official Zmigrod Demo event....50
6.5 Non-functional Demonstration....55
6.5.1 Front camera solution....55
6.6 Demonstration Run in Sicily /Italy....56
6.6.1 The Location and the Security system....56
6.6.2 The security installations....56
6.7 Demonstration Run in Villecresnes/France....58
6.7.1 Experimentation objective....58
6.7.2 The location and the site description....58
6.7.3 The security installations....59
6.7.4 General conclusions....59
6.7.5 Conclusions by system....60
6.7.6 Images of the Villecresnes Demo....61
6.7.7 Conclusions....62
6.8 Lessons learnt from the demonstrations....63
6.8.1 Enabling security solutions....63
6.8.2 Network communication....64
6.8.3 Modern and practical approaches to video and video-based analytics....65
7 SP6 Future design for Security....67
7.1 Vision of Railway in next 10-20 years....67
7.2 Modelling the railway security systems in the framework of complex system dynamics....68
7.2.1 The first developed model....68
7.2.2 The second developed Model....69
7.3 Future design for prevention....69
7.4 Future design for mitigation....70
7.5 Future design for crisis management....70
8 High Probability Low Impact (HPLI) events within PROTECTRAIL....71
9 Conclusions....73
10 The PROTECTRAIL Consortium....74

DEFINITIONS AND ACRONYMS

Acronym	Meaning
BPMN	Business Process Management Notation
CBRNE	Chemical, Biological, Radiological, Nuclear and Explosives
CMS	Crisis Management System
DSCP	Differentiated Services Code Point
ECS	Emergency Communication System
EDA	Event Driven Architecture
EHP	Emergency Help Point
HMI	Human Machine Interface
HPLI	High Probability Low Impact
ICT	Information and Communication Technology
IP	Internet Protocol
ISM	Integrated Security Management
LOS	Line Of Sight
LTE	Long Term Evolution
MCG	Mobile Communication Gateway
MPLS	Multi-Protocol Label Switching
NTP	Network Time Protocol
OBCU	On Board Control Unit
PIS	Passenger Information System
PoE	Power over Ethernet
QOS classes	Quality of service classes. In Each class flows a certain traffic with different requirements (bandwidth, delay Jitter)
RCS	Rail Control System
RTT	Round Trip Time
SOA	Service Oriented Architecture
SOCC	Security Operational & Control Centre
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VRF	Virtual Router and Forwarding
WCG	Way-side Communication Gateway
Wi-Fi	Trademark name for Wireless Communication Technology
WS	Web Services

1 INTRODUCTION

Security is a cornerstone of any sustainable mobility policy and mobility system. Making rail transport secure is complex as it must be open and accessible and enable an efficient flow of passengers and goods. At the same time, a rail, like any other transport system, faces a broad spectrum of threats, ranging from low-probability-high-impact events (e.g. terrorist attack) to high-probability-low-impact (e.g. vandalism) that make different security technologies necessary (e.g. chemical sensors, intrusion detection systems, video management systems). This leads to the challenge of integrating the various security technologies into a coherent and easily manageable system.

The PROTECTRAIL consortium and its 29 members, consisting of railway operators, railway manufacturers, security technology providers, research organisations, and major railway associations, came together to improve railway security in the light of the challenges outline above. PROTECTRAIL objective was to integrate the growing influx of security technologies into rail operations and make them interoperable to improve security. For this reason, PROTECTRAIL designed an *interoperability framework* built on a system-of-systems approach. This is a modular architectural framework into which asset-specific and interoperable security solutions can be "plugged", giving operators and infrastructure managers the possibility to continuously adapt their security systems to the changing security needs with minimal non-recurring engineering costs. This framework basically consists of a set of rules and standards which facilitate the integration and communication amongst various security technologies.

It is based on three key ideas:

1) **interoperability** is improved through standardisation,
2) **re-use** of existing and relevant international standards is preferred, and
3) simplicity is key to long-term adoption.

PROTECTRAIL based its interoperability framework on design patterns which are successfully used in other industries. These include the following elements:

- A reusable **Service-Oriented Architecture** (SOA);
- An **Event-Based Architecture** for data exchange between various security components and decouple the components from each other;
- Reusing of well-established and proven **standards** which reduce the non-recurring cost of software integration;
- Planning of an **extendable** architecture for the future to extend the framework with upcoming standards;
- Building **modular** components with web services;
- Supporting **discoverable** components to reduce the configuration effort and improve the reusability;
- Building on an **IP network** (cabled or wireless) which is dimensioned to support consistently the **video surveillance streams** necessary to assess, confirm and investigate security incidents.

PROTECTRAIL tested this interoperability framework during field demonstrations concentrating on four priority facets: Event-Driven Service-Oriented Architecture, Network Communications, Video Management, and Security Technology. In the course of PROTECTRAIL it became clear that security systems need to be designed in a future-proof manner. For this to happen, the operator or infrastructure manager implementing a security system must devise a security master plan that contains fundamental ICT principles and an overarching IT architecture. This master plan should not focus on *what* technology to deploy but on *how* to deploy it.

The project has been organised around 6 Sub-Projects (SP) as reported in Figure 1.

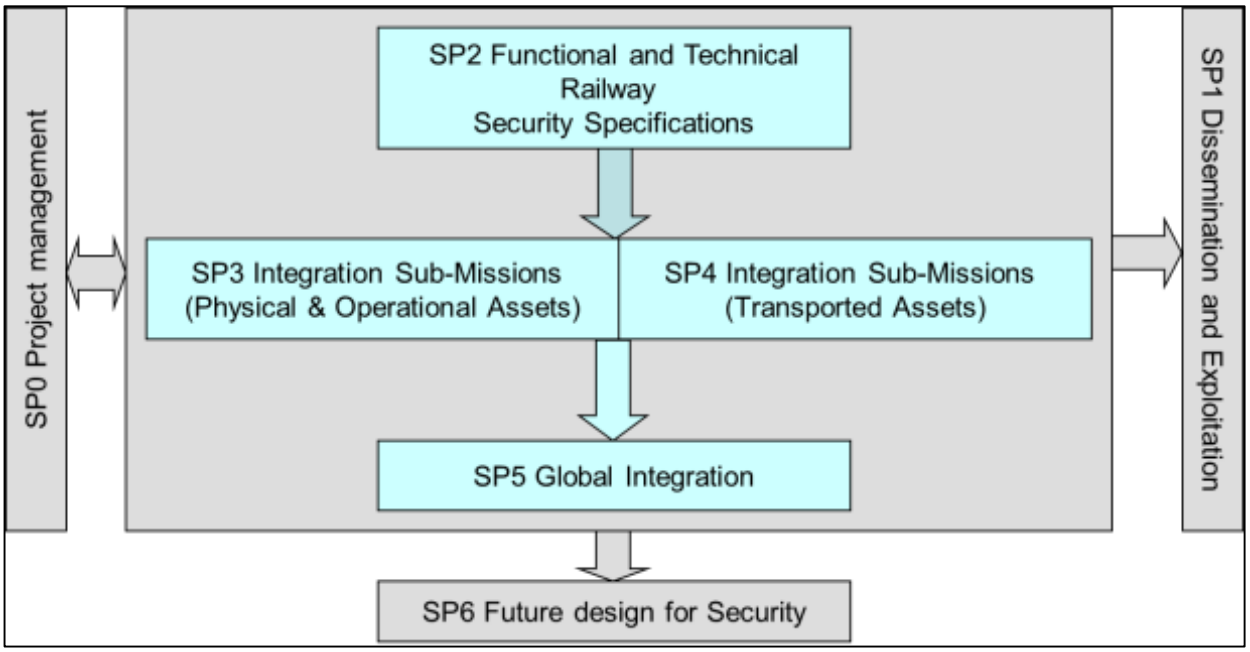


Figure 1 The PROTECTRAIL Structure

In SP1 the dissemination mechanisms of the project (web-site, workshops, etc.) have been organised and set-up, main events have been organised (the list of the most important is reported at the end of this document), and key reports including the PROTECTRAIL White Paper and the Report on recommendations for National and EU authorities, standardisation bodies and UIC Code have been published.

In SP2 the first, second and third rounds of user requirements elicitation, specification and prioritisation and assessment of regional disparities have been completed and the Stakeholder Advisory and Validation Group has been managed through the organisation of several meetings in Europe to feed the work of both SP2 and SP5 with input from other stakeholders. SP2 has also supported the project demonstrations with privacy and ethics recommendations.

In SP3 and SP4 the planned work on the single missions demonstrations, described in more details in the next paragraphs, for both physical and operational assets and transported assets has been achieved through the design, development and validation of the in-lab prototypes.

In SP5 the general principles for the SOA-based interoperability framework have been defined as first step. Then the main scenarios to be demonstrated in the main Polish demonstration site and in the French and Italian satellite demonstration sites have been produced in parallel with the detailed design of the ICT architectures for the security of both passenger and freights and for crisis management. Finally the main demonstration in Poland and the satellite demonstrations in France and Italy have been designed, organised and successfully implemented. In particular the main demonstration has shown the integration of almost all the in-lab prototypes developed in SP3 and SP4 into a single railway security system, the satellite demo in France the application of security solutions to high speed railway line in harsh environments while the satellite demo in Italy has demonstrated a cross-border application of the PROTECTRAIL integration framework for the protection of railway lines. SP5 has been concluded with a cost-and-benefit analysis of the applied technologies extended to the application of considered technologies to High Probability Low Impact (HPLI) events.

In SP6 two basic models of railway security forecasting based on 2 different approaches have been designed, implemented and validated offering possible future solutions to increase railway security by protection and mitigation means and effective and efficient measures to support and/or increase the capability of crisis management. SP6 has also delivered a vision of future railway system in next 10-20 years.

2 SP1 DISSEMINATION AND EXPLOITATION OF RESULTS

2.1 OBJECTIVE OF THE SP1

The objective of SP1 was to guarantee proper diffusion of knowledge and projects results inside and outside the consortium in order to ensure sector acceptance and implementation of the results. The promotion of the project involved

- the project partners to exchange knowledge,
- the end-users to achieve sector acceptance of the project results and ensure that final implementation will be possible,
- the stakeholders outside the consortium such as national and EU authorities, standardisation bodies, external industry, external academic community,
- the general public to be informed.

2.2 MAIN RESULTS OF SP1

2.2.1 DISSEMINATION

Dissemination was a horizontal activity, accompanying all other sub projects throughout the whole duration of the project. All relevant target groups had access, depending on their rights, to the project knowledge in the PROTECTRAIL dedicated knowledge platform.

A public website was implemented at the very beginning of the project and updated during the whole project. In parallel various adequate media was used: brochure, project newsletter, press releases, articles in UIC e-news (UIC electronic weekly newsletter with more than 5000 addresses), the project video, flyers, posters, roll-ups, publications, etc. All these communication media can be downloaded on the website at http://www.protectrail.eu.

Various conferences and workshops was organised to address the different target groups and ensure that rail end-users were properly involved and informed of the PROTECTRAIL viable and integrated set of railway security solutions:

- Public conferences were held during the life of the project to inform widely on the project development and to disseminate the results to the different actors and decision-makers from the railway business and in particular:
    - PROTECTRAIL Info day on 04/05/2011 in Paris;
    - PROTECTRAIL Info day at the 8th annual UIC world Security congress on 24/10/2012 in Bratislava;
    - PROTECTRAIL Final conference in Paris on 27/05/2014.
- Workshops to ensure that the project was running in the right direction for end-users in and outside the consortium; external entities (European organizations, police and security forces) participated actively in the workshops. The main workshops were the following:
    - workshop on regional disparities on 14/03/2011 in Brussels;
    - workshop on user requirements and priorities on 01/06/2012 in Roma;
    - workshop on new technologies on 01/06/2012 in Roma;
    - workshop with police authorities on crisis management on 04/09/2012 in Paris.
- The following demonstrations events to show the solutions in real conditions
    - PROTECTRAIL Main Demonstration on 08-11/10/2013 in Zmigrod (PL);
    - PROTECTRAIL stand with demonstration during the 9th UIC world security congress on 13/11/2013 in Paris;

- PROTECTRAIL High-Speed Lines Demonstration in Villecresnes near Paris on 25/02/2014;
- PROTECTRAIL High Probability Low Impact (HPLI) Contest and Demonstration on 27/05/2014 in Paris;
- PROTECTRAIL Traditional Lines Protection Demonstration on 27/05/2014 in Paris with remote connection to the Palermo Brancaccio station in Italy.

All these events acted as platforms to facilitate the sharing of information and collaboration between members of the consortium and all other participants and helping to develop synergies that will go beyond the development of the project.

In addition the PROTECTRAIL partners presented the results of PROTECTRAIL in a wide range of international events gathering a majority of the decision-makers from the different railway stakeholders

2.2.2 EXPLOITATION

One of the key issues in the dissemination and exploitation process was to initiate a cooperation framework with the National and EU authorities and standardisation bodies and to generate possible proposals for recommendations to be adopted by National and EU authorities and standardisation bodies. For this purpose the project partners produced a White Paper which summarises the most important lessons learnt of the project and which gives technical recommendations for future users of the PROTECTRAIL framework. It's the reference document that will support guidance (recommendations) towards technical standardisation. The White Paper is available on the PROTECTRAIL website.

In addition to the white paper, a UIC leaflet which regroups the main recommendations focusing on Organisational and Human Factors to be taken into account by rail end-users will be available for UIC members within the security platform.

The exploitation report describes the steps to be taken after the end of the project and especially the activities that will be carried out by all the PROTECTRAIL partners with their own resources and how they will continue to use the results of PROTECTRAIL. There is a strong interest among the consortium and among stakeholders to introduce the results of PROTECTRAIL into the railway security market. PROTECTRAIL can benefit both suppliers and end-users by reducing non reoccurring engineering costs which make security solutions unnecessarily expensive to supply. Once implemented the PROTECTRAIL framework should help deliver better products at a better price.
The project has laid a solid foundation for further exploitation activities after the end of the project. UIC will continue to host and maintain the PROTECTRAIL website, the private workspace and the mailing lists; to disseminate the results in international events related to rail security; and will have a permanent contact point to answer to the request of interested stakeholders.

PROTECTRAIL supported standardization is in progress to accommodate the IT revolution and associated ubiquitous communications:

- PROTECTRAIL had a window of opportunity to feeding its recommendations to the official M487 process. The M487 mandate is a result of the request of the European Commission to the European standardisation organisations to draft three European standardisation roadmaps in the security sector under Action 1 of their Communication on Security Industrial Policy with the aim to promote the global competitiveness of the EU security industry while enhancing the security of Europe. PROTECTRAIL partners derived from the project's interoperability framework, guidelines for a minimum level of data interoperability necessary for proper multi-stakeholder crisis management. By feeding PROTECTRAIL findings into the standardisation process and embedding them in European standards is the only future-proof option to initiate acceptance among stakeholders that were not partners of the project.IEC62676 with ONVIF CCTV and intrusion detection has been promulgated;
- Through its CCTV Experts Group on CCTV, jointly established with FP7 SECUR-ED, PROTECTRAIL experimented ONVIF interoperability scheme for all its video-surveillance

components or services (including for video analytics modularity) and fed-back through its members to IEC/CENELEC TC79, while IEC 62676 was in its finalization phases. IEC 62676, promulgated in October 2013, incorporates the ONVIF profiles validated in PROTECTRAIL, consistently with the event based SOA model implemented. IEC 62676 is also the base for the on-going development by IEC TC9 of a rail on-board CCTV standard (IEC 62580-2) consistently with the architecture defined in IEC 62580-1.

- PROTECTRAIL had a decisive role in the finalization of ISO 22311 Video-surveillance Export Interoperability, promulgated in November 2012 and the results of the final demonstrations, which implemented for the first time the standard, will feed the amendments to Edition 1, especially with regard to the data model for the metadata attached to the video streams. ISO 22311 defines minimum interoperability requirements in the export of video files to forensics investigators to facilitate a consistent exploitation of evidence produced by different and heterogeneous video systems (typically on-board and wayside). This roadmap to update ISO 22311 has been presented in June 2014 to the ISO TC223 meeting in Lucerne and is scheduled to enter its active phase mid-2015. It is worth noting that ISO 22311 is already called in the procurement specifications established by key European public transport operators.
- IEC/TC9 (railway non-safety standards) is adapting to the new situation with integration of new security solutions and IEC 62580-2 on-board CCTV remains a hot and active topic. IEC TC9/WG46 is already well aware of PROTECTRAIL, with Alstom, Bombardier Transportation, SNCF and Thales active members. In particular, PROTECTRAIL approach on interoperability framework is consistent with IEC WG46 62580-1 and therefore IEC WG46 team is seeking for PROTECTRAIL partners expert advice on injecting some of PROTECTRAIL results.

Finally some of the key PROTECTRAIL results will be transferred by the founding members as background knowledge into the Shift2Rail joint undertaking of the European Commission and the private sector for rail research.

3 SP2 FUNCTIONAL AND TECHNICAL RAILWAY SECURITY SPECIFICATIONS

3.1 OBJECTIVE OF THE SP2

The main scope of the SP2 was to generate a set of functional and technical specifications to comply with needs and priorities of railway stakeholders and/or having impact on railway security policies and on the human rights to privacy. The activities of the SP2 were spread over the entire life of the project in order to refine requirements and specification taking into account possible variations due to changed environmental conditions/technological evolutions. Among the SP2 responsibilities there was also the task of collecting information and feedbacks from the European railway stakeholders on the various activities of each SP2 work package. In the figure below are synthetized all the SP2 work package activities and their dependencies.

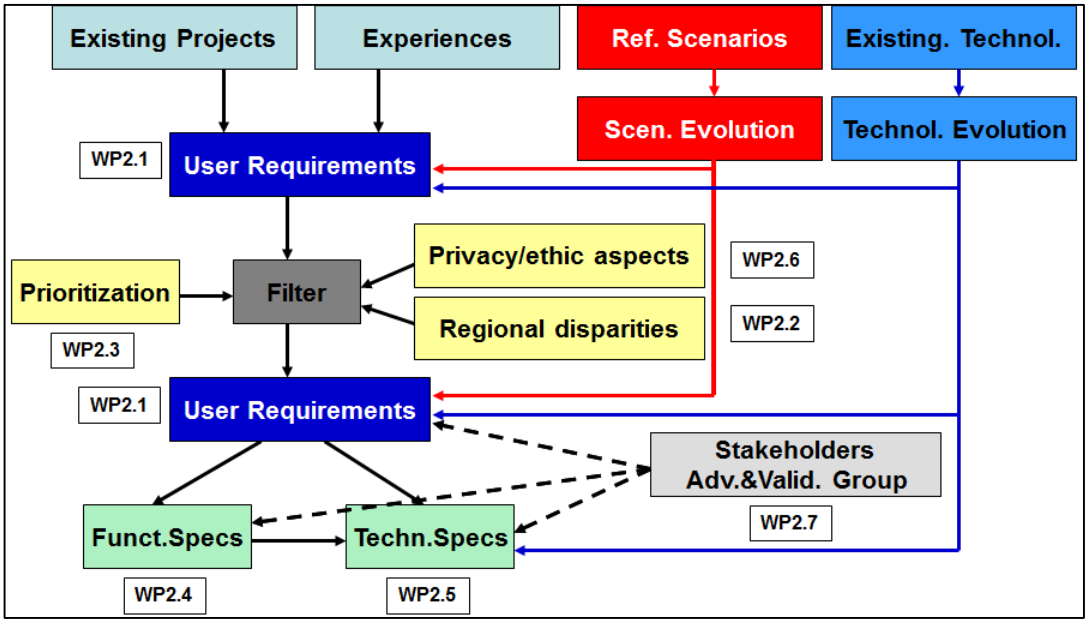


Figure 2 SP2 WPs and Dependencies

3.2 MAIN CHALLENGE

The main challenge of the SP2 was to synchronize all the activities of the its WPs in order to obtain a single line of reasoning that would allow, starting from the identification of the stakeholder requirements and their prioritization, to identify and refine the functional and technical specification and a set of reference scenarios to be used as a starting point for all the activities of SP3 and SP4 taking into account the applicable privacy policies. It must be considered that all the SP2 results have been achieved working closely with the major railway stakeholders both inside and outside the project and this aspect has been another important challenge to be addressed in terms of organization and integration.

3.3 MAIN FINDINGS

The SP2 work led to the following results:

- Identification and prioritization of a structured set of security related stakeholder requirements containing the main present and potential emerging threats for the railway system;
- Definition of a subset of scenarios which provides details on security issues identified by the interviewed stakeholders;

- Elaboration of a socio technical functional requirements analysis aimed to highlight the various functions to be developed in order to satisfy the various security end stakeholder requirements. The focus has been put on the relationship among the various functions to explore the complexity of the various PROTECTRAIL missions.
- Definition of a set of technical performance specifications and technical and operational constraints as a complement to the identified functional specifications.
- Analysis of the regulation and privacy rights in order to provide guidelines for the implementation of viable solutions that include and respect privacy and citizen's rights.

3.4 MAIN BENEFITS TO END-USERS AND INDUSTRY

The SP2 activities have allowed identifying the needs and the priorities of the major railway stakeholders in terms of security aspects. Therefrom have been derived devoted functional and technical specifications to be used as guidelines for the implementation of integrated security systems. Consequently the end-users and, more generally, the industrial world can find an updated set of information about the major railway security threats, the needs of the railway operators and a complete set of information useful for the implementation of security systems able to satisfy the current priorities of the railway world.

4 SP3 INTEGRATION SUB-MISSIONS (PHYSICAL & OPERATIONAL ASSETS)

4.1 OBJECTIVE OF THE SP3

The scope of SP3 was to demonstrate the feasibility of solving the identified railway protection submissions through an efficient and cost effective integration of technologies. Closely reflecting the main needs in the railway sector, these sub-missions focused on protection of key assets:

- stations and buildings;
- structures;
- tracks;
- signalling & power distribution;
- communications and information systems;
- rolling stock clearance;
- staff clearance and access right management.

The high level objective of SP3 was the design and development of in-laboratory proof-of-concept performance prototypes able to demonstrate the feasibility of the protection of **fixed assets**. In Figure 3 are synthetized all the SP3 work packages and their dependencies.

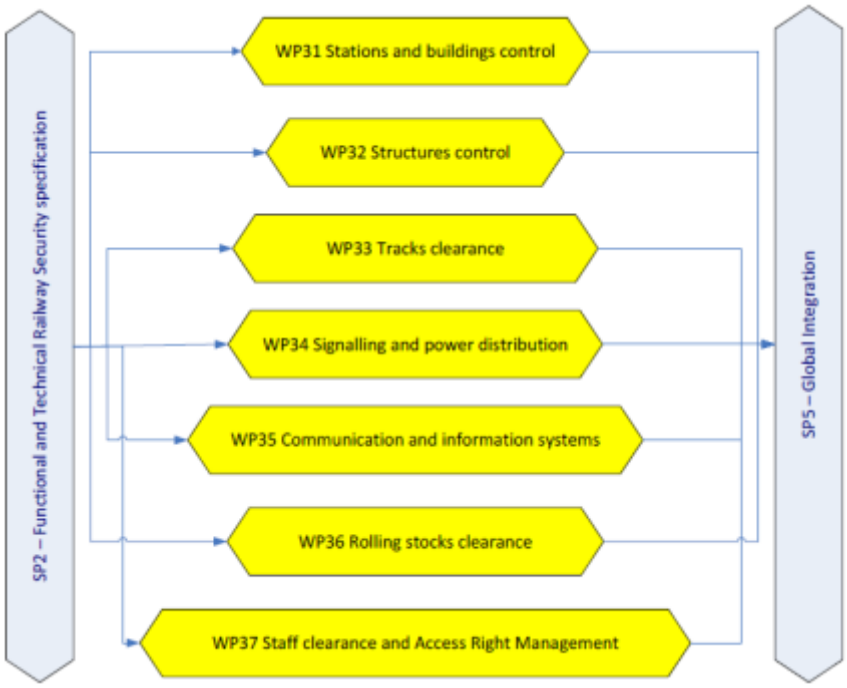


Figure 3 SP3 WPs and Dependencies

4.2 THE SP3 WPS RESULTS

Here below are reported the in-laboratory proof-of-concept performance prototypes obtained by each SP3 work package for each specific protection solutions:

4.2.1 STATIONS AND BUILDINGS

The mission of this work package was the monitoring and control of railway station assets, particularly buildings and public sites within the precinct (such as platform/track interface, passenger

premises, short-term and long-term parking areas, office building, taxi and bus stations etc.). Such mission has been addressed through the following main technical objectives:

- integration of different and heterogeneous sensors and video analysis algorithms
- a unique situation display.

These objectives entail a series of technological challenges:

- Security performance (low false alarms) in a real operational environment
- Alignment of different events and metadata in a unique integration framework
- Added value and user friendly information display
- Data management
- Video Analytics interoperability
- Semi-automatic tracking in crowded areas.

Inside Figure 4, Figure 5 and Figure 6 are synthetized the monitoring and control solution developed inside this task, which have been tested in lab as reported above and which have also been shown during the PROTECTRAIL demo in Zmigrod.

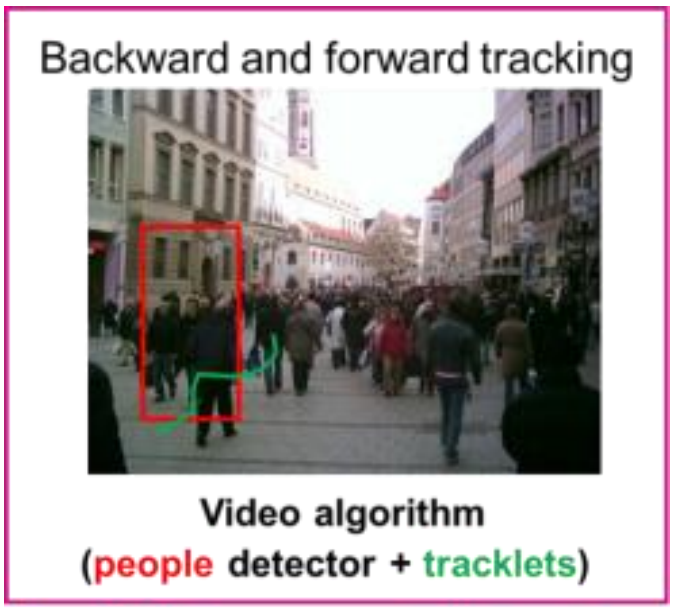


Figure 4 Backward and forward tracking

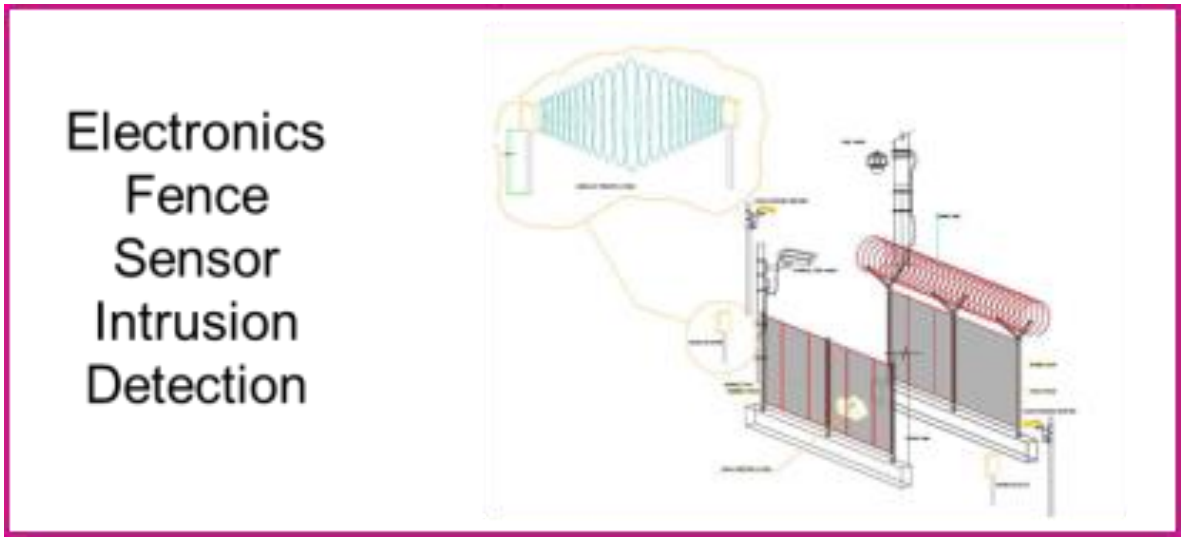


Figure 5 Electronics Fence Sensors for Intrusion Detection

Figure 6 CCTV Basic Services

4.2.2 STRUCTURES

Managing possible terrorist incidents presents new challenges. Within the railway system it has been identified areas of vulnerability in which terrorist attack, natural disaster or accident can create severe damage by risking the lives of many people and/or affecting this important means of logistics. Areas of tunnels, bridges, embankments and railway yards have been defined as one of the security risk areas within the railway system. The mission addressed by this work package aimed to pursue the protection of railway subsystems against all kind of threats that have a major impact on the functioning of structures (e.g. tunnels, bridges, embankments, yards).

To this scope an “Expert system for CBRNE consequence analysis” has been developed and integrated with the PROTECTRAIL system. This software tool gives visual output regarding damage to infrastructure, the size of the area to be evacuated, and the hazardous area for first responders. It supports the crisis management team during a crisis, but can also be used during the planning phase for training activities. The software can be applied in various types of infrastructure ranging from tunnels and bridges to stations and buildings. The solutions were run and demonstrated during the official Zmigrod demo days.

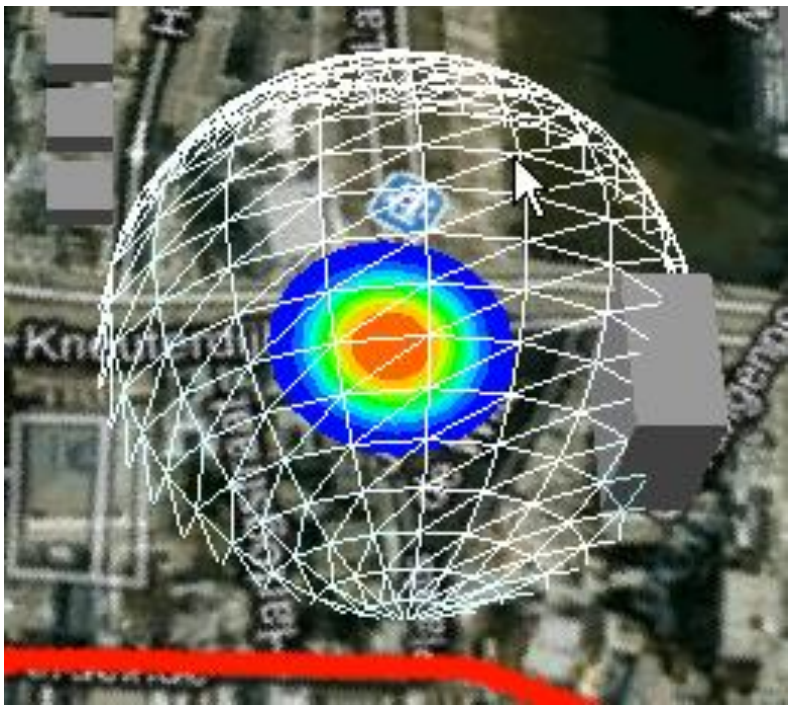


Figure 7 Structures Control

4.2.3 TRACKS

During the activities of this work-package it has been developed three different systems:

- The Level Crossing Video Surveillance HD System;
- The High Speed and High Accuracy 3D Profiling of Tracks and Ballast system;
- The Automatic Detection of Intrusion in Tracks, Tunnels and Bridges subsystem.

Relating to the **Level Crossing Video Surveillance HD System**, the system demonstrated its ability to record continuously in a local storage the video obtained with a camera that covers the level crossing area. The video recording is synchronized with the level crossing equipment. In normal operation, the video is recorded in standard quality mode and when a train approaches to the level crossing area, the level crossing equipment sends a signal to the video equipment and the video recording changes to high quality mode. When the train leaves the level crossing area, the level crossing equipment sends a signal to the video equipment and the video recording changes again to the standard quality mode. The in lab tests where successfully performed in Madrid and then the system was installed, integrated and demonstrated as fully efficient in Zmigrod demonstration test site.

Relating to the **High Speed and High Accuracy 3D Profiling of Tracks and Ballast system** (BPDS Sensor), this system is composed for a 3D acquisition and IR laser combined with an optical chain to generate a profile on the railway, a 3D camera to create an image by concatenating the profiles and an acquisition software to store both 3D and 2D images with localisation and time. The algorithm makes possible to detect any singularity provided by any object that would be ten times bigger than a piece of ballast and higher than the level of the ballast. For buried objects, the difference between the level of the ballast between two sleepers and the expected one shall be identified when higher than 10 cm. The system was demonstrated as reliable and in line with the requirements during the Zmigrod demo days with the commission officers.

Relating to the sub-system for **Automatic Detection of Intrusion in Tracks, Tunnels and Bridges**, a Network Video Analytics (VA) device performs intrusion detection on media data and metadata received from an IP streaming device. This system was delivered and integrated in Zmigrod. The Video Analytic system learns the default background model of the defined zone and automatically adapts to changing environment. Whenever any discrepancy occurs between incoming frame and the model, the moving object is tracked or associated to the previous detection. After few seconds of constant track, an alarm is triggered. Operators visually confirm the alarm, using management station. The environmental properties such as weather conditions, strong wind, rain, snow, fog, day and night, moving trains, cars, people which do not violate sterile zone do not to trigger an alarm. The solutions were run and demonstrated relevant expected performances during the official Zmigrod demo days under commission officers' supervision.

4.2.4 SIGNALLING & POWER DISTRIBUTION

The objectives of this work package were of 3 types:

- monitoring technologies, i.e. technologies to monitor suspicious events related to the signalling and power distribution systems and to implement consequent strategies to reduce the potential impacts;
- track-side physical security, i.e. improvements of the physical security of track-side railway signalling and power distribution components (those hosted in stations or other railway buildings are covered by other security sub-missions of PROTECTRAIL);
- ICT protection of computer-based signalling systems.

The architecture of the realized prototype was composed by an ICT network, simulating a command and control system for railway environment and an armoured rack for hosting railway signalling and power distribution equipment with sensors for detection of tampering and unauthorized accesses.

The rack, as depicted in Figure 8, was equipped with an anti-intrusion/control access system consisting of a central unit connected to sensors, an electromechanical lock, a terminal device, a management SW and an adapter. The sensors used and their related functions are the following:

- electromagnetic sensor connected to the front door whose purpose is to detect the opening of the front door;
- electromagnetic sensor connected to the rear panel whose purpose is to detect the intrusion from the rear panel;
- inertial sensor connected to the rack whose purpose is to detect the shaking, lifting, bumping or moving of the rack;
- glass breaking sensor with piezoelectric technology connected to the front door glass whose purpose is to detect the breaking of the glass;
- lock position sensor, indicating the status of the lock (open/close).

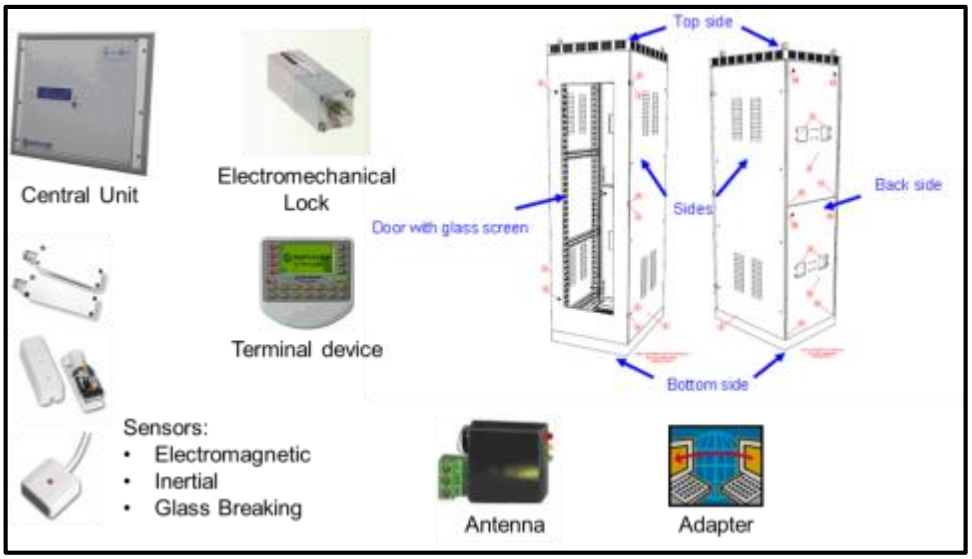


Figure 8 Signalling & Power distribution protection system

Regarding the ICT protection of computer-based signalling systems it must be said that the railway domain is supplied with a telecommunication network, required to collect events and alarms from the railway environment and to manage it (configuration and commands).

The purpose of the here briefly described architecture solution, depicted in Figure 9, was to prevent, detect and report alarms related to the following cyber-attacks: network asset modification; Port scanning and Foot printing; Denial of Service; Man in the middle; Virus infection; Rootkit injection; Central location disaster.

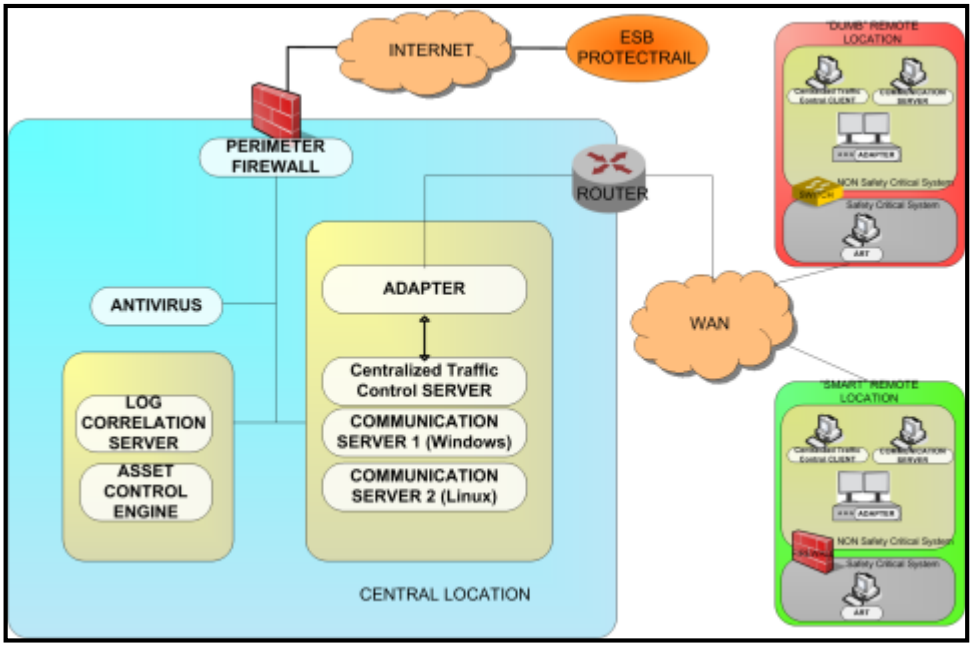


Figure 9 Signalling & Power distribution Cyber Security

The systems were run for many tests in Zmigrod. They demonstrated systematic alarm emission when any forbidden action attempt occurred. The high performance of the system in an integrated environment was demonstrated during all the tests and demonstration with the commission officers.

4.2.5 COMMUNICATIONS AND INFORMATION SYSTEMS

The work package identified the integrated ICT solution necessary to improve the security of rail transportation and reduce disparity in European railway ICT systems. The system incorporated the general technology definitions and design of the different ICT systems inside PROTECTRAIL identifying the different sub-systems and defining their interfaces; integrating the various sub-systems; evaluating the integrated sub-systems for the Pan-European interoperability; identifying solutions to reduce the bandwidth needed to control the supervised devices located in the periphery; identifying the best solution to monitor the QoS of the ICT system and prevent bottleneck or corruption of services.

Focus of this work package was communication infrastructure supporting information and security services and its characterization in term of information security and service availability. Communication infrastructures enabled broadband IP communication through wired and wireless media, in accordance with the amount of data to be transmitted in Zmigrod, like video, in parallel to operational data like alarms or controls. Railway-specific ICT systems offered resilient multi-service communication.

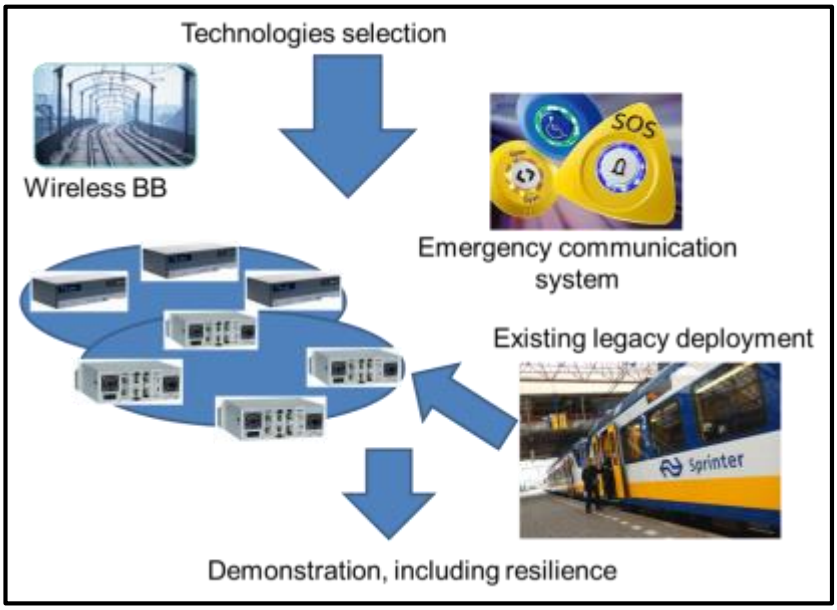


Figure 10 Communications and Information systems

4.2.6 ROLLING STOCK CLEARANCE

The purpose of the Work Package was to implement security protection solutions for rolling stock clearance. A main target was to achieve integration into the system architecture. Context was about rolling stocks: locomotives, wagons for passengers / goods and other material like construction machines (dangerous goods are not contained). The target was to show how the security subsystems installed on-board the rolling stock and at ground level for operation in travel situations can be used to demonstrate the train clearance. In addition, the check of the train clearance in a low power autonomous mode with generic transmission means was targeted to provide its surveillance when it is unattended. During the Zmigrod integration and tests process, the systems demonstrated good performances and low false alarm rate for the following detections :

- People intrusion through the gantry in the virtual depot
- Car out of predefined limits of the train gauge at right, left or top of the train through gantry detection
- People intrusion in the train opening a door, through sensors activation

- People moving in the train through camera integrating motion detection
- Intruder trying to access the virtual cabin identified without valid authorization (Access control at the entrance of the cabin, the driver needs to present his badge and put his finger on the device so that his fingerprint and vein are acquired and compared to the biometric data stored on the card. Face recognition in front of the driver seat, so that authorized people only could drive the train).
- Full transmission from the train to the ground through the telecom systems

Zmigrod tests demonstrated the relevant ability of the systems to run under various environmental conditions (sun, rain, cold, etc.), showing that the technology is ready for operation.

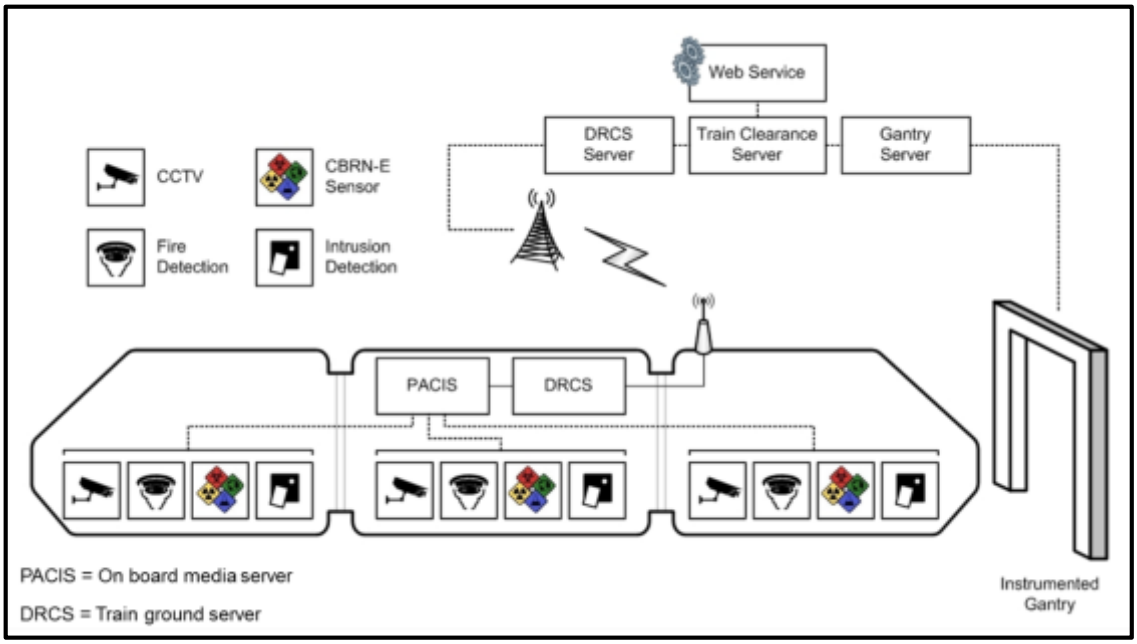


Figure 11 Rolling Stock Clearance

4.2.7 STAFF CLEARANCE AND ACCESS RIGHT MANAGEMENT

The scope of the work package was to provide the relevant mechanisms to manage the staff access rights management. The objective included the driver cabin, the supervision of the driver during a journey, the logical access control to the information system (on board & the ground system) and to any sensitive building. The objective covered also the mechanisms to ensure that authorized staff is not under an external constraint.

Correct identification of the staff member was shown when a staff member tried to use his ID Card to access a sensitive area. His identity was correctly confirmed by comparing his fingerprints captured live with his fingerprints stored in the ID Card and all other relevant conditions being met, access was every time granted by the system. The correct detection of access attempts by unauthorized persons in case of an unauthorized person attempts to gain access to the sensitive building, using the ID Card of a staff member was demonstrated the system not granting access with a systematic high reliability. The same successful result has been observed at the entrance of the driver cabin, where the access control was different from the one used at the entrance of the sensitive building (here, vein and fingerprints were acquired). Here, the test was made with a recently fired employee. This person still had his ID card and tried to access the control cabin with it. As his ID card was not deactivated, he could enter in the corresponding area. However, as the access hour was suspicious, the system generated an event for informing the operator someone was entering the driver cabin. Moreover, the suspect was then detected by a camera installed at the front of the train commands and recognized the user as an unauthorized person trying to drive the train. As a result, another alarm was sent right away.

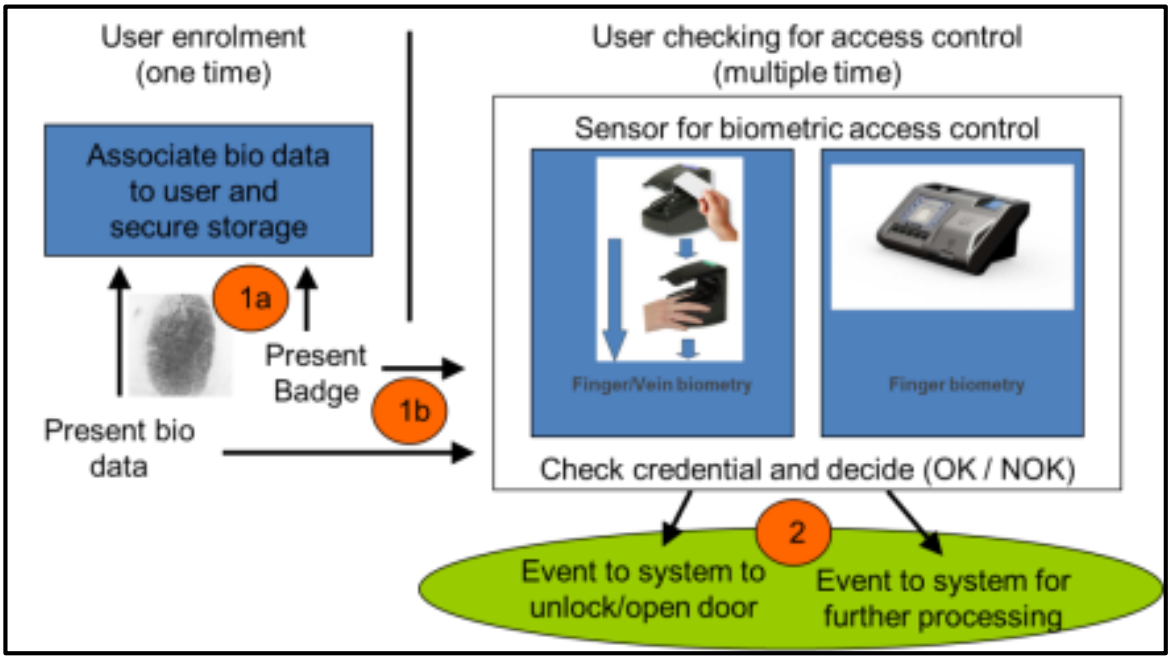


Figure 12 Staff clearance and access right management

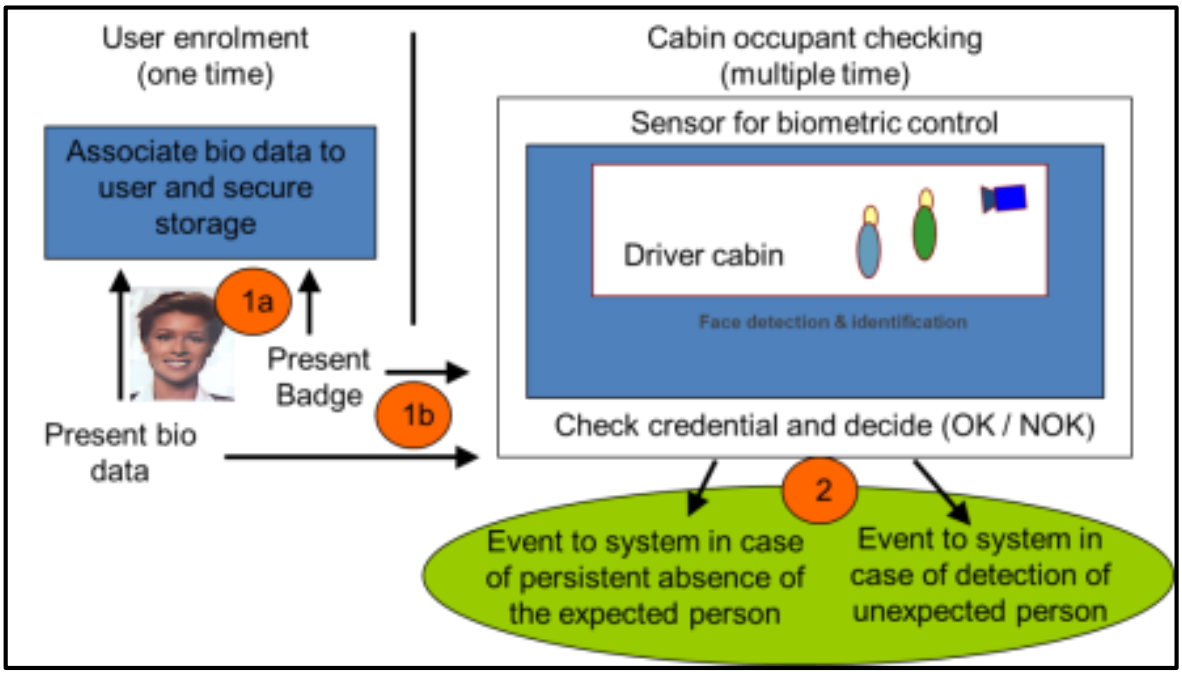


Figure 13 Staff clearance and access right management

5 SP4 INTEGRATION SUB-MISSIONS (TRANSPORTED ASSETS)

5.1 OBJECTIVE OF THE SP4

The high level objective of SP4 was the design and development of in-laboratory proof-of-concept performance prototypes able to demonstrate the feasibility of the protection of **transported assets**.

SP4 was split into four Work Packages, featuring four sub-missions:

- **passenger clearance control**: improved detection of threats (e.g. CBRN-E, hidden object on people, tracking people, abandoned object detection…) and abnormal situations on board or just before boarding;
- **luggage clearance control**: improved detection of threats like explosive devices or other suspicious devices in ordinary baggage to cause immense disruption in mass transportation networks;
- **freight clearance control**: improved detection and discrimination of threats introduced into transported freight;
- **special tunnel and fast tracks security.**

In each sub-mission architecture has been designed in order to integrate (also in different time scale) the necessary protection solutions and handle different technologies coming out from legacy system as well as existing or new generation technologies. In Figure 14 are synthetized all the SP4 work packages and their dependencies.

Figure 14 SP4 WPs and Dependencies

5.2 THE SP4 WPS RESULTS

Here below are reported the in-laboratory proof-of-concept performance prototypes obtained by each SP4 work package for each specific protection solutions:

5.2.1 PASSENGER CLEARANCE CONTROL

The objective of this work package was to design and integrate appropriate technologies for passengers clearance control. This work-package was focused on the detection of threats on-board, before boarding and within the station area.

During the Project the following capacities have been identified and developed:

- For face matching and luggage reconciliation according RFID chip people and luggage are detected and/or recognized simultaneously and the system verifies the coherence between what has been detected and what was registered at the beginning. For example, the owner of a luggage is supposed to still have his luggage (and not the luggage of another person, except when it is someone from the same family).

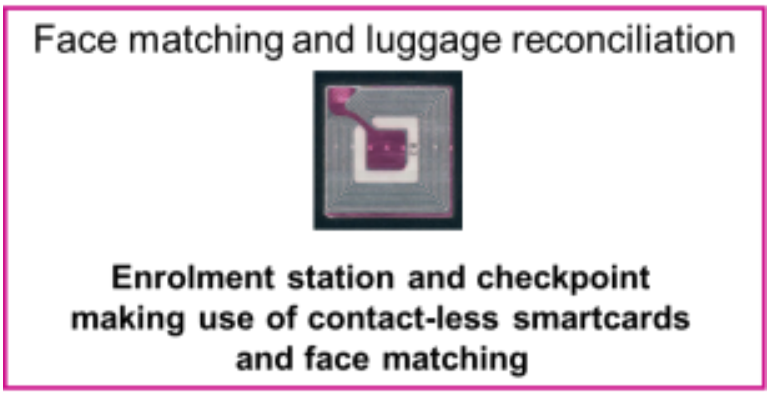


Figure 15 Face Matching and Luggage reconciliation

- The Passenger detection of radioactive agents addresses:
  - The detection of artificial radiation sources using analysis based on gamma spectroscopy. The gamma spectroscopy is done with high efficient scintillation detectors using advanced single nuclide analysis and natural background suppression.
  - The detection of toxic and combustible gases: detection of explosive and toxic gases using semiconductor based gas detectors.
  - The detection of radioactive aerosols: continuous collection of radioactive aerosols on a filter (internal pump) with simultaneous detection of filter activity. Subsequent Alpha spectroscopy for natural Radon background suppression is performed. Radiobiological relevant levels of long-living radio nuclides are detected within one minute.

Figure 16 Detection of Radioactive Sources

- The passenger clearance control covers:
  - Left luggage detection (or abandoned object detection), which monitors a video stream coming from cameras and tries to detect abandoned objects like an unattended luggage. It would also detect removed objects, for example if someone removed a garbage bin.

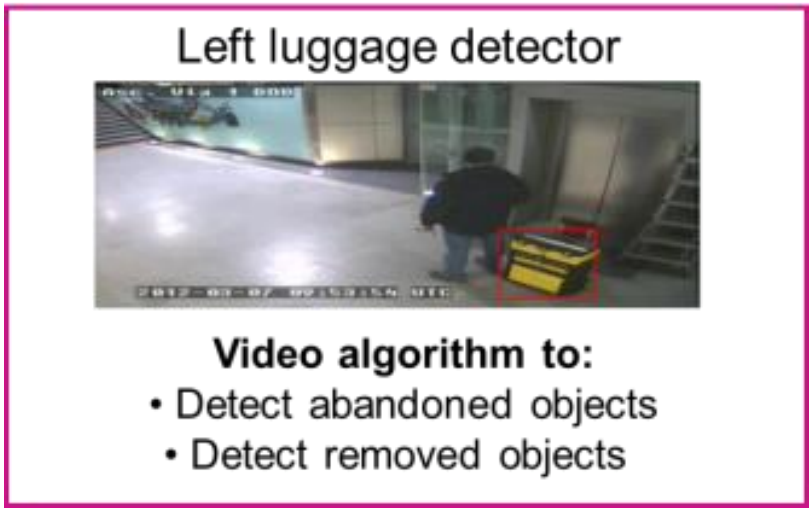


Figure 17 Left Luggage Detector

- People on-board detection, which monitors multiple video streams coming from depot (or other area) cameras and tries to detect when a person is leaving the train through either doors or windows. This capability will detect and report the positions of people in the depot, based on the result from multiple basic algorithms (human detectors, tracking, etc.) running on different video streams. Then automated/semi-automated scenarios will be applied using finite-state-machine reasoning on parameters like time, location, train position, etc., to raise alarms if someone is present in non-authorized areas.

Figure 18 People On-Board Detection

5.2.2 LUGGAGE CLEARANCE CONTROL

The objective of this work package was the research design and integration of appropriate technologies for “on request” luggage clearance control (such as sampling or unattended luggage control). The two main capacities developed are:

- The hand-held Luggage device (detection of explosive gases and toxic gases) which addresses:
  - Detection of radioactive sources: the system is capable to detect artificial radiation sources using analysis based on gamma spectroscopy. The gamma spectroscopy is done with high efficient scintillation detectors using advanced single nuclide analysis and natural background suppression.
  - Detection of toxic and combustible gases: detection of explosive and toxic gases using semiconductor based gas detectors.

- Detection of radioactive aerosols: continuous collection of radioactive aerosols on a filter (internal pump) with simultaneous detection of filter activity. Subsequent Alpha spectroscopy for natural Radon background suppression is performed. Radiobiological relevant levels of long-living radio nuclides are detected within one minute.

- A portable equipment for luggage clearance control which aims to control a suspected luggage by using two detection technologies: the 2D transmission X Ray imaging and 3D neutron imaging which provides a 3D image of the atomic composition. These data are analysed in order to detect the presence or not of threats. The different types of threats are the explosive, the toxic chemical and the radiologic threats.

All these equipment have been installed and successfully demonstrated in Zmigrod.

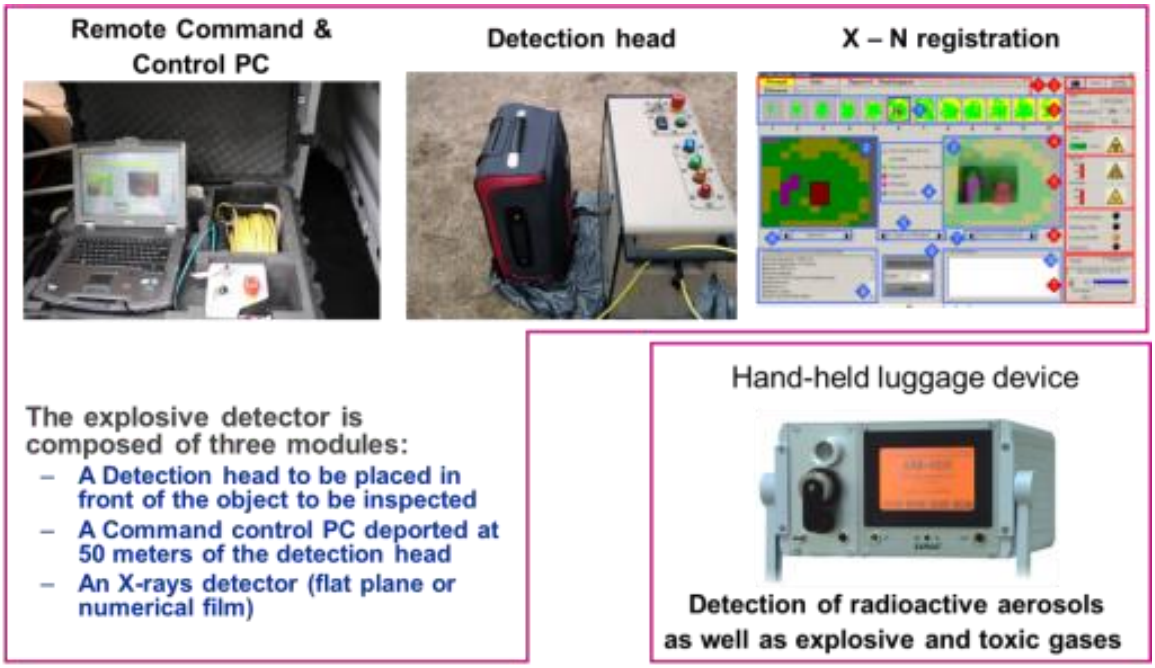


Figure 19 Luggage clearance control

5.2.3 FREIGHT CLEARANCE CONTROL

The objective of this work package was the research, design and integration of appropriate technologies for freight clearance control. The capacities developed are:

- The Freight control (mobile device) which addresses:
  - Detection of radioactive sources: the system is capable to detect artificial radiation sources using analysis based on gamma spectroscopy. The gamma spectroscopy is done with high efficient scintillation detectors using advanced single nuclide analysis and natural background suppression.
  - Detection of toxic and combustible gases: detection of explosive and toxic gases (Cl2,HCN,Ammoniak,Co,Co2,Phoshine)
- The cargo inspection system focused on demonstrating the inspection of transported freight arriving at a railways infrastructure or transported by rail. A freight clearance solution is typically composed of one or more non-intrusive inspection systems and technologies:
  - A Side X-Ray transmission imaging, with an X-Ray emission part and a detection part located to the opposite side of the freight to be inspected.
  - Inspection set of workstations and IT items, allowing to inspect the set of non-intrusive data.

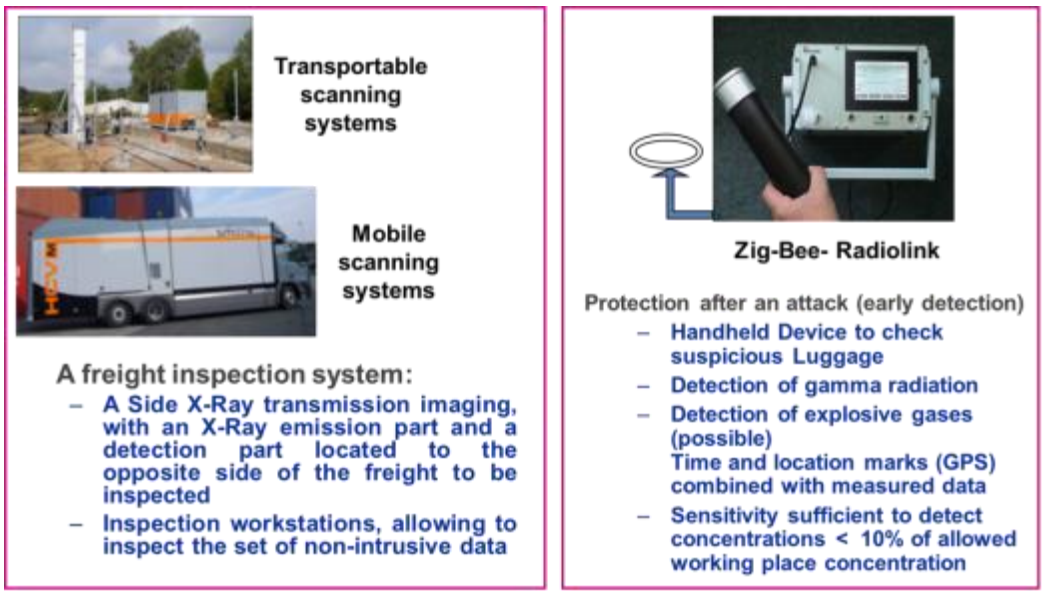


Figure 20 Freight Clearance control

All these equipment have been successfully demonstrated in Zmigrod.

5.2.4 SPECIAL TUNNEL AND FAST TRACKS SECURITY

All the activities of this work package are described and reassumed inside the Demonstration Run in Villecresnes/France section 6.7.

6 SP5 GLOBAL INTEGRATION

6.1 THE PROTECTRAIL INTEGRATION FRAMEWORK

PROTECTRAIL based its interoperability framework on design patterns which are successfully used in other industries. These include the following elements:

- A reusable Service-Oriented Architecture (SOA)
- An **Event-Based Architecture** for data exchange between various security components and decouple the components from each other
- Reusing of well-established and proven **standards** which reduce the non-recurring cost of software integration
- Planning of an **extendable** architecture for the future to extend the framework with upcoming standards
- Building **modular** components with web services
- Supporting **discoverable** components to reduce the configuration effort and improve the reusability
- Building on an **IP network** (cabled or wireless) which is dimensioned to support consistently the **video surveillance streams** necessary to assess, confirm and investigate security incidents

Figure 21 Basics of the interoperability framework

Event-Driven Architecture (EDA) consists of numerous event producers and event consumers from various locations and various stakeholders of public transport operations. Security **sensors and devices** from on-board and wayside (i.e. sensors and devices like CBRNE detectors, intrusion detection, laser scanners and devices like video cameras and recorders, person tracking) send events ranging from basic alerts with limited environmental information to more complicated alerts with various information and resource fields which are vital for a better understanding of the situation on the ground. These sensors and devices are called event producers.

PROTECTRAIL identified the need for a common **Event Format** which includes location (and in all probability the affected area), absolute occurrence time (in UTC), a unique event identifier and type, attached resources as well as source and contact information. PROTECTRAIL chose the Common Alerting Protocol (CAP) of OASIS as the best existing standard for the public transport sector. The OASIS specifications define a data model for a wide range of applications like safety, security, health, weather and environmental threats, telecommunication and cyber security. PROTECTRAIL adopted the XML Schema representation of CAP to implement the event providers and consumers based on that standard. The proposed event format inherited the following CAP standard features:

- Multi-operational and multilingual messages

- Three dimensional and flexible geographic description
- Message update and cancellation
- Links to further information such as images, reports and videos.

Today CAP is used extensively for weather and earthquake warnings in public and commercial Emergency Alert Systems like Google Public Alerts; it remains to be endorsed by the international security standards.

Interoperability relies on both, a common data model and shared representation. **Shared representation** is important for all stakeholders to collaborate based on the same information assets. It starts with the same wording, shared facility information and ends in common geographical maps.

For a reliable message interchange, PROTECTRAIL recommends the implementation of the **Event Broker** as key element in the interoperability framework. PROTECTRAIL used the Eventing Framework specification **WS-Notification** which can contain any type of XML data format. A **Message Server** manages all incoming and outgoing messages and can deliver and handle high performance, clustering, transactions and a wide range of cross-language clients and protocols. If an event consumer is not available the message server can store undelivered messages and retry delivery out of a message queue. The PROTECTRAIL implementation of the event broker was based on the most popular open source message server, called Apache ActiveMQ, and supported three different data structures for events, namely the **Common Alerting Protocol** (CAP), a project specific resource and the ONVIF format.

In future, new event frameworks and data structures can be **easily extended**. This is normally done by adding new web service endpoints. Endpoints are unique URL's for providing public accessible and reusable Web Services which can be used for service composition and orchestration.

The role of the **Security Command and Control Centre (SOCC)** is to ingest and correlate various event sources into a single platform and thus improves the situational awareness among those persons that need to work with the information, for instance security operators or first responders. Several SOCC's can share a situation and cooperate. Typically such a system visualises the events in a GIS map and shows related video cameras, recorded videos and it provides operational and security related procedures. Simple events can be correlated to a major incident which means that the event contains additional information on for instance a responsible person, severity, certainty, and urgency. The SOCC system helps the operator in his daily work to suppress nuisance alarms, to group similar alarms, and to relate the event with other information and sensors. The SOCC guides the operator through a stressful situation through electronic Standard Operational Procedures (eSOP). These procedures are programmed today but can be executed as a graphical business process in the future. To allow for a continuous improvement of the eSOPs during operation, the decisions and actions of the operator can be recorded. With such a system the operator can be trained with simulated operational situations.

A **Crisis Management System (CMS)** is a solution to manage a crisis with various responders and any class of requested stakeholders. A CMS has to handle multiple operators, transportation modes and locations. A crisis manager has to act and make decisions based on all available real time information. This information can come from external experts and external media types like news feeds, live and recorded, as well as fixed and mobile video that need to be integrated. As situations evolve, hand-over from CMS to CMS may prove to be necessary.

In PROTECTRAIL the information abstracted from the events was standardised, processed and eventually disseminated by the SOCC and the CMS to passengers and other relevant stakeholders using various sources like **Passenger Information Displays and Announcement Systems**.

Figure 22 Participants in a global security context

PROTECTRAIL is only at the beginning of a process which will require further standardisation, but the proposed interoperability scheme is prepared to integrate upcoming standards which have been identified, such as: for investigations ISO22311, for IP-based security products like ONVIF Profile S (a subset of IEC 62676), or IEC 62580-1 for on-board embedded devices based on DPWS.

6.2 DEMONSTRATION RUN IN ZMIGROD/POLAND

6.2.1 DEMO SITE CHARACTERISTICS

The demo site selected for the PROTECTRAIL demo is a “test track” owned and managed by the Instytut Kolejnictwa nearest the city of Żmigród. The area is in the Trzebnica County in the south-western Poland and it lies approximately 22 kilometres north-west of Trzebnica, and 40 kilometres north of the regional capital Wroclaw. In the area there were the following assets to be used for the demo:

- Main buildings:
  - reception and offices;
  - control tower;
  - meeting and conference room (40 persons);
  - lodging service;
- Electric substation;
- Approximately 8 km of electrified tracks;
- Link with the Zmigrod railway station (3 km);
- viaducts and a footbridge;
- Freight wagons and 2 passengers’ wagons.

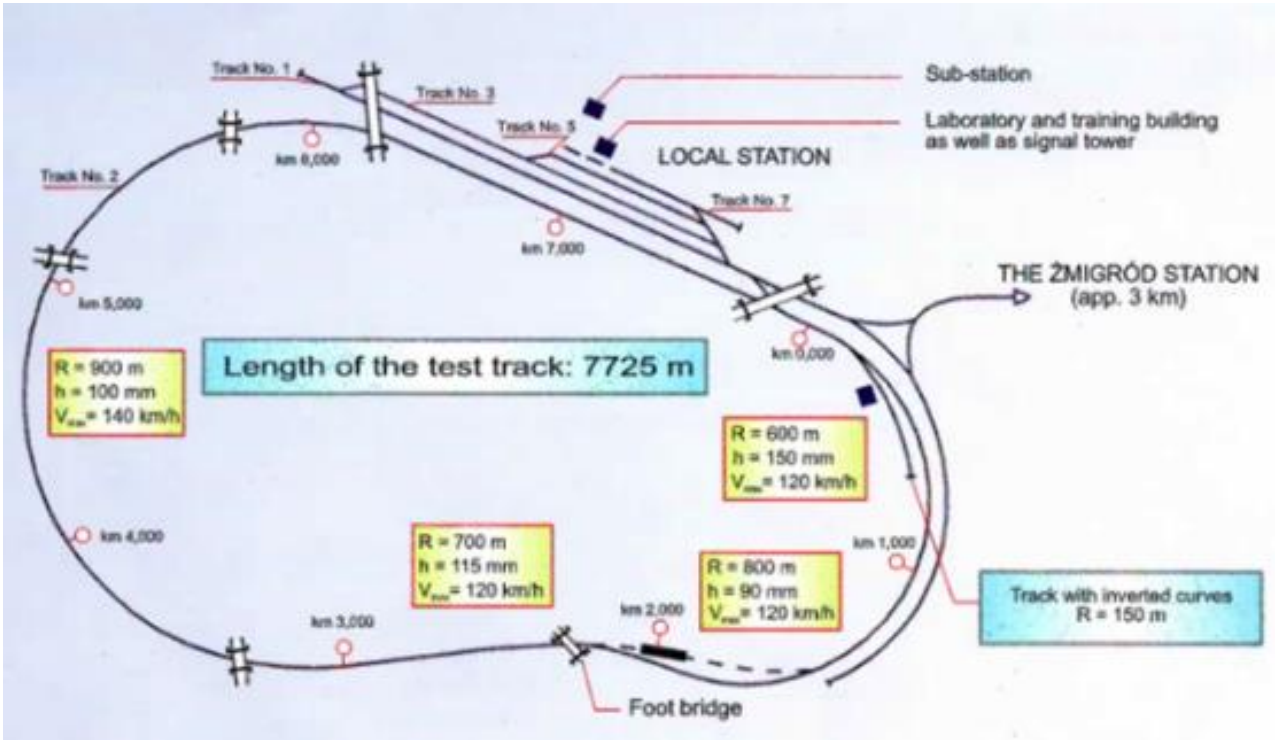


Figure 23: The Zmigrod test track

6.3 ON-BOARD AND WAY-SIDE EQUIPMENT INSTALLATION

6.3.1 THE VIDEO MONITORING SYSTEM

The following cameras have been installed wayside (Figure 24):

- 4x outdoor cameras for intrusion detection
- 1x outdoor Thermal camera for intrusion detection
- 1x outdoor High Definition PTZ camera for intrusion detection
- 1x indoor camera installed inside the passenger alert system
- 1x outdoor camera on the platform
- 1x outdoor camera on the level crossing
- 5x outdoor cameras installed for the people tracking algorithm

The following cameras have been installed wayside (Figure 25):

- 10x on-board cameras inside the 2 wagons
- 1x front-looking cameras on the locomotive

Figure 24 Wayside video monitoring system

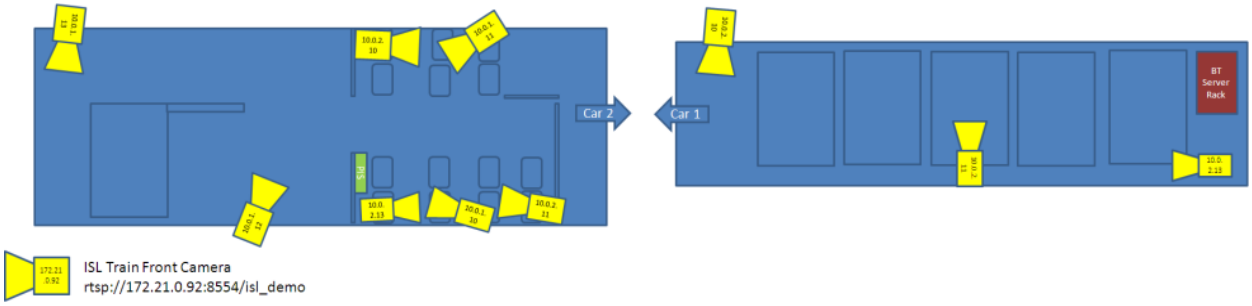


Figure 25 On-board video monitoring system

6.3.2 THE PLATFORM

In order to allow participants of PROTECTRAIL demo to discover all the state-of-the-art security solutions in real operational conditions a platform was built near the test track number 2. On the platform the following devices provided have been installed: emergency communication system which consists of camera and SOS column.

Additionally the passenger information system has been mounted on the platform. Those devices were used for person tracking in the suspect left luggage context.

Figure 26 The Platform Construction

Figure 27 The platform at the end of the construction works

Figure 28: The PROTECTRAIL platform

6.3.3 THE CONTAINER

For PROTECTRAIL partners' needs, it has been provided three steel containers, each measuring 6m x 2m. These containers were combined giving the area of 36 m^2. The final container acts as a Control Command Centre and is shown in Figure 29 and Figure 30. It is equipped with windows, door, air conditioners, cupboards, swivel chairs and tables. In the container a lot of devices and equipment of PROTECTRAIL partners have been installed.

Figure 29 External Container View

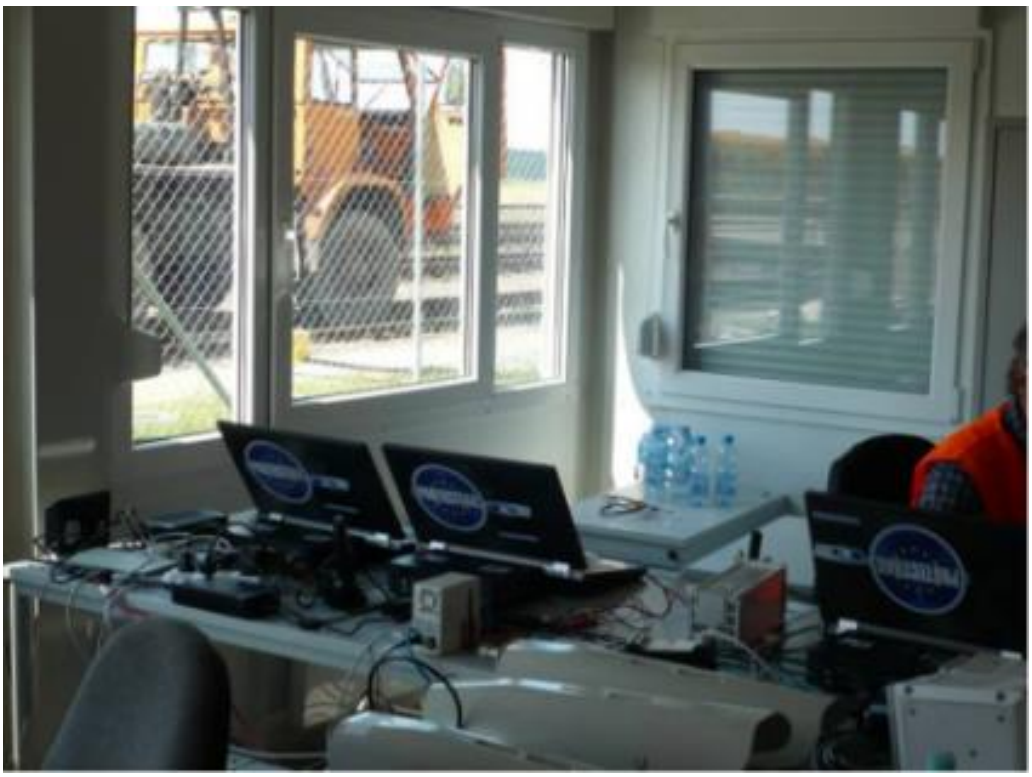


Figure 30 Internal Container View

6.3.4 THE GANTRY

Within the PROTECTRAIL project, additional gantry was installed over the traction on the track number 7. The gantry was set on steel pots with 8,6 m height and was used in order to attach the sensors and cameras to it. On the gantry has been also installed the system for check the clearance gauge of every train passing through the gantry using lasers and cameras. This system includes sensors on gantry and intelligent components inside the shelter near the gantry.

The acquisition system includes 3 kinds of sensors:

- lasers
- ultrasound sensor
- cameras (without lighting system)

Laser sensors are used to check the clearance gauge of passing trains (3 pairs of sensors installed on the gantry) and also to detect train arrival on both sides of the gantry (2 pairs of sensors installed wayside, front and back of the gantry). Every laser sensor is composed of one emitter and one receiver; those two parts of the same sensor are perfectly aligned in order to work properly.

An ultrasonic sensor was installed on the gantry in order to detect all entrance of people when the track is free of train. There are 4 identical cameras installed on the gantry.Three of these camera will positionned in order to face perfectly the left, right and top clearance gauge. The last camera will be use to provide a global view of the train from one side of the track.

Figure 31 The Gantry

6.3.5 THE FENCE

For the Zmigrod Demo it has been built a fence in order to detect people crossing boundaries. The fence has 58 m length and is placed along track number 7. It consists of wire mesh, posts and a wicket. At the end of the fence a mast has been installed to which a CCTV camera is attached. The electronic sensors have been installed on the fence for intrusion protection.

Figure 32 The installed Fence

6.3.6 LOCO AND CARS

The real scale security test of PROTECTRAIL project required the use of loco and cars. The loco and two cars were rented from Polish rail transporter PKP Intercity S.A. One of the cars was free space, second one with compartments. One of the rented cars was not in commercial use any longer and required thorough renovation. The renovation works included:

- electrical system
- lighting installation
- painting of walls, windows, ceilings and door
- insertion of partitioning wall
- installation of seats
- removal of old lamps
- elimination of unnecessary holes
- radiators enclosing

In the car the following devices have been installed: on-board CBRNE detector for intrusion detection, on-board smoke sensors, driver cabin access control system and face checking system , on-board people detection system for intrusion detection, on-board radio nuclear detectors, Passenger Information System and on-board network video recorder. The on board to on ground communication has been realized by using the on-board control unit. Electrical power in the cars was supplied from the power supply installation (when the cars parked) or from the diesel generator installed outside the car (when the cars were moved).

Figure 33 The PROTECTRAIL Loco

Figure 34 The PROTECTRAIL Cars

6.3.7 THE ZMIGROD ARCHITECTURE

The complexity of Zmigrod network architecture is shown in Figure 35.

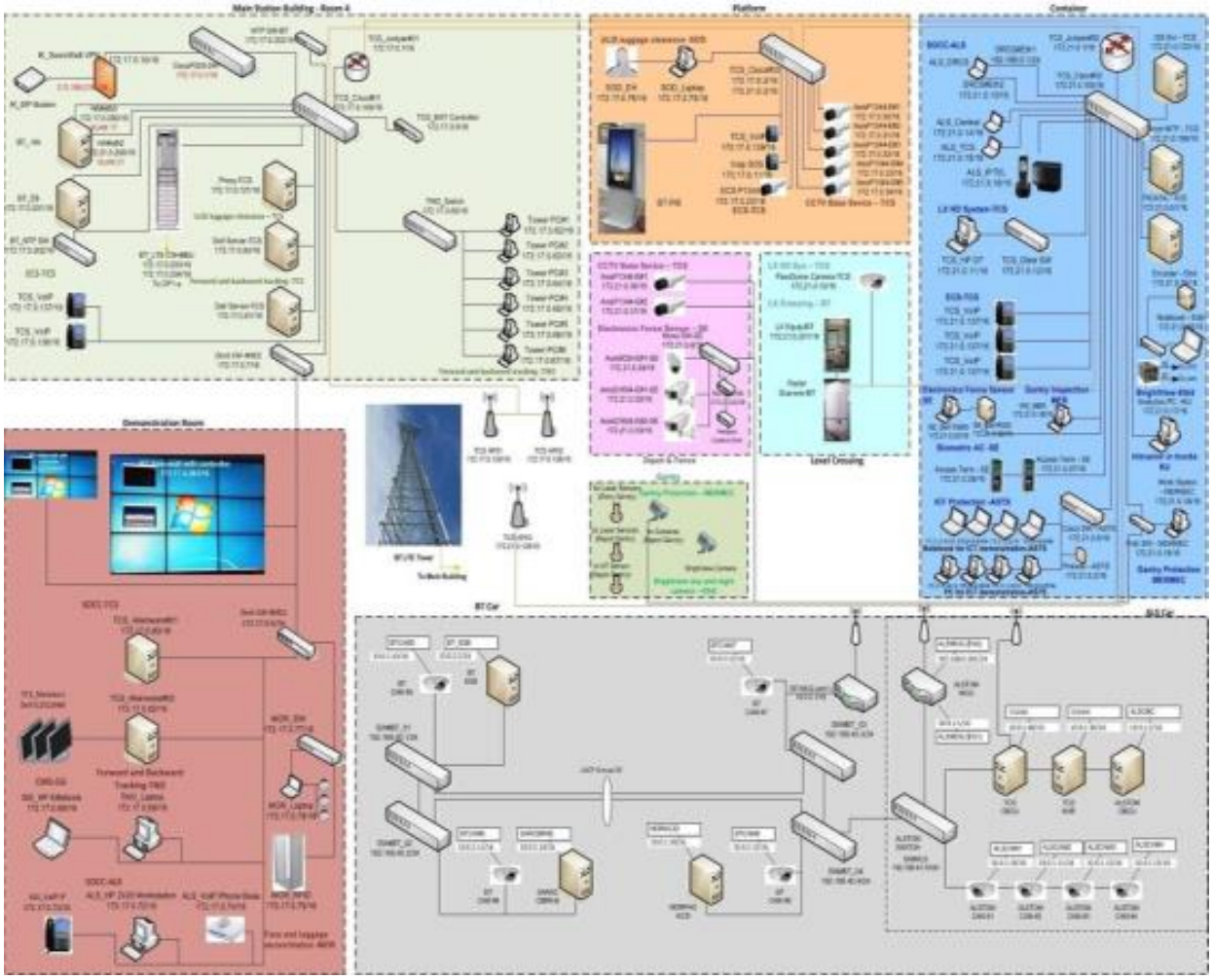


Figure 35 Overall Zmigrod Network Architecture diagram

6.3.8 SCENARIO DESCRIPTION

To prepare the demonstration in Zmigrod SP5 members needed to bring lab tested capacities defined in SP3 and SP4 into valid scenarios The SP5 members brought the existing security solutions defined in SP2 in a valid order and grouped them in realistic scenarios. The PROTECTRAIL members set up the main scenarios CBRNE on platform, intrusion detection, CBRNE on-board and CBRNE on freight trains. The leader of each scenario was the responsible Crisis Management System (CMS) and Security Operational & Control Centre (SOCC) provider.

The PROTECTRAIL members modelled the scenarios as BPMN 2.0. Business Process Modeling Notation representing processes of an enterprise, so the existing processes may be analyzed and improved by other professionals. The model consists on following elements:

- **Swimming lanes** represent responsibilities and locations like Security Operation & Control Centre, Crisis Management, onboard, platform, public authorities. The naming shall be homogeneous through all modeled processes.
- One **Start Node** represents a unique identified system event. Starting from a single start node, the process can be branched out with **Gateways** symbols.
- **Activities** represent different types of actions. It can be messages between systems, manual instructions, human interaction, execute a program.

- In general a process can have many **End Nodes**.

6.3.8.1 SCENARIO 1: PERSON TRACKING IN SUSPECT LEFT LUGGAGE CONTEXT

6.3.8.1.1 Start, detection and confirmation

- A luggage is left on the platform
- The luggage is detected **on the platform** as potentially abandoned by a person (passenger, visitor, staff)
- The person presses the help button and informs the operator through an Emergency Communication System (ECS)
  - an event is sent to the railway SOCC with spatial information
  - the 2-way communication between operator and the person as video and audio is recorded for future forensic activities
- The operator tries to understand if the luggage was really left unattended by someone by observing the related video cameras.
- The SOCC send out a message to the Passenger Information System (PIS) don't leave the luggage on the PIS on the platform

6.3.8.1.2 Suspect Tracking

- The SOCC operator identifies the suspect that has abandoned the luggage with the following actions
  1. operator start the workstation for the person tracking in the recorded video
     .1.1. manual backtrack to the moment the person drop the luggage
     .1.2. mark the person in the tracking solution
     .1.3. start the person tracking in the recorded video
     .1.4. The person tracking solution will send out an event for person tracking started.
     .1.5. If the person detected in another camera tracking solution will send out an update event.
     .1.6. If the end of the recorded video is reached tracking solution will send an event to SOCC with all available information (GPS position of the camera, camera ID, position of the person, time)
  2. The person leaves the area with the train.
  3. The on-board and the wayside camera record the videos for the investigation use case in scenario 3.
  4. SOCC passes the control to CMS through a decision making event (i.e. an event specific to start the CMS) with all the links to the required information (involved events, related CCTV links, geo-location/location of the event, etc.) that the CMS shall use to start the procedure.
  5. While the containment team neutralises the luggage, the SOCC operator follows the perpetrator on board using live CCTV video streams (no tracking on-board) through LTE and WiFi wireless connections and understands in which station the perpetrator has left the train and informs the authorities.

6.3.8.1.3 Containment and management (under CMS control)

- The following happens at this point under the control of CMS:
  2. An event containing a message for the Wayside Passenger Information System is sent, by the CMS, to inform people about the best procedure to adopt to evacuate the dangerous area
  3. The CBRNE Containment Team is sent on site
  4. The CBRNE Containment Team communicates with the CMS through the CMS handheld device connected via WiFi of the platform

5. The CMS handheld device (CMSHD) is discovered dynamically by the CMS and is used for communications btw. the team and the CMS. CMSHD can act also as additional camera on site If the luggage is hidden from CCTV, the team can use the CMSHD as a mobile camera connected via WiFi to allow situational awareness. The real-time video stream is used by CMS exploiting the RTSP URL in order to observe the scenery.
6. In order to increase the situational awareness of the situation and adopt the correct procedure to face a possible threat, the CMS needs some help from mobile devices on site to obtain information - radioactive material and explosive mobile detectors are discovered dynamically by the CMS
7. If there is a real threat due to the luggage content
   .7.1. the CMS manager starts the containment procedure by identifying and performing the correct steps needed to tackle the situation
   .7.2. CMS manager checks if the procedure is correctly applied and ticks completed events using a workflow manager
   .7.3. if a radioactive threat is detected, it is shown on the map.
   .7.4. if the luggage contains explosive material, the CMS manager starts the CBRNE consequences analysis tool. CMS shows on the map the result of CBRNE consequences analysis tool to represent and evaluate on the map, the potential consequences of a possible explosion on the surrounding environment (i.e. to evaluate if the potential risk goes beyond what procedures prescribe).
   .7.5. based on the output of the CBRNE consequences analysis result or on a possible radioactive detection, a decision can be made to start further actions not formalised in procedures (e.g. to evacuate a nearby village that may be involved by the explosion of the luggage content)
8. the process is stopped

6.3.8.1.4 Forward tracking when the suspect arrives in another station

- The SOCC operator, supports the police trying to catch the suspect by tracking him with the support of the Person Tracking solution
- The operator follows the person in the map view of the SOCC the whole time and follow the person on the related camera
- The operator continuously informs the authorities via phone

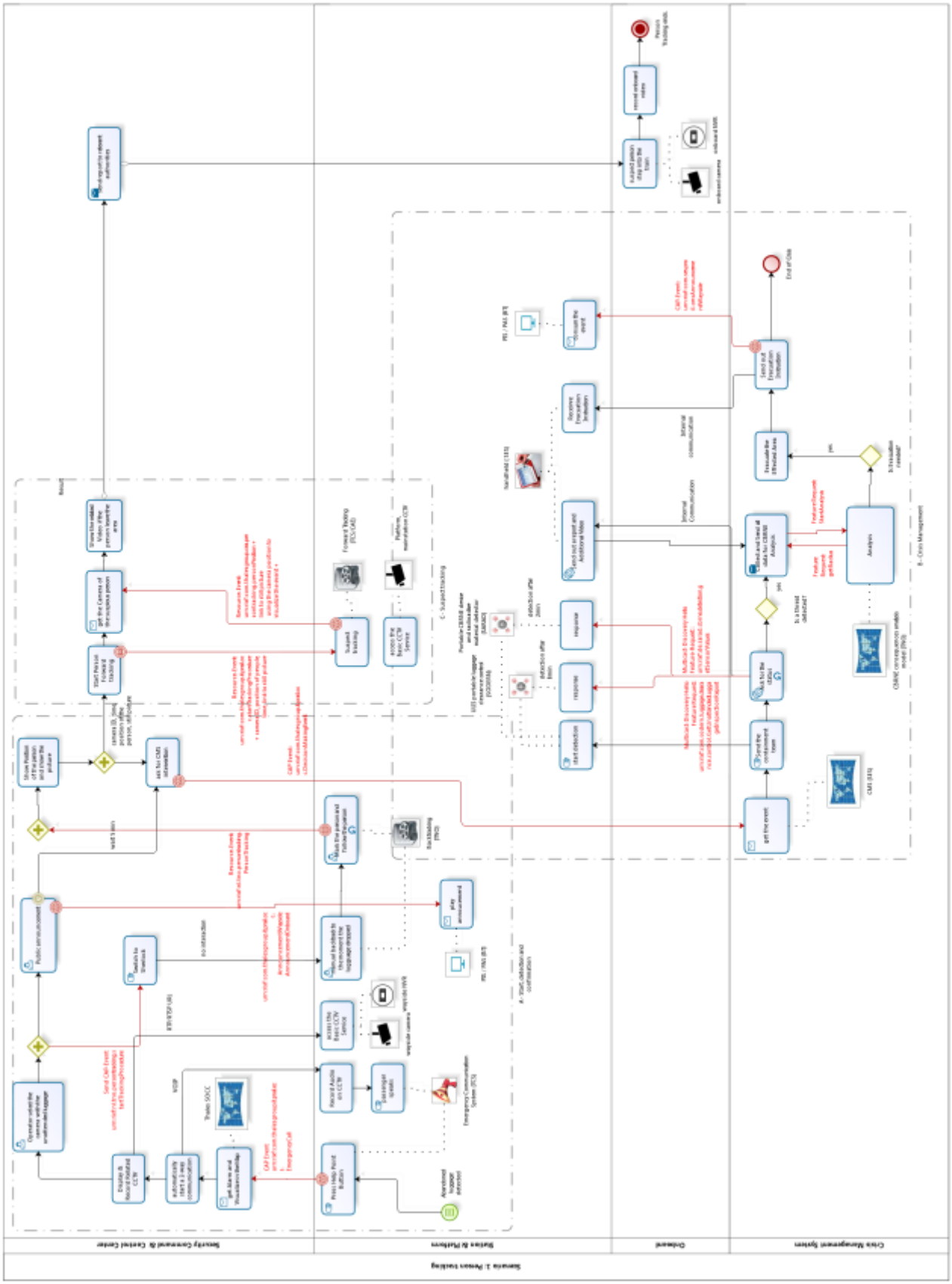


Figure 36 Scenario 1 - Station platform CBRNE detection and Person Tracking video analytic

6.3.8.2 SCRIPT OF SCENARIO 2.1.1 - PLACEMENT OF AN EXPLOSIVE IN PARKED CAR AT DEPOT

1. A suspect person enters the depot, crossing the wayside train clearance system
   1.1. An intrusion alarm is raised at the SOCC supervisor level
   1.2. The SOCC operator requests for a still picture of the intrusion (wayside train clearance system)
   1.3. The SOCC operator sends a security roving staff on site towards the wayside train clearance system
2. The intruder then walks in the depot and enters a car of a parked train:
   2.1. An door intrusion alarm is raised at the SOCC supervisor level
   2.2. The event is confirmed by the People Detection On-board Intrusion Detection System and/or by On-board movement sensor that detects that someone is entering a supposedly empty area (the area around the doors of the parked train)
   2.3. The SOCC operator requests for the on-board video stream
   2.4. The SOCC operator contacts the security roving staff and informs the team of the intruder location
3. The intruder moves in the car:
   3.1. An on-board movement intrusion alarm is raised at the SOCC supervisor level (both People Detection On-board Intrusion Detection System and On-board movement sensor detect it)
   3.2. The SOCC operator requests for the on-board video stream
   3.3. The SOCC operator contacts the security roving staff and informs the team of the intruder movement direction
4. The intruder hides an improvised explosive device (or put fire inside) in the car:
   4.1. An CBRN-E (or fire alarm) alarm is raised at the SOCC supervisor level
   4.2. The SOCC operator contacts the security roving staff and engages the explosive emergency procedure

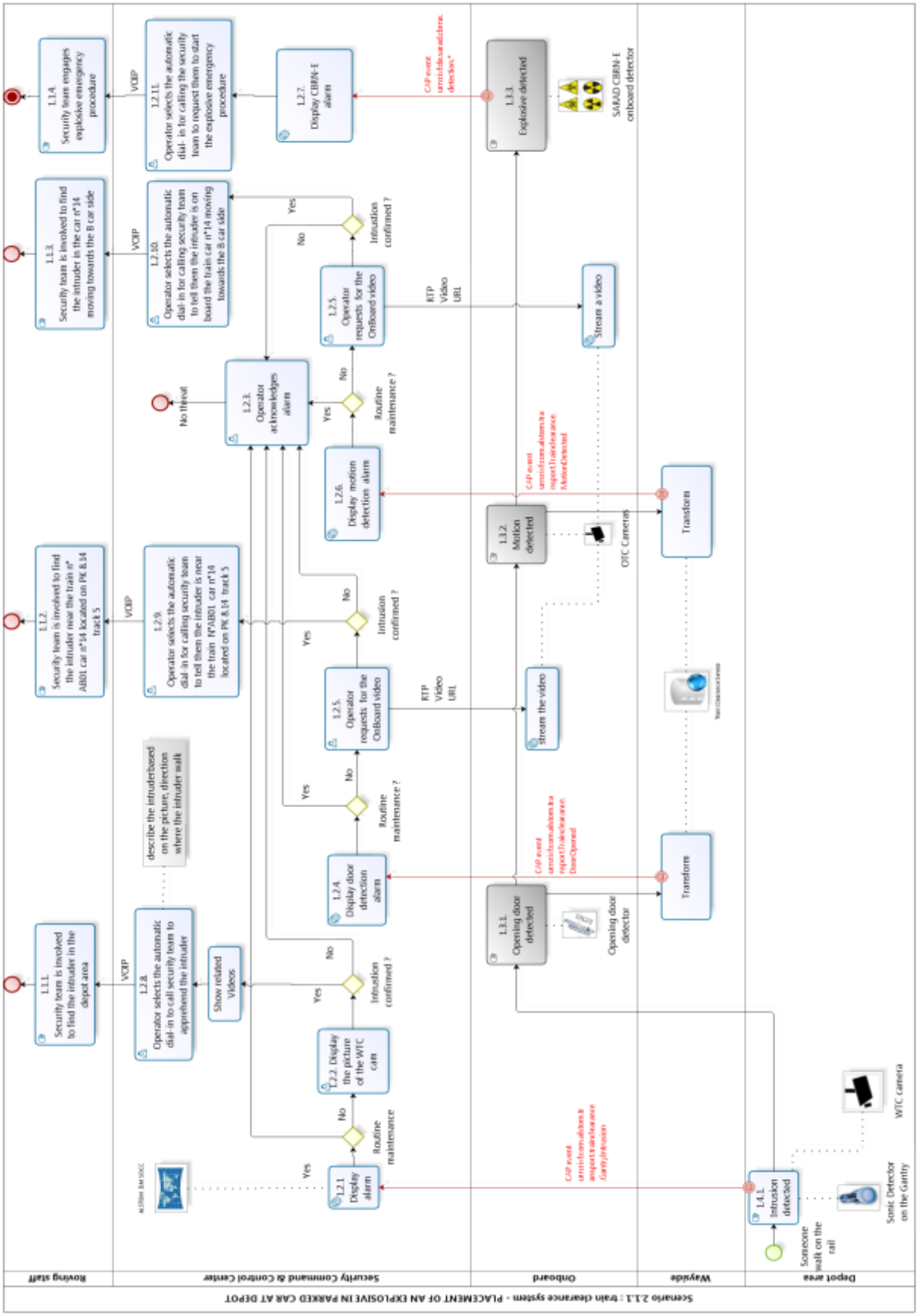


Figure 37 Scenario 2.1.1 - Placement of an explosive in parked car at depot

6.3.8.3 SCRIPT OF SCENARIO 2.1.2

1. A suspect person is hidden inside a car of a train entering the depot. The intruder is not detected at the wayside train clearance system.
2. After a few minutes, the intruder finally moves in the car in order to install himself in a more comfortable way:
   - 2.1. The suspect movement is detected on-board (both People Detection On-board Intrusion Detection System and On-board movement sensor detect it)
   - 2.2. An on-board movement intrusion alarm is raised at the SOCC supervisor level
   - 2.3. The SOCC operator requests for the on-board video stream
   - 2.4. The SOCC operator contacts the security roving staff and informs the team of the intruder location
3. The intruder starts a fire to stay warm with a device he brought within the bag he came with:
   - 3.1. Smoke is detected by on-board smoke detector
   - 3.2. A smoke alarm is raised at the SOCC supervisor level and
     - 3.2.1. the Train Clearance System generates a complex event using a decision matrix in order to combine the consecutive events (intrusion alarm + smoke alarm) representing a potential arson alarm
     - 3.2.2. the SOCC consumes the complex event to inform the operator that the CMS has been notified of the potential arson threat (the OASIS CAP alert message would reference the two aforementioned prior events).
     - 3.2.3. the CMS consumes the complex event, visualizes the event on the map and the on-board cameras on the videos list giving the possibility to the CMS manager to analysing the on-board streaming videos for improving the situation awareness on the basis of the received information and on the videos provided, the operator at the CMS decides that the event was linked to an homeless intrusion not requiring the intervention of the crisis management teams
     - 3.2.4. the CMS operator contacts the SOCC operator by phone to confirm that for the CMS level there is no problem and the scenario is closed
     - 3.2.5. this part of the scenario ends
   - 3.3. The SOCC operator contacts the security roving staff and informs the team of the smoke detection
4. The intruder sees the security team approaching the car through the window. He decides to exit the car and runs in the depot and escapes the security team:
   - 4.1. A door intrusion alarm is raised at the SOCC supervisor level
   - 4.2. The event is confirmed by the People Detection On-board Intrusion Detection System and/or On-board movement sensor that detect that someone is exiting from the window of the train
   - 4.3. The SOCC operator contacts the security roving staff and informs the team of the intruder movement and directions
5. The intruder exits the depot through the wayside train clearance system and escapes, and additional alarm is sent to the SOCC
6. The SOCC, given the sequence of events and the security team report on the train, concludes the intruder was a homeless person who tried to stay in the car overnight and that it was not a terrorist.

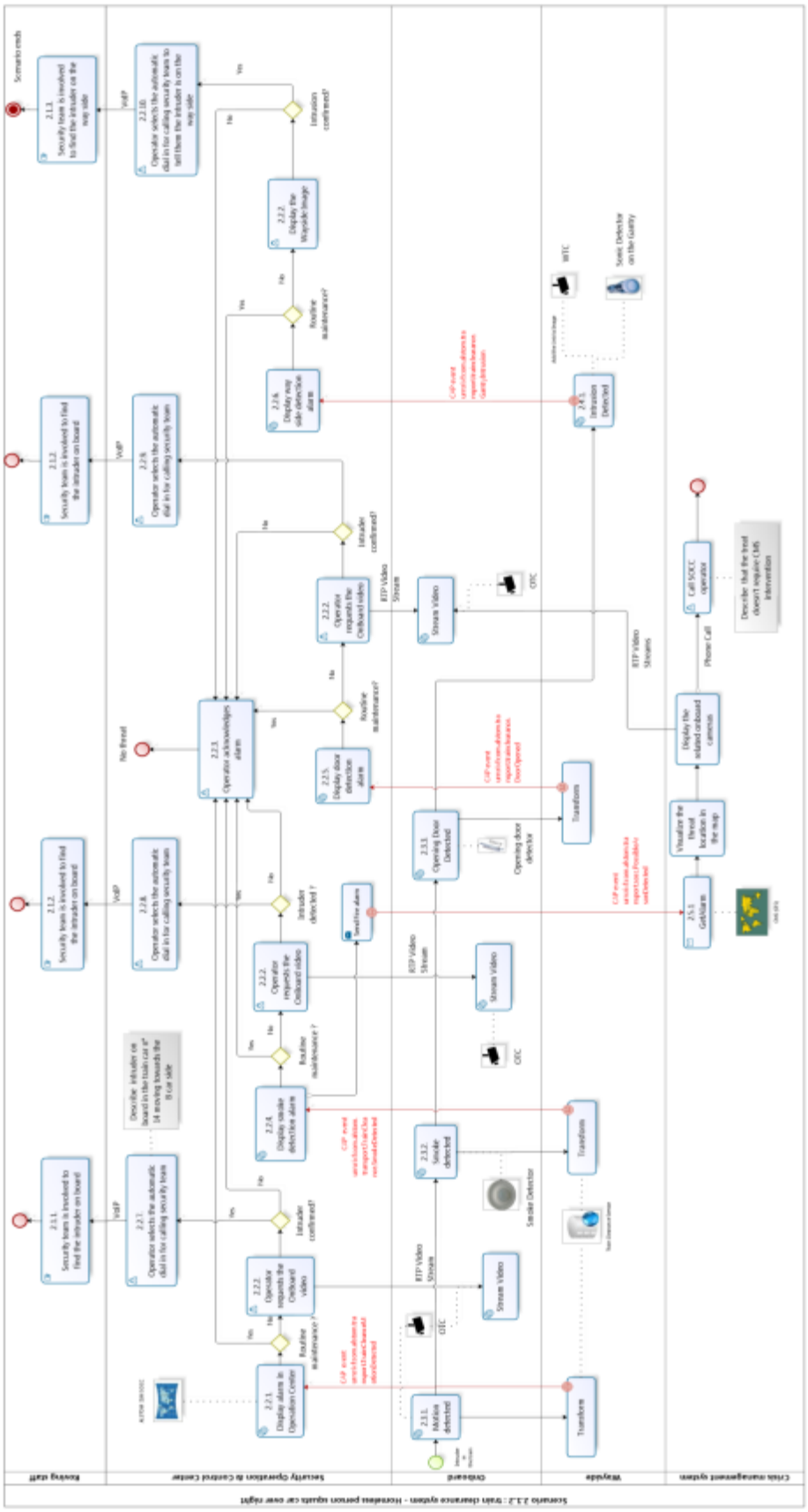


Figure 38 Scenario 2.1.2 train clearance system - Homeless person squats over night

6.3.8.4 SCRIPT OF SCENARIO 2.1.3 - TRAIN SYSTEMS CLEARANCE - HIJACKING OF TRAIN

1. An intruder enters the depot clinging to the exterior of a train as it enters the wayside train clearance system:
   1.1. An intrusion alarm is raised at the SOCC supervisor level
   1.2. The SOCC operator requests for a still picture of the intrusion (wayside train clearance system)
   1.3. The SOCC operator sends a security roving staff on site towards the wayside train clearance system
2. After the train stops, the intruder walks to a locomotive and enters in the driving cabin using an employee key
3. The intruder uses the biometric access control system to take control of the locomotive:
   3.1. An intrusion alarm is raised at the SOCC supervisor level, the intruder appears to be an ex-employee recently laid off
   3.2. The SOCC operator informs the security team of the location of the intruder and calls the police
4. The on-board face recognition system detects a not authorised person intrusion:
   4.1. An intrusion alarm is raised at the SOCC supervisor level
   4.2. The SOCC operator requests for a still picture of the intruder

- The Police, arriving on site, arrest the intruder. The police conclude that the intention of the driver was to take control of the train in order to cause a collision. The ex-driver motivation for this action was that he was unhappy because he was laid off.

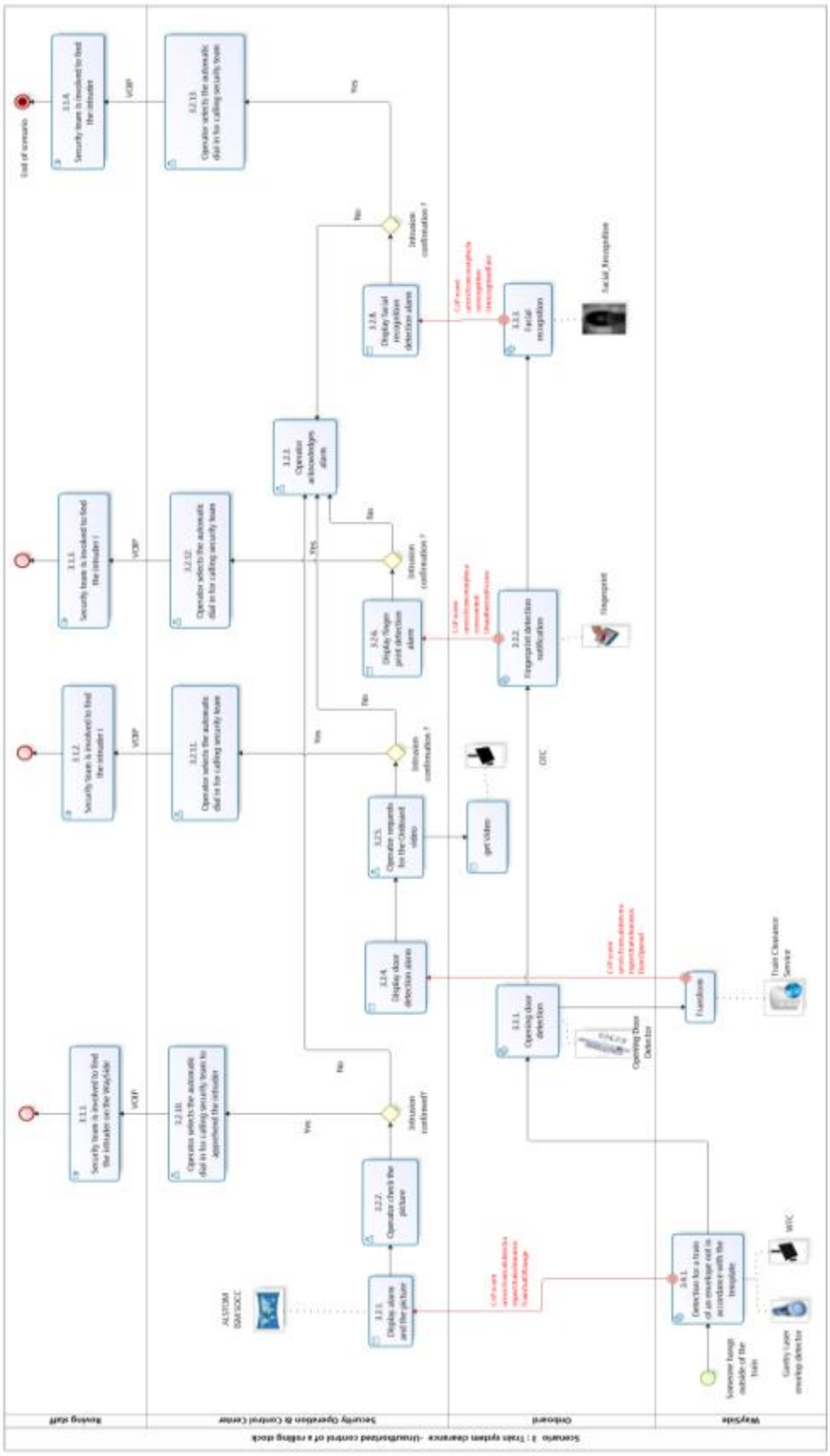


Figure 39 Scenario 2.1.3 Train Systems clearance - Hijacking of Train

6.3.8.5 SCRIPT OF SCENARIO 2.2 - LEVEL CROSSING AND INTRUSION DETECTION

1. A person arrives by vehicle (car, van, etc.) to the place and approaches level crossing
   1.1. the person leaves deliberately the vehicle in the middle of level crossing area to generate an accident with an approaching train as a diversion
   1.2. the level crossing protection system generates an alarm and the SOCC operator observes and record the scene in HD mode
   1.3. The operator send the driver the stop instruction via Operator Wireless Communicator
   1.4. the person goes towards the fenced area and leaves the FOV of HD camera
   1.5.
2. The person trigger 4 intrusion alarms:
   2.1. The day camera detect someone step in the area far from fence
   2.2. The video analytics detects an intrusion near the fence
   2.3. The fence detector detects if the intruder climb over the fence and force a door in the fence.
   2.4. The video analytics detects the intrusion in the depot area.
3. The SOCC operator get the 4 alarms with camera URLs and follows the intruder on video
4. The intruder tries to enter the container room by forcing the door. A room intrusion alarm is sent to SOCC and SOCC operator confirms by video the intrusion and decides to send a staff person to check what's going on.
5. The intruder tries to access via password and type in a wrong pass code. A access deny alarm will send to the SOCC.
6. The intruder tries to open the rack door by forcing the electromechanical lock with the idea of disabling signalling trying to cause interruptions
7. A rack intrusion alarm is sent to SOCC
8. The intruder discover that the seal is broken and closes immediately the door and tries to vandalise the rack by breaking the rack back panel
9. Also a tampering alarm is sent to SOCC
10. The SOCC operator update the security guard about the current situation
11. The intruder connects his notebook to the server. The ICT protection sends an alarm for unauthorized device to the SOCC.
12. The intruder starts a scan in the network. The ICT protection sends an alarm for Cyber Attack to the SOCC.
13. The Security guard catch the intruder in the container.

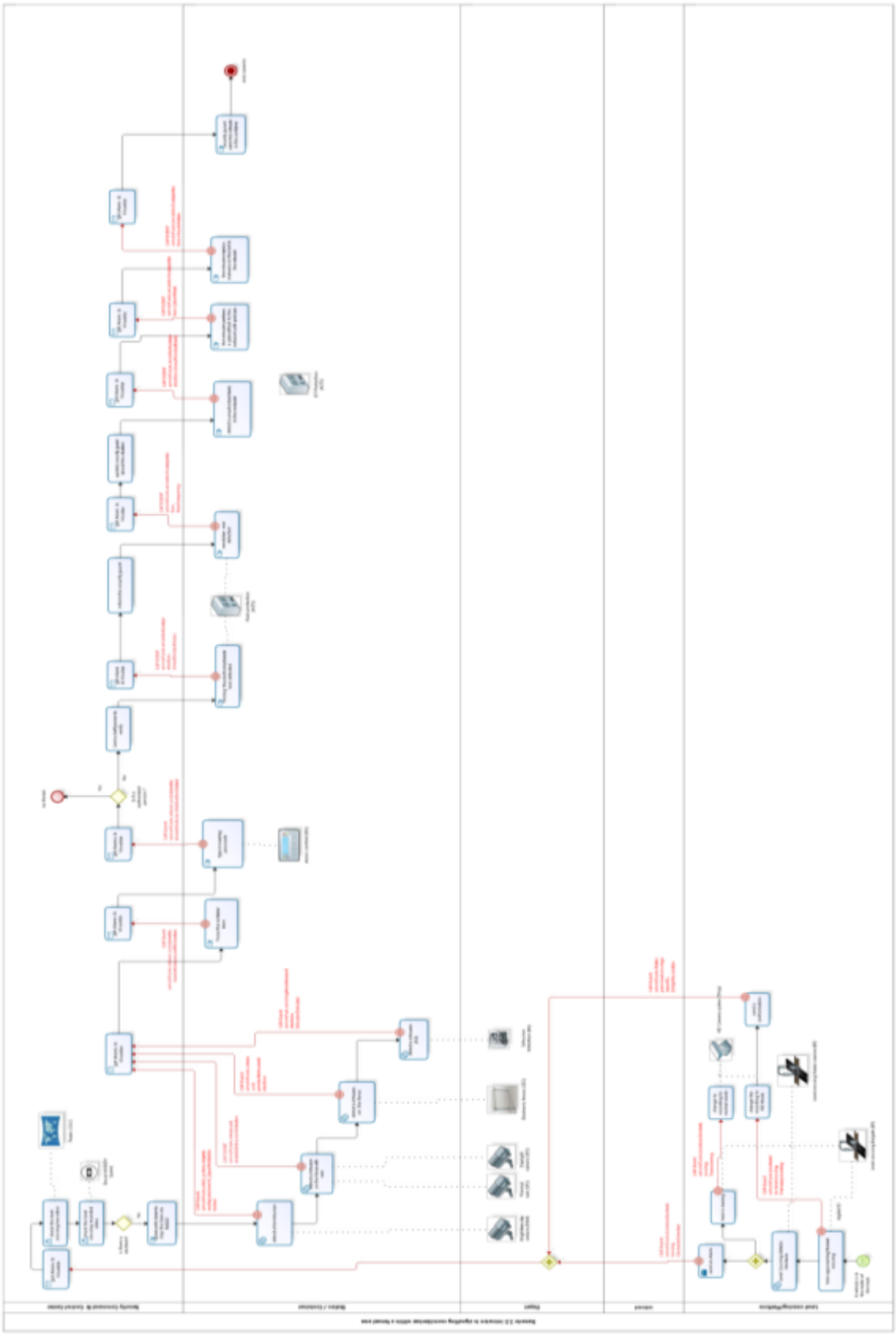


Figure 40 Scenario 2.2 - Level Crossing and Intrusion Detection

6.3.8.6 SCRIPT OF SCENARIO 3 - LUGGAGE RECONCILIATION, CBRNE DETECTION ON-BOARD AND INVESTIGATION

1. A perpetrator passes the RFID-Gate at main station with a luggage and then enters a train car
2. The perpetrator leaves the train without the luggage
3. The perpetrator passes through the RFID-Gate on the main station without luggage
4. The people and luggage reconciliation capacity detects this event and generates a precursor of the CBRN-E event
5. The SOCC receives the event from the gate and show related CCTV
6. The SOCC operator creates a report with the image of the suspect person and send it to the police via email.
7. After a while the CBRNE detector detects a radioactive Aerosol on-board and send an alarm.
8. The SOCC operator escalate the situation to the Crisis Management System
9. If the event contains info from radiation detection on-board device that can be considered a threat, CMS manager starts performing the planned steps needed to face the emergency.
    - 9.1. step-by-step instructions are displayed to CMS personnel. CMS manager checks if the procedure is correctly applied and ticks completed events using a workflow manager, in particular:
        - 9.1.1. Show the threat position and the train position on CMS map
        - 9.1.2. An event containing a message for the on-board Passenger Information System (PIS) is sent, by the CMS, to inform people about the procedure to adopt to face the situation
        - 9.1.3. CMS connects to the ERICARD (the CEFIC Emergency Response Intervention Cards http://www.ericards.net/) that provides guidance on initial actions for rescue teams when a chemical and/or radiological transport accident occurs. CMS manager insert into the ERICARD HCI the radioactive substance detected by radiation detection on-board device
        - 9.1.4. CMS sends to the Rescue staff, by means of CMSHD, guidance on initial actions provided by ERICARD
        - 9.1.5. The CMS manager chooses a safe location where to stop the train and pre-positions the rescue staff to it
        - 9.1.6. The rescue staff reaches the train and switches on the CMS handheld device
        - 9.1.7. The CMS handheld device (CMSHD) is discovered dynamically by the CMS and is used for communications btw. the rescue staff and the CMS. CMSHD can act also as additional camera on site to improve the situation awareness (people symptoms and conditions)
        - 9.1.8. CMS shows videos from on-board cabin and from CMSHD
        - 9.1.9. Rescue staff carries out the adopted procedure
10. In parallel train manager follow the on-board situation using a PDA. The PDA access all live cameras and recorded videos of the on-board NVR.
11. Post-event analysis start with the removing of the cartridge of the on-board NVR and plug the cartridge into the workstation of the investigator
12. Find the suspect person and the abandoned luggage in the recorded video

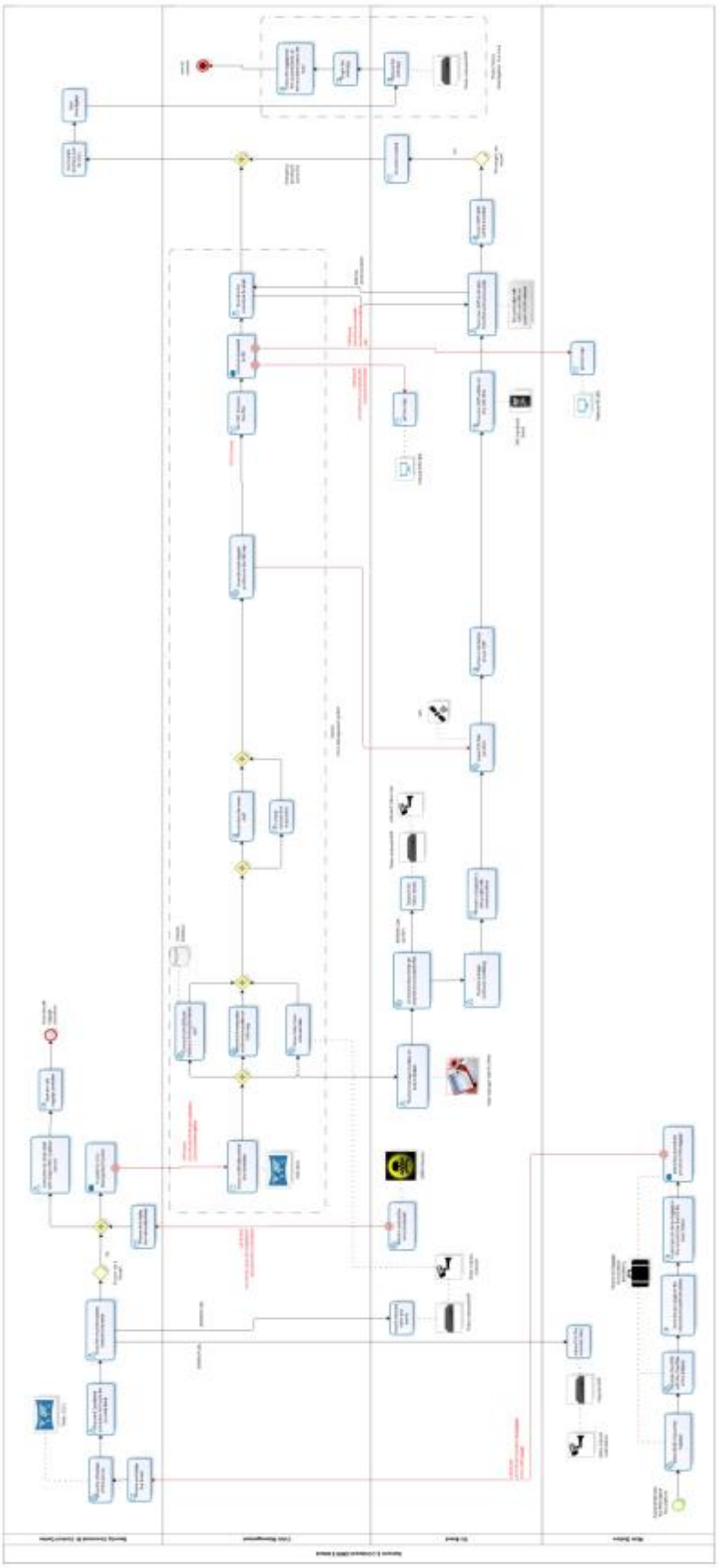


Figure 41 Scenario 3 - Luggage Reconciliation, CBRNE detection on-board and Investigation

6.3.8.7 SCRIPT OF SCENARIO 4 - CBRNE SCANNING FOR FREIGHT TRAINS

1. An on-board CBRNE detector detects a chemical threat in the freight train and sends an alert to the SOCC.
2. The SOCC visualizes that event and sends the train to the depot for the detailed screening.
3. The train will be send through the fixed installed X-ray Scanner. The Scanner isn't installed in Zmigrod. The video of the 2 sides of the incoming freight train is shown.
4. The X-ray scanner will simulate the detection of the radioactivity source and send out an alarm to the SOCC.
5. The SOCC will visualize the general "radioactivity source detected" alarm
6. As the next step the operator analyse the prepared x-ray images and localize the threat on the X-Ray scanner Image Operator Workstation.
7. The operator creates a report with spatial description and the picture of the X-Ray Image.
8. This report will send out as alarm to the SOCC with a link to the image. This alarm will be displayed in the SOCC with car number and Image of the X-Ray.

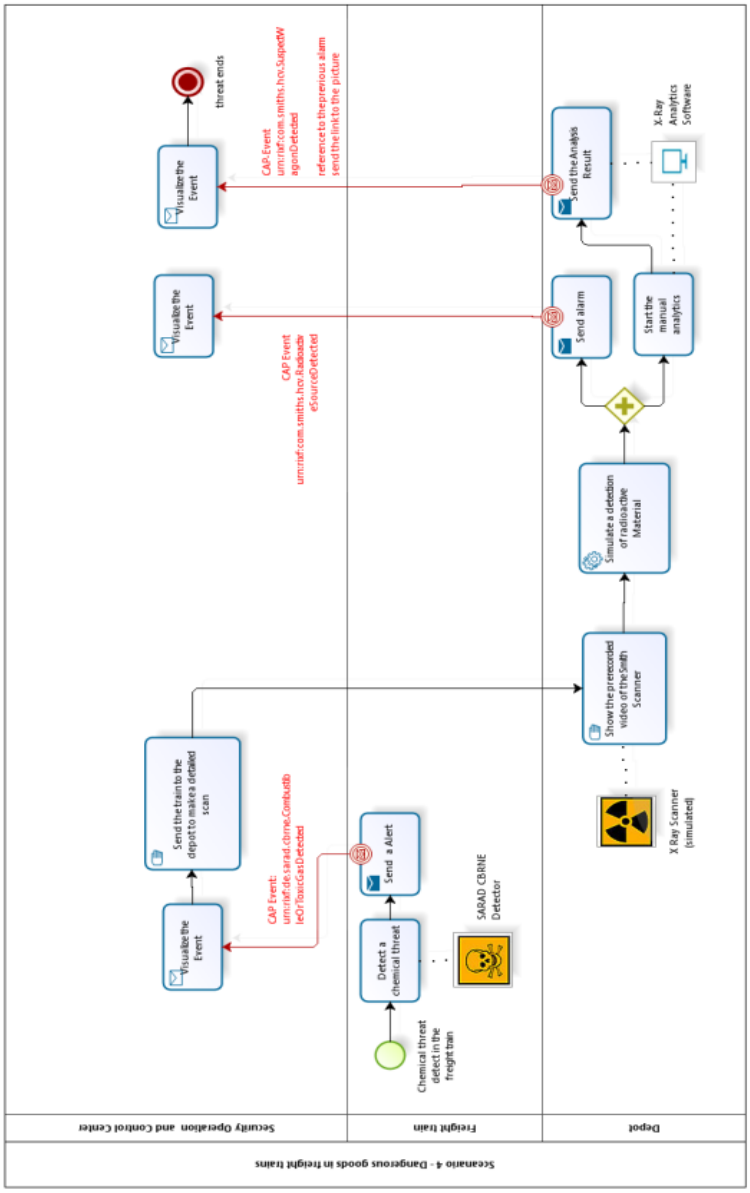


Figure 42 Scenario 4 - CBRNE scanning for freight trains

6.4 THE OFFICIAL ZMIGROD DEMO EVENT

About 100 people – among them EC representatives, partners, railway stakeholders, transport authorities and rail police – attended this final demonstration.

The IK Institute hosted this demonstration at the Zmigrod site. It allowed participants to discover all the state-of-the-art security solutions in real operational conditions, beyond laboratory tests. It represented an opportunity to understand how to protect railway systems and find solutions applicable for their specific challenges. For security providers from the industry, it was the perfect occasion to demonstrate their ability to integrate solutions in an interoperable manner. Here below some pictures of the event.

Figure 43: The Control Room

Figure 44: The PROTECTRAIL demo room

Figure 45: The audience on the day of the demo

Figure 46: The audience on the day of the demo

Figure 47: One of the Security Operation & Control Centre (SOCC) used in the demo

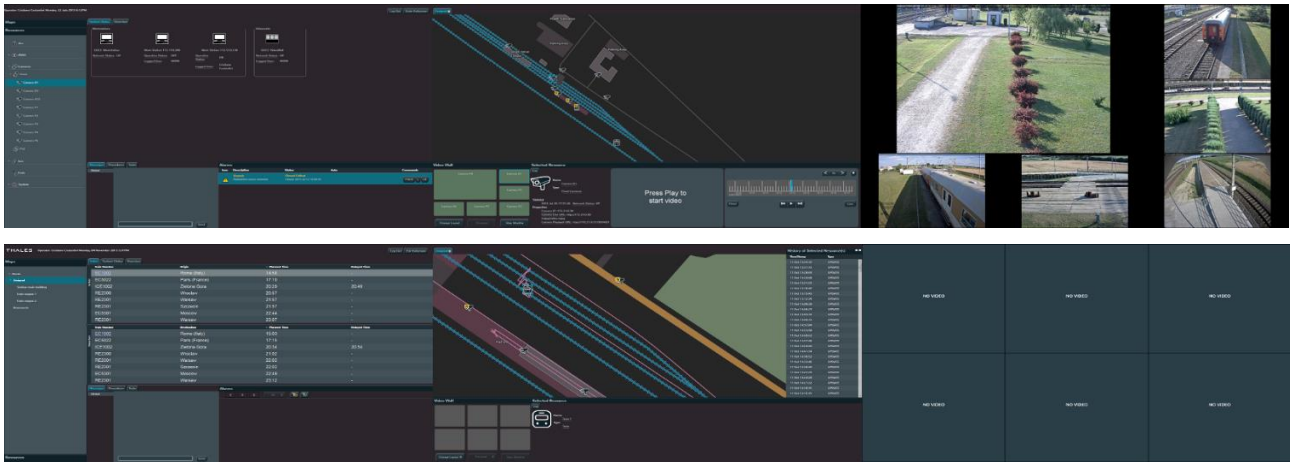


Figure 48 – Screenshots capture from the SOCC for the PROTECTRAIL project

Figure 49 Crisis Management System (CMS)

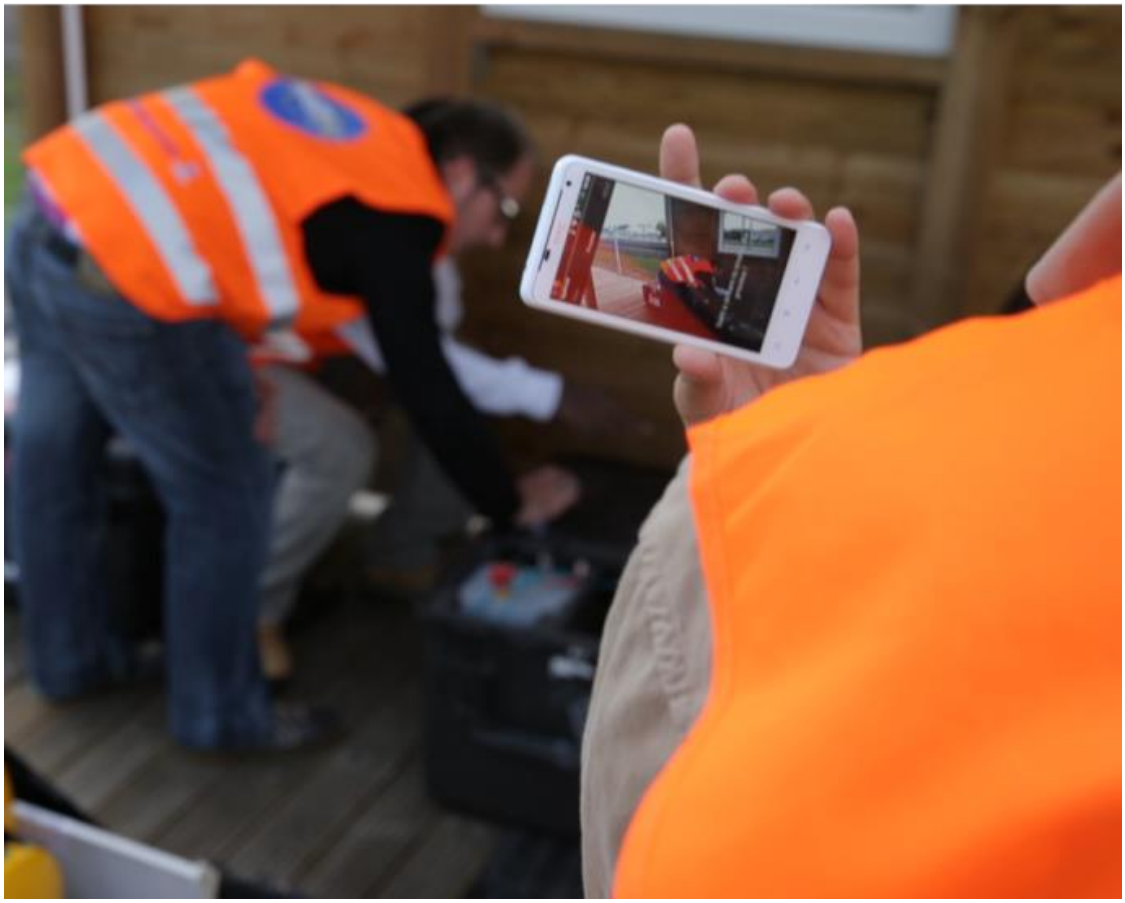


Figure 50 CMS Handheld Device

Figure 51: The presentation of results during PROTECTRAIL demo

Figure 52: The tour of the PROTECTRAIL demo site

Figure 53: The tour on board the PROTECTRAIL train

6.5 NON-FUNCTIONAL DEMONSTRATION

6.5.1 FRONT CAMERA SOLUTION

A solution based on image processing to help secure the itineraries frequently used by convoys during field operations has been developed and applied on the PROTECTRAIL. This system allows drawing attention of the vehicle occupants to any visible changes occurring along the route since a previous passage. As demonstrated in PROTECTRAIL, Change Detection can be used for the safety of railways also.

A forward looking camera has been mounted on the roof of the tractor (Figure 54). Very promising results were achieved, suggesting that a Change Detection system would be especially well suited to railway security monitoring.

Figure 54 Camera mounted on the roof of the tractor (left) and sample image of the Change Detection system used for railway monitoring (right).

6.6 DEMONSTRATION RUN IN SICILY /ITALY

6.6.1 THE LOCATION AND THE SECURITY SYSTEM

The selected location is placed in Sicily, near Palermo and more precisely nearby the Palermo Brancaccio station. The selected stretch of railway line is situated near the industrial and residential Brancaccio district, which is located halfway between the city centre and the southern outskirts of Palermo.

The nearby station of Brancaccio is divided into a part for freight trains and in another one for the stops of the trains arrived at the gates of the city. The station overlooks a huge open track with nodes and branches that allow the entry of trains or locomotives in deposits or in the various industrial warehouses located throughout the area.

6.6.2 THE SECURITY INSTALLATIONS

The demo site has been made up with three different cooperative systems: an intrusion detection system mounted on the fencing, a composite CCTV system and a cables duct alarm system.

For the preparation of the area a section of 50 m of the boundary wall between the road and the railway line has been demolished. In place of the wall it has been installed an active fence equipped with a set of inertial sensors (in Figure 55 is shown the site at the end of the fences installation). Here below are reported the main features of the fence:

- Piezo-dynamic sensors that sense the vibrations, including those which involve cutting, climbing and breaking of the structure;
- Precise revelation: each sensor is uniquely identified, so as to allow the identification of the exact point of alarm;
- Detection and reporting of the separation of sensors from the fence on which it is attached. This device also allows checking, via software, that each sensor is properly secured to the fence.

Figure 55 The active fences installed

At the two ends of the fence it has been installed two poles, the first one equipped with a thermal camera and an optical camera while, on the other side of the fence, a single optical camera has been installed on the second pole. Both optical cameras are equipped with an IR illumination system

with a remote control system. For what concerns the thermal camera, unlike many conventional video surveillance cameras, it does not require any ambient light or illumination. It detects infrared (heat) waves to provide users with thermal images in challenging environments, including complete darkness, over water and in dark corners, where threats are difficult to detect due to lighting constraints and weather conditions.

In the duct buried near the railway line, containing signalling equipment, it has been inserted, for a distance of 100 m, an optical fibre to detect unauthorized access. The main elements of the system are:

- Re-enforced Optical fibre cable;
- Optical Transmitters (TX) and Optical Receivers (RX);
- Alarm control unit connected to the Optical Receiver;
- Optical switches to detect opening of ducts;
- Installation of steel shelves with cable ties so to delay cable theft attempts and to amplify stress sensitivity of the fibre optics.

The here briefly described system is able to detect, in every moment of the day and in all weather conditions, any attempt of intrusion into the railway line through:

- The video analysis of the videos collected by the optical and thermal cameras: Video streams are analysed in real time to detect:
    - Motion
    - Loitering
    - Unattended objects

In Figure 56 is shown the area of the demo site covered by the video analysis.

- The alarms provided by the inertial sensors mounted on the fence in case of "climb over" attempts as shown in Figure 57 or “fence cutting attempts” as depicted in Figure 58;
- The alarms provided by the optical fibre protection system in the case of unauthorized opening of the duct as shown in Figure 59.

Figure 56 The area of the demo site covered by the video analysis

Figure 57 Climb-over attempt

Figure 58 Fence cutting attempt

Figure 59 Unauthorized opening of the duct

Track protection system here introduced is monitored by the Operative Control Centre and locally managed by the Security Management System (SMS):

- SMS integrates all the technologies and collects all the data/alarms/diagnostics coming from cameras and active fences;
- SMS records and stores all the information to allow further analysis;
- Operators can manage information (alarms, video streams, diagnostics) by an user-friendly interface.

Moreover the track protection system has a 'rules engine' server, that defines a complex security behaviour and maximizes the probability of detection, reducing false alarm rates.

The system has been shown and tested during PROTECTRAIL final conference in Paris on the 27th of May 2014.

6.7 DEMONSTRATION RUN IN VILLECRESNES/FRANCE

6.7.1 EXPERIMENTATION OBJECTIVE

The objective was a realistic experimentation covering around 1 kilometre of in-service track over three months (day/night, all-weather conditions, etc.) in order to realistically evaluate solutions with all data recorded to emulate a process keeping a remote operator in the loop, able to assess the alarms. The conditions were to do so without impacting the high frequency line operations.

6.7.2 THE LOCATION AND THE SITE DESCRIPTION

The selected site is located in Villecresnes (France), on the South-East TGV line, 25 km from Paris. A satellite image of the area is reported in Figure 60.

Figure 60: Villecresnes TGV demo site

6.7.3 THE SECURITY INSTALLATIONS

Different solutions were considered but the following are the ones that have been demonstrated for fences, tunnel, buildings and/or overview protection, and combined:

- PROTECTRAIL partners:
  - PROTECTRAIL TGV Supervisor
  - Automatic intrusion detection on thermal cameras
  - Compact system for real-time movement analysis
  - Tunnel entrance intrusion detection system (thermal + visible)
- Others:
  - Radar system
  - Scanning laser barrier for tunnel entrance protection

Data (videos and alarms) were stored on a distant site in order to run the video algorithms in a safe zone and avoid complex processing on the experimentation site. Transmission of data was performed thanks to a WiMESH network onsite then through optical fiber between Villecresnes site and the storage site (~33 km).

6.7.4 GENERAL CONCLUSIONS

All the detections have been understood thanks to the video: video or image is essential for the operator to assess the alarms reported by the systems in place. Thermal cameras are mandatory to validate alarms occurring at night time, but it was also useful to detect persons behind vegetation, not visible with normal cameras.

False detections are due to criteria complexity, and this demonstration proves that reality is very different from in-lab tests (for example projected shadows, trains speed, lights reflection, vegetation, animals, etc.). In addition, this demonstration run over a long period of time allowed some partners to improve their system during the experimentation, and a distinct enhancement was observed.

On the preparation aspect, the integration of alarms from different partners (both PROTECTRAIL and not PROTECTRAIL) was easy.

Finally, an operational conclusion of this experimentation is that there is a clear need for a long period of tests to have realistic conclusions… 3 months was great but not sufficient!

Moreover, ideally, all videos should be viewed (everything has been recorded) in order to define false-negative rate: potential intrusions detected by no sensor are not checked but the likelihood is very low as there was a lot of alarms & the systems were redundant on the access points!

6.7.5 CONCLUSIONS BY SYSTEM

6.7.5.1 SCANNING LASER BARRIER FOR TUNNEL ENTRANCE PROTECTION

A scanning laser barrier has been installed to protect tunnel entrance from possible intrusions. This system is used in addition to the following system named “Tunnel entrance intrusion detection on thermal and visible cameras”.

The scanning laser barrier proved to be effective as all intrusions inside the tunnel have been detected. Some false alarms were due to shiny trains passing or windows. However, this can be improved if the sensor is installed closer to the tunnel to allow to visualize the back wall of the tunnel (fixed reference): this was not possible for this experimentation due to security constraint (forbidden to be too close of the entrance for a temporary installation).

6.7.5.2 TUNNEL ENTRANCE INTRUSION DETECTION SYSTEM (THERMAL + VISIBLE)

This system, based on a Video Algorithm applied on a thermal and a visible camera, was used to check the surroundings of the tunnel entrance. On the visible camera, all intrusions have been detected.

On the thermal camera, conclusions are more difficult as the camera had to be restarted frequently and was off half of the time. But there were fewer false alarms per day on: the reason is that it was less sensitive to luminosity changes. So the thermal camera could be used alone, even if both cameras can be used for data fusion.

The videos of this system were also useful to validate the alarms coming from the scanning laser barrier system.

6.7.5.3 AUTOMATIC INTRUSION DETECTION ON THERMAL CAMERA

Placed above the tunnel entrance and looking along the tracks, an automatic intrusion detection system on a thermal camera has been installed.

Due to settings, the emails were not delivered to the relevant address so assessment was done on around one month recordings, but most of the human intrusions were detected. The camera was used extracting full time the video stream but it can also be used as initially designed, i.e. to work alone and to send email including short video sequence only when an intrusion is detected.

6.7.5.4 RADAR SYSTEM

Looking at around 450 meters of tracks, a radar system has been installed coupled with a visible camera.

After test and configuration phase, this system had good results with ~1 false alarm per day on (mostly due to wind). On this system, when an intrusion was detected, the camera associated zoomed and the intruder was followed during its presence in the protected area.

During the night, alarms were manually validated thanks to an additional camera part of the “automatic intrusion detection system on thermal camera” (see below) (as the radar was only automatically associated with a visible camera).

6.7.5.5 AUTOMATIC INTRUSION DETECTION ON THERMAL CAMERA

Looking at the same area as the radar system (around 450 meters of tracks), an automatic intrusion detection system on thermal camera has been installed.

This system proved to be effective as all human intrusions were detected,, both during day and night, as well as in fog conditions. Some alarms due to trains and foxes were reduced during the experimentation thanks to filters improvement and clustering on the fragmented detections.

Depending on the area to protect, it is possible to increase the focal length of the camera optics to gain detection on a longest distance.

6.7.5.6 COMPACT SYSTEM FOR REAL-TIME MOVEMENT ANALYSIS

A compact system for real-time movement analysis was installed to protect the entrance of the area where some technical buildings are present.

Based on transversal movement analysis, it proved to have good results with significant intrusions reported with at least 1 alarm per person intrusion, and an efficient filtering of trains, cars and irrelevant movements (vegetation, catenary wires). Moreover, night mode was validated using standard CMOS sensor. This system did not need high bandwidth as intrusion assessment was done on photographs only.

It was the first evaluation of this system in a specific intrusion detection application: thanks to PROTECTRAIL, this system changed its TRL from 5 to 6.

6.7.5.7 TGV SUPERVISOR

The TGV supervisor system proved to be a good and simple tool for an operator to interpret alarms real-time and post-event.

It is a web-application (no deployment needed on workstations) that can be displayed on one or two monitors, with the following elements: map, alarms, video streams live and recorded.

It adds convenient features to classic video functionalities: snapshots, in addition to trick-play features, and also, an easy extraction of videos as AVI files and ISO22311 files (useful for forensics purpose).

Regarding the alarms, they are strongly linked to videos, for an efficient real-time and post-event analysis: alarms are displayed as a list, geo-localized on a map and overlaid on the video.

Finally, cartography can use any WMS (Web Map Service) server or Google Maps.

6.7.6 IMAGES OF THE VILLECRESNES DEMO

Here below is reported a set of images trying to synthetize the results of the system installed and demonstrated in Villecresnes:

Figure 61 Visible and Thermal view

Figure 62 Intrusion Detection at night time (thermal camera)

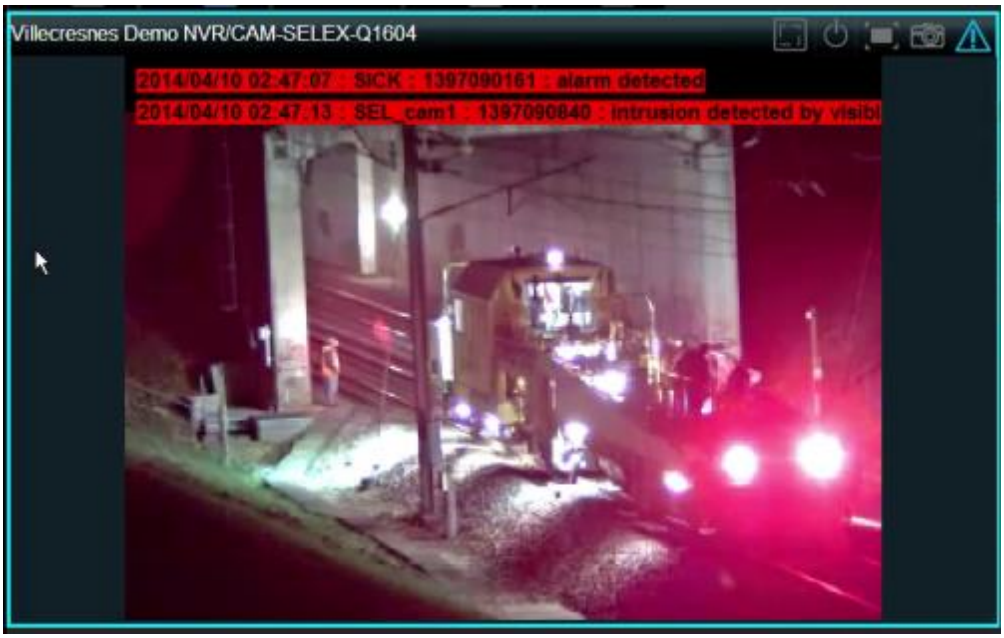


Figure 63 Tunnel Entrance Protection

6.7.7 CONCLUSIONS

This experimentation was a temporary test with some constraints which would not be present for a real implementation:

- Temporary masts moving due to the wind
- Field of view forced by the installation constraint (out of the fenced area)

However, this experimentation has been really appreciated by all the partners. Tests in real environment are much more valuable than tests in-lab to improve the solutions and having the possibility to test on a long period allowed to have various scenarios representative of real life.

6.8 LESSONS LEARNT FROM THE DEMONSTRATIONS

6.8.1 ENABLING SECURITY SOLUTIONS

The challenge of combining a large variety of technological and procedural security solutions lies in the technical integration of the various systems and in the ability to combine the strength of these devices in a global and coherent system. This section provides theoretical background information on interoperability.

The PROTECTRAIL approach allows for technical, syntactic and semantic interoperability of the different systems as defined in the Levels of Conceptual Interoperability Model (LCIM):

- Technical interoperability is achieved using standardised common communication protocols in order to exchange data between the participating systems,
- Syntactic interoperability is achieved using a common data model such as the Common Alerting Protocol (CAP) of the Oasis Consortium in the PROTECTRAIL demonstration and
- Finally semantic interoperability is achieved by defining the content of the information exchanged in restricting the data model used.

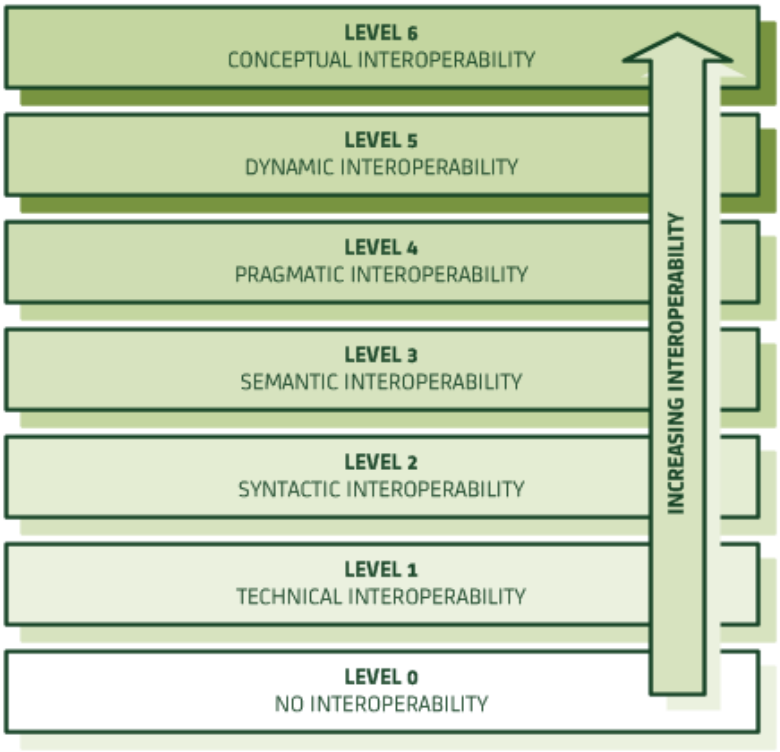


Figure 64 Increasing interoperability levels

In order to achieve a higher level of interoperability, shared methods and procedures are required in order to efficiently use the available information in the context of a security incident. With this goal in mind, Security Operation Control Centre solutions from different partners can be integrated in a global security system.

These control centres actively share contextual information during the development of security incidents using the interoperability framework and also apply predefined and agreed security methods and procedures in response to the different security threats. These procedures and methods can be applied separately in the different security control centres hence providing a high level of interoperability between such heterogeneous systems.

Future implementers may benefit of the lessons learned from PROTECTRAIL:

- Interoperability is to be achieved block by block and needs to be built on strong foundations; technical interoperability is not enough to guaranty system level interoperability.
- The use of open standards or documented norms facilitates the adoption of an interoperability framework, especially when a large number of partners with different objectives are involved.
- The end-user of the system should be involved in the definition of an interoperability framework in order to achieve high level interoperability.
- Real interoperability can only be achieved if all actors in railway security can agree on a common implementation of security interoperability standards.

6.8.2 NETWORK COMMUNICATION

PROTECTRAIL has proven the importance of state of the art network architecture for railway security applications. In line with the general requirements for interoperability and modularity, PROTECTRAIL confirmed that the visibility of train and other railway facilities can be improved using various security applications. These applications require HIGH BANDWIDTH bi-directional communication links to be able to exchange messages with each other.

PROTECTRAIL members installed various security solutions with many geographically distributed data collection points, both stationary and mobile. These capacities were connected via various communication channels such as high speed optical networks, coaxial cables, and wireless links. The data collected from various sources were preserved with full consistency by using NTP-based time synchronisation with geo-location.

Providing diversified railway security and infotainment applications, including video surveillance, voice communications, system maintenance, e-booking, and other broadband services, mandates high a quality IP-based Ethernet network. While wired networks are already mature enough to support these applications, wireless networks have proven to be a challenge due to the non-deterministic nature of radio signals when the train moves at high speed.

When designing a network for on-board and wayside applications, the following best practises should be considered:

- Train to wayside communication links form a crucial subsystem in delivering diversified railway security and infotainment applications on-board. Delivering such a communication subsystem and fulfilling the QoS requirements of a broad range of applications is always going to be a challenge. PROTECTRAIL succeeded in showcasing a multi-modal Train to Wayside Communication System (TWCS), using various modern wireless technologies. This TWCS make use of existing commercial telecom infrastructure (i.e. LTE, HSPA+, HSPA, etc.) and optionally, it combines these networks with private wireless technologies (i.e. 802.11 n Wi-Fi). As it provides redundancy between commercial and private network it increases the end-to-end throughput by combining both networks when available.
- For real-time video streaming, a case by case trade-off between UNICAST and MULTICAST must be made. While UNICAST may be beneficial when there is only one or few consumers, MULITCAST helps preserve scarce bandwidth when there are multiple consumers scattered over different locations. An on-board Network Video Recorder (NVR) server with MULTICAST streaming feature could be used. **Adaptive variable bit rate streaming** could also be beneficial for preserving scarce bandwidth but there is no mature solution due to a lack of standards.
- Cyber security is of growing importance for the railway sector. The railway industry needs to establish security standards and best practices for information security management like the ISO 27000 series. In this context security technologies like VPN for secure collaboration in distributed locations and MPLS for high-performance routing in large networks and redundant network connections in case of a failure or an attack, virtual LANs for a secure segregation and guarantee a quality of service for safety related applications.

6.8.3 MODERN AND PRACTICAL APPROACHES TO VIDEO AND VIDEO-BASED ANALYTICS

In line with the general requirement for interoperability and modularity stated above, PROTECTRAIL integration confirmed that the sole implementation of the video-surveillance industry standards (IEC 62676-1&2 and even ONVIF profiles) is not enough. This is further complicated by the regulatory need for stability and trustworthiness as well as privacy protection imposed on security video systems.

The lessons learned from PROTECTRAIL are recommendations for:

- A generalised use of RTP/RTSP streams carrying video H264 compressed metadata time stamped at the frame level, consistently with the security events described above
- Full modularity of the basic services associated to video, independently of their physical implementation
- Video-surveillance systems are networks of distributed PC's; as such they are potential targets of cyber-attacks, against which they must be protected (physically, by training staff or with software)
- Digital video, especially when live information with low latency is required, has stringent needs for communications channels (no buffering is allowed); this implies a good quality of service for the communication but also an optimised set-up in the network architecture to minimise throughput at any point of the network in all circumstances (typically a case by case trade-off between UNICAST and MULTICAST)
- The system must preserve full consistency between time and metadata associated with the streams, the events produced by the analytics (see below) and the supervision tools.
- By law the operators generally cannot access the recorded video files for **privacy protection** reasons. If the operator wants to use the video for operational security or training, they have to remove the privacy related attributes for instance by using face blurring.
- If the control centre wants to access the on-board videos in real time, the infrastructure is not prepared to get a constant video streams today. ONVIF and RTSP are made for networks with a constant bitrate. For videos streaming on wireless networks the solution is an **adaptive bitrate** for video streaming depending on the existing wireless infrastructure.

Several video analytics solutions have reached a reasonable level of maturity, such as:

- *Video tracking:* video tracking is the process of locating an object (or more than one) that moves in time, using a camera. An algorithm analyses the video frame and gives as output the position of the target objects. The main difficulty in video tracking is to capture the correct position of targets in consecutive frames, especially when objects see their aspect change over the time and move at a higher frequency than the frame rate. Semi-automatic tracking is a tool provided to video-surveillance operators to support them in doing more efficiently a task performed today manually, after appropriate training. This function can be activated locally for benign events, but can also be run at the security control centre in real-time in case of more complex situations, before the situation is handed over to the police, or after the event to help selecting the appropriate video sections requested by the police for forensic investigations.
- *Crowd Detection:* crowd density detection provides information that may be relevant for safety. It is also a key parameter for making the right decisions in several security-related crisis situations. It must be noted however that in many large cities crowds as such are not considered a situation critical to detect for security reasons. Similarly multiple individuals collapsing in a station must be detected to confirm a chemical attack in a given area.
- *Face recognition:* a face recognition system is a biometric technology which is well-accepted by the population as it is close to a human recognition process and is almost non-intrusive. Therefore, many systems include biometry in order to identify or confirm the identity of a person. Nevertheless, this technology may be difficult to implement as it is sensitive to many variations (aging, facial expression, lighting, face orientation, beard, hair, clothing, etc.).

- *Intrusion detection:* to detect objects existing in restricted areas, it is necessary to extract objects in video frames. Object extraction consists of background generation, configuration of region of interest (ROI), extraction of object candidates based on background subtraction and contour labelling, noise elimination, and calculation of object information such as size and position. Algorithms of intrusion detection can help in:
    - Detection of persons in areas that are supposed to be empty;
    - Perimeter anti-intrusion (including in-service tracks);
    - Graffiti prevention.

Regarding such analytic applications, the lessons learned in PROTECTRAIL are recommendations for:

- A minimum configuration required for analytics: For example many analytics require an initial calibration for each camera (e.g. to determine its 3D location and orientation or to adjust to internal lighting conditions). To make larger setups (50+ cameras) manageable it is recommended to either automate these calibration procedures with sufficient quality or to use solutions that do not require such configuration.
- Using analytics for decision support and not as fully-automated security solutions: Complex systems are never 100% fail safe or fail in unexpected conditions. An interactive system provides functionality to support an operator who is the human-in-the-loop.
- Metadata standardisation: Full consistency for video analytics remains an open issue as there are no well-established industry standards and video analytics are a quickly evolving market. Maintaining consistent metadata definitions will require attention when solutions are integrated, especially when a new solution needs to fit into a legacy system. In this situation, the most future-proof approach is to stick on the minimum criteria for events outlined above and rely on associated URLs for details.
- Wider system (e.g. Storage/Playback/GUI/other) requirements: Video analytics usually need more performance or have wider requirements than basic video solutions. Some analytics require for instance high frame rates/high resolution playback of stored data instead of a lower resolution, lower frame rate data. Other analytics might need an extra monitor because they require certain user interactions or provide information that cannot be displayed on a video stream. It is recommended that the video-surveillance systems that might be extended at a later time with analytics are designed for upgrade, typically to support analytics (e.g. room for servers or extra monitors, etc.).

In addition to the real-time (or near real-time) solutions described above, collected videos must be usable for forensic analysis. This implies minimum video quality (sometimes mandated by law), proper and unambiguous identification of the scenes, time of occurrence and the ability to be decoded by police systems. ISO 22311, recently promulgated, addresses these requirements.

PROTECTRAIL also recognises that video-surveillance can be extremely useful for security management and crime investigation, but that it also might result in an unnecessary intrusion into citizen privacy. When video surveillance is used a balanced guided by regulations complemented by common sense needs to be struck.

7 SP6 FUTURE DESIGN FOR SECURITY

As mentioned above in SP6 two basic models of railway security forecasting based on 2 different approaches have been designed, implemented and validated offering possible future solutions to increase railway security by protection and mitigation means and effective and efficient measures to support and/or increase the capability of crisis management. SP6 has also delivered a vision of future railway system in next 10-20 years. In the Figure 65 is shown the SP6 relationship between WPs and to other SPs, while in the paragraphs below are reported the main results obtained by this sub project.

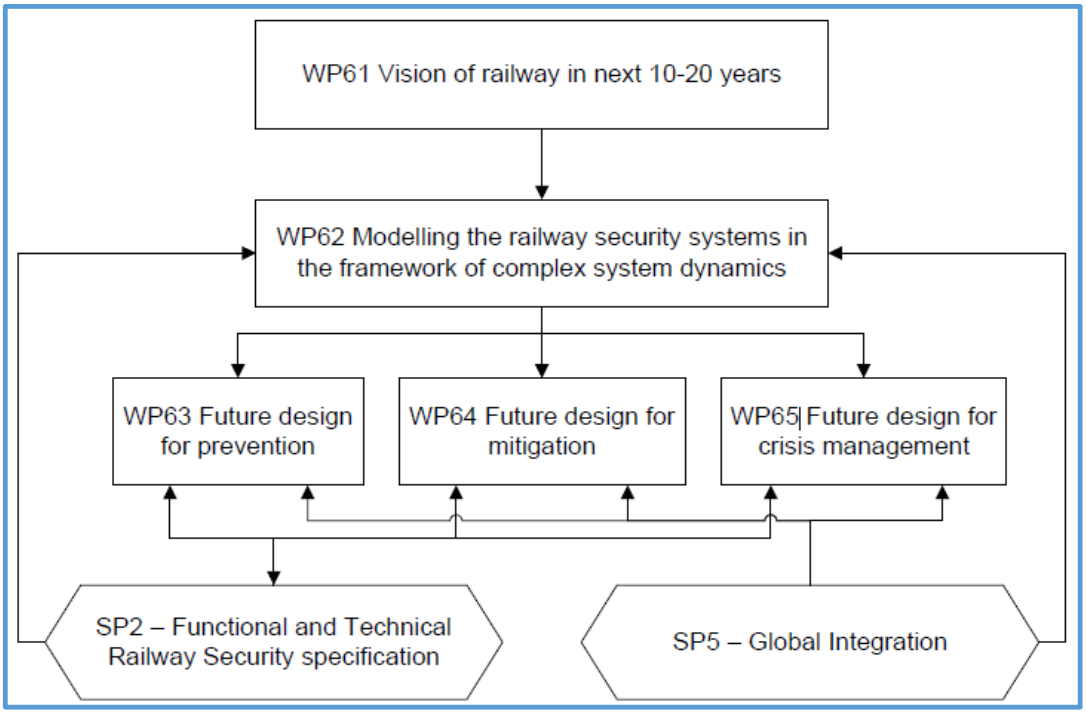


Figure 65 - SP6 relationship between WPs and to other SPs

7.1 VISION OF RAILWAY IN NEXT 10-20 YEARS

The aim of the work package was to develop a vision of all the stakeholders in Europe of the railways of the next 10 to 20 years. From the activities of the WP it was found that the major inputs for the vision within a coherent security context are addressing the following for railways:

- Rail passenger services : the development of High speed (size of the network, commercial speed, evolution of rolling stock), the development of daily transport (capacity, efficiency, liability and regularity, intermodality), the development of rail station (urban integration, ticketing, interoperability between the functions);
- Rail freight: the development of international corridors in order to increase the traffic (Europe North South, between Europe and Asia for example)
- For the infrastructure: the increasing use of tele-transmission and satellite in signaling and protection of traffic; implementation of ERTMS.

Regarding future trends of traffic volume and infrastructure expansion the base ground information is coming from the 2011 white transport paper that somehow sets the trends and objectives for all transport modes in the Trans European Network-Transports (TEN-T). It is also been considered all the other EC policies for the 2020-2050 period regarding the energy and environmental (including clime change). The instruments of the 2011 White Paper has been adapted to a new context of an enlarged Europe, rising petrol prices, Kyoto commitments and globalisation. A European sustainable mobility policy needs more policy tools to optimise the performance of each transport mode and their combined use. The Commission adopted a logistics action plan in 2007 in order to create better synergies between road, sea, rail and river, and integrate various transport modes in logistics chains.

This will give the industry a competitive edge but also diminish the environmental impact per unit of freight. The discussions and information collection on different UIC platforms (freight; high speed and passengers) also lead to consolidate the information at the global level. That consolidated the feeling the rail transport will grow sustainably in the next 20 years.

7.2 MODELLING THE RAILWAY SECURITY SYSTEMS IN THE FRAMEWORK OF COMPLEX SYSTEM DYNAMICS

The main objectives of the WP were:

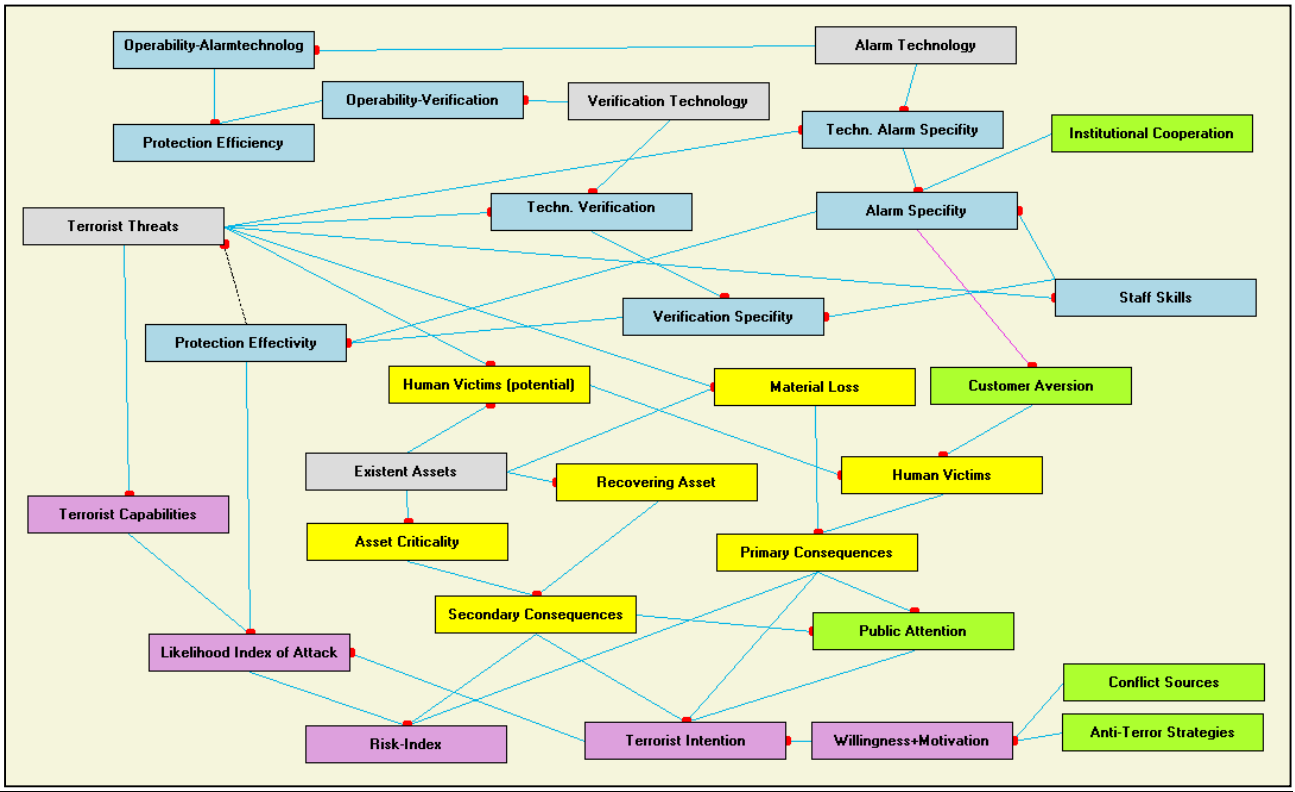
- The description of the railway system model and of scenarios of system evolution.
- The development of software to generate the system model.

During the Project it has been developer two different models described in the two sections below.

7.2.1 THE FIRST DEVELOPED MODEL

The first one is a basic model of railway security developed using 29 Key Factors (the intended user for the model is an asset owner) while the second model has been developed in order to fulfil the needs of WP64. This model complements the previous model in the sense that it does not model a single asset, but it models the strategic level: a national railway system.

The identified Key Factors are not independent from each other. The aim of the *Model* is to describe these mutual interactions and analyse the impact on security if one or more Key Factors are changed. The network of identified Key Factors is given in the following figure: (The arrow-heads are marked by red points.



First text line of the Key Factors:	Name of Key Factor
Key Factors related to system configuration	Key Factors related to consequences
Key Factors related to Technology	Key Factors related to terrorism
Key Factors related to external impacts	

Figure 66 - Network of used Key Factors.

The interactions between Key Factors are symbolized by arrows. Arrow-heads are marked by red circles. Blue coloured arrows indicate an increasing impact on the target factor red coloured arrows

indicate a decreasing impact. Regarding this first model it estimates the risk closer to the reality by considering a set of factors influencing consequences and possibility of an attack, for example the terrorist capabilities to apply distinct weapon types. The Model has been designed as a tool to analyse and compare the implications of different sets of assumptions to the risk connected with the considered asset. Thus it is intended for usage by consulting experts or persons responsible for planning and design of security measures for the considered assets with a medium or long-term time horizon.

The Model uses the Key Factors describing the relevant factors influencing the security of individual railway assets. Each Key Factor belongs to one of the following groups:

- Existent Assets;
- Terrorist Threats;
- Consequences;
- Protection Technology;
- Environmental Impacts.

7.2.2 THE SECOND DEVELOPED MODEL

The second model has been developed, has already mentioned, to support the analyses of WP64 in the following way:

- The direct impacts of changes are put into the model and the model shows the reaction of the system to that impact. For example : Suppose there is a certain new measure against copper theft from a track. This measure is added to the model, including the causal relations that represent the expected direct effects this measure has on any influence factor (objective security, subjective security and railway performance). E.g. the material impact will shrink. Subsequently, the model shows how the system reacts to this change;
- The model will help to identify indirect relationships and causal loops which can be essential to explain the net effect of an intervention;
- The model itself can be analysed to determine where an intervention would potentially have the highest impact to reach a certain goal. As this third use is not a direct requirement for the model, it will be determined in WP64 if this will actually be part of the analysis.

The model will thus help us to analyse a scenario systematically. Input for the model will be the impact of a measure on the defined influence factors. Running the model it is possible to determine:

- The impact of a change on all influence factors;
- The influence path that leads to the changes.

This information has been subsequently used in the analysis to quickly identify:

- The impact of a measure on the KPIs;
- The impact of a measure on security;
- The way (reasoning) in which this impact is manifested.

This information has been then used in a broader analysis to determine a relative comparison of the effectiveness of measures (design, materials, technologies or tools) to reduce the consequences of an attack.

7.3 FUTURE DESIGN FOR PREVENTION

The scope of the WP was to develop a model to design and evaluate measures to prevent terrorist and criminal attacks on railway assets. The developed model has been based on design principles of the first model developed in inside the WP6.2 modifying it in order to meet the special requirements of prevention. Prevention in this report has been defined as collection of measures reducing the vulnerability of individual assets and preserving the business continuity of railway operation. The economics of investigated solutions have been analysed in terms of cost effectiveness to give the possibility to the user to compose 'security solutions' with respect to priority and available budget. It has been identified a set of about 30 key factors to estimate the effectiveness of preventive measures with respect to terrorist or criminal threats to individual assets. Because of the wide variety of railway

asset all numerical estimations are based on a virtual medium sized asset of about 200 000 passengers per day. However the selected key factors and their mutual interactions can be used as a guideline to design a prevention system of any particular asset. The present and future states of interesting key factors have been computed for several scenarios, among others: "High and Low Probability Attacks" and "Cyber Criminality".

7.4 FUTURE DESIGN FOR MITIGATION

Based on the comprehensive system approach developed in WP 6.2 the WP 6.4 investigated how design, materials, technologies or tools could be selected and deployed in the system to reduce the consequences of an attack: e.g.: performing safer evacuation of people and first aid to victims; increasing the resilience of infrastructure by use of new materials, by setting rules for new infrastructures or enhancing / retrofitting legacy procedures and organization rules will be also addressed. The WP investigated the impact of the mitigation measures on the survivability of people (employee, customers, neighbour of railway), components and infrastructures (e.g. due to the blast effects of an explosion). Furthermore it has also examined how the security measures could be designed to be compatible with: operators investment and/or operational cost constraints, quality of service and security constraints, competitive position of rail transportation. The WP produced a description of the developed model and its validation and the detailed version of the analysis done showing that the chosen approach was valid. It also provided a user guide describing how the process of the selection of the best mitigation measures should be carried out. Furthermore, this user guide gives categories and types of mitigation measures and it gives the analysis results of a set of mitigation measures.

7.5 FUTURE DESIGN FOR CRISIS MANAGEMENT

The WP analysed how to understand and report an emergency situation, e.g. evaluating and establishing the parameters of the emergency, dispatching emergency response personnel and equipment to the emergency site, coordinating the activities of all emergency response personnel, protecting people, personnel, and equipment at the emergency site. The main steps to achieve the objectives described above were

- Identify and describe the organizational structures of national crisis management agencies and of crisis management within railway undertakings. Describe differences and commonalities.
- Use different information sources to identify potential future developments in these organizations
- Use the software developed in WP62 to transform the information collected above into a formalized model of external and internal influence factors and to define in which way crisis management is influenced by externals and which consequences this has for internal instances, in general crisis management and in railway related crisis management.
- Also integrate into this model technical developments in the railway security area, especially (but not restricted to) those which have been integrated and demonstrated within PROTECTRAIL SP5.

The results of the WP activities consist of a collection of possible or likely future scenarios and their expected consequences for important goals of crisis management. A typical scenario example is a significant increase of terrorist activity. The developed model shows for this case

- how the performance of crisis management will decrease (more fatalities, more damages) if the national and/or the railway crisis management organizations remain unchanged;
- how this effect can be neutralized by either more country wide security measures installations or more and better educated crisis management personnel.

The model also shows the interdependency between terrorist attacks and normal criminality (concerning security measures).

The technique used for modelling with the software and for generating the above results is explicitly described and thus opens for any reader (e.g. decision makers) the possibility to modify the model and to define additional scenarios (if the software is available).

8 HIGH PROBABILITY LOW IMPACT (HPLI) EVENTS WITHIN PROTECTRAIL

The PROTECTRAIL project, following the RP2 review outcome, has agreed to expand its focus from the protection of railway from terrorist attack (that was the focus of the call) to the wider objective of protecting the railway from High Probability Low Impact (HPLI) security events. To this scope it has been decided to publish a Call for Demonstration and to develop a Cost and Benefit Analysis.

Inside the contest the following proposals have been received:

- Door blocking (in real time - with a real door)
- On-board crowd density detection (from NVR)
- Privacy protection for CCTV (technology enabler - integrated in both above)
- On-board to ground protocol for emergency and situation assessment (enabling technology)
- People tracking from NVR
- People flow measurement
- Reporting of events from the field
- Trespassing/restricted area encroachment

The above HPLI solutions have been presented at the PROTECTRAIL final event, all integrated within the PROTECTRAIL integration framework, thus demonstrating that the proposed integration process is quickly applicable to any new solution.

Figure 67 - An HPLI solution at the final event

Regarding the Developed Cost and Benefit analysis for HPLI events it has been developed a CBA process composed of the following steps:

1. Identifying and create a formal mapping of all types of events which have the potential to cause inconveniences to passengers, to the operating organization and to other members of the public;
2. Estimating the frequency at which each of those types of damage causing events occur.

3. Estimating the overall annual cost (or "loss value") associated with each type of event. This has been done by shaping a set of functions each of which expresses the dependency of the cost associated with a given category of loss on the frequency of occurrence of any type of event.
4. Calculating the Loss-Value-Function (LVF).

At the end of the study it has been applied the developed methodology to a real case study to show the potentialities of the proposed CBA in a context where the need for an efficient use of limited resources fosters the application of risk oriented methodologies in the design and implementation of railway security systems.

9 CONCLUSIONS

Looking back at four years of PROTECTRAIL, it becomes clear that PROTECTRAIL was not a security project like others but an integration project. The objective of PROTECTRAIL was to define a security system and reach a level of standardisation for ICT in rail that has already been achieved in other industries. The methodology for the integration of security technologies has worked and shown to be adequate to the scope, efficient, scalable and able to evolve in time thanks to its simplicity, non-proprietary nature and standardisation. It can accordingly be recommended for new systems. It is important to note that the integration of security technologies in the railway sector is difficult but achievable even within the current European and national legislative framework and with existing standards. Key lessons of the security architecture recommended by PROTECTRAIL are:

- with the minimum set of information available in an event (time, nature and geo-location) together with smart services like discovery it is possible to efficiently and flexibly manage situational awareness in both fixed and mobile security applications;
- the SOA-based architectural framework and the information content of the standard events are much more important than the SOA tools to implement the framework and the envelope that contains the event (concepts and information are resilient to evolution, changes or obsolescence of information technologies tools and solutions);
- the seamless resilient integration of different wired (Ethernet and MPLS) and wireless (LTE, ZigBee, WiFi) communication technologies has proved to be a key success factor.

By establishing standardised events and SOA principles in security and rail infrastructures, the industry achieves a better interoperability, and the time to integrate new security solutions, the cost to develop and test new solutions is reduced drastically, and security stakeholders understand each other during security events and crisis situations.

If implemented in the railway sector, the PROTECTRAIL results will help the rail sector to advance and to catch up with security in other fields. In the railway sector too security needs to be approached in a comprehensive and coherent manner and must be based on a system that is able to integrate new security solutions, be it to minimise the risk of a terrorist attack or reduce costly everyday forms of crime such as metal theft. When looking further into the future however it becomes evident that PROTECTRAIL can only be a first step. Slowly but surely the ICT world is moving towards an “Internet of Things” and the railway sector needs to be part of this development.

As always when discussing security it must be kept in mind that even though security is a fundamental value in our society, it does come with economic costs (for investment, deployment, operation and maintenance) and social costs, in terms of potentially reduced freedom and privacy for citizens. When prioritising one over the other, a careful balance needs to be struck.

All in all, PROTECTRAIL with its future-proof methods and recommendations is clearly a success for the railway sector and the European Commission can be thanked for the efficiency of its financial commitment. PROTECTRAIL will help railway transport play an irreplaceable role in mobility by making it even safer against petty acts of vandalism and sophisticated terrorists attacks. This is particularly important during a time when the complexity in the sector grows due to new technologies and new and more actors.

10 THE PROTECTRAIL CONSORTIUM

Ansaldo STS S.p.A.
www.ansaldo-sts.com
IT

Nederlandse Organisatie voor toegepastnatuurwetenschappelijk onderzoek TNO
www.tno.nl
NL

Selex ES S.p.A.
www.selexelsag.com
IT

Union Internationale des Chemins de fer
www.uic.org
FR

Bombardier Transportation GmbH
www.bombardier.com
DE

Alstom Transport S.A.
www.alstom.com
FR

Thales Communication and Security S.A.
www.thalesgroup.com
FR

Sarad GmbH
www.sarad.de
DE

UNIFE – The European Rail Industry
www.unife.org
BE

Morpho S.A.
www.morpho.com
FR

Ductis GmbH
www.ductis.de
DE

Železničná spoločnosť Slovensko a.s.
www.zssk.sk
SK

Joint Stock Company Lithuanian Railways
www.litrail.lt
LT

RFI Rete Ferroviaria Italiana S.p.A.
www.rfi.it
IT

PKP Polskie Linie Kolejowe S.A.
www.pkp-sa.pl
PL

D'Appolonia S.p.A.
www.dappolonia.it
IT

Elbit Systems Ltd.
www.elbitsystems.com
IL

Facultés Universitaires Notre-Dame de la Paix
www.fundp.ac.be
BE

EPPRA
www.eppra.com
FR

Kingston University Higher Education Corporation
www.kingston.ac.uk
UK

SODERN S.A.
www.sodern.com
FR

Smiths Heimann S.A.
www.smithsdetection.com
FR

Instytut Kolejnictwa
www.ikolej.pl
PL

CEA Commissariat à l'Énergie Atomique
www.cea.fr
FR

Institut Franco-Allemand de Recherches de Saint-Louis
www.isl.eu
FR

TCDD - Turkish State Railways
www.tcdd.gov.tr
TR

MER MEC S.p.A.
www.mermecgroup.com
IT

Société Nationale des Chemins de fer Français
www.sncf.com
FR

Contact persons:

Mr. Vito Siciliano
Ansaldo STS S.p.A.
vito.siciliano.prof110@ansaldo-sts.com

Ms. Sonia Caviglia
Ansaldo STS S.p.A.
sonia.caviglia@ansaldo-sts.com