PROTECTRAIL

Newsletter

Introduction

Key Facts

Welcome to PROTECTRAIL, the FP7 project to increase the security of mainline rail transport in Europe. The project is co-funded by the European Commission that contributes EUR 13 million to the overall budget of EUR 21 million. PROTECTRAIL brings together 29 partners from eleven countries. These include industrial partners, such as security providers and railway manufacturers, as well as railway operators and users. Having six large railway operators on-board facilitates the cooperation between industry and users as well as guaranteeing the future market uptake of the security solutions developed in the project. Furthermore, PROTECTRAIL also engages with international standardisation bodies to share the knowledge developed in project. The project started in September 2010 and will run for 42 months until March 2014.

Why PROTECTRAIL

Today, we witness an increased demand for security. Railways in Europe need to be enabled to minimise the risk of terrorist attacks, as the Al-Qaida threats of the summer of 2013 show, but they also need to be enabled to protect themselves against other, less visible, criminal activity that causes expensive damage to our transport systems. These include for instance damage to railway infrastructure, like copper theft, or to rolling stock, such as graffiti. PROTECTRAIL aims to provide the tools that can help manage these security threats and that can prevent criminal activity.

Not reinventing the wheel but creating a modular architectural framework

PROTECTRAIL does not focus on inventing new security solutions. Rather, PROTECTRAIL takes existing solutions such as CCTV, or CBRN-E sensors, and makes them interoperable. The idea is to build separate components for a security system that can be plugged together and integrated in internal and external systems to be used by different operators, in combination with legacy systems, and in big and small networks. PROTECTRAIL envisages a model that is similar to a plug-and-play solutions that already exist in the IT sector today. Therefore, PROTECTRAIL develops a global, modular architectural framework, and much of the work of the project is to develop a flexibility of design, creating a system of systems approach that makes plug-and-play possible while at the same time allowing for innovation.

Testing selected security solutions

PROTECTRAIL also identifies and develops security solutions that respond to the needs of the railway users, based on a risk assessment. The solutions must be extremely reliable and function in real operating conditions, i.e. in bad weather, under bad lighting conditions, and in crowded areas. They must detect threats quickly without disrupting the daily flow of passengers or goods which would reduce the attractiveness of railways and they must not produce false alarms which could lead to unnecessary shut downs of the railway system. The solutions of PROTECTRAIL must be scalable and transferable to be used by a large variety of different operators and they are examined on ethical grounds. Finally, given the budget situation in many European countries, they must provide a real cost benefit. The selection criteria for the solutions developed are therefore tough. In order to make sure that the solutions do not work in labs only but also in real-life situations, PROTECTRAIL puts them to test in demonstrations. Based on the needs of the operators and on risk assessments, PROTECTRAIL developed real-life scenarios in which the solutions are tested. The tests that take place in Zmigrod, Poland, include situations that operators face, such as intrusion, criminal activities of staff, lost luggage, CBRNE detection. Two other demonstrations take place in Villecresnes, France, and in Sicily.

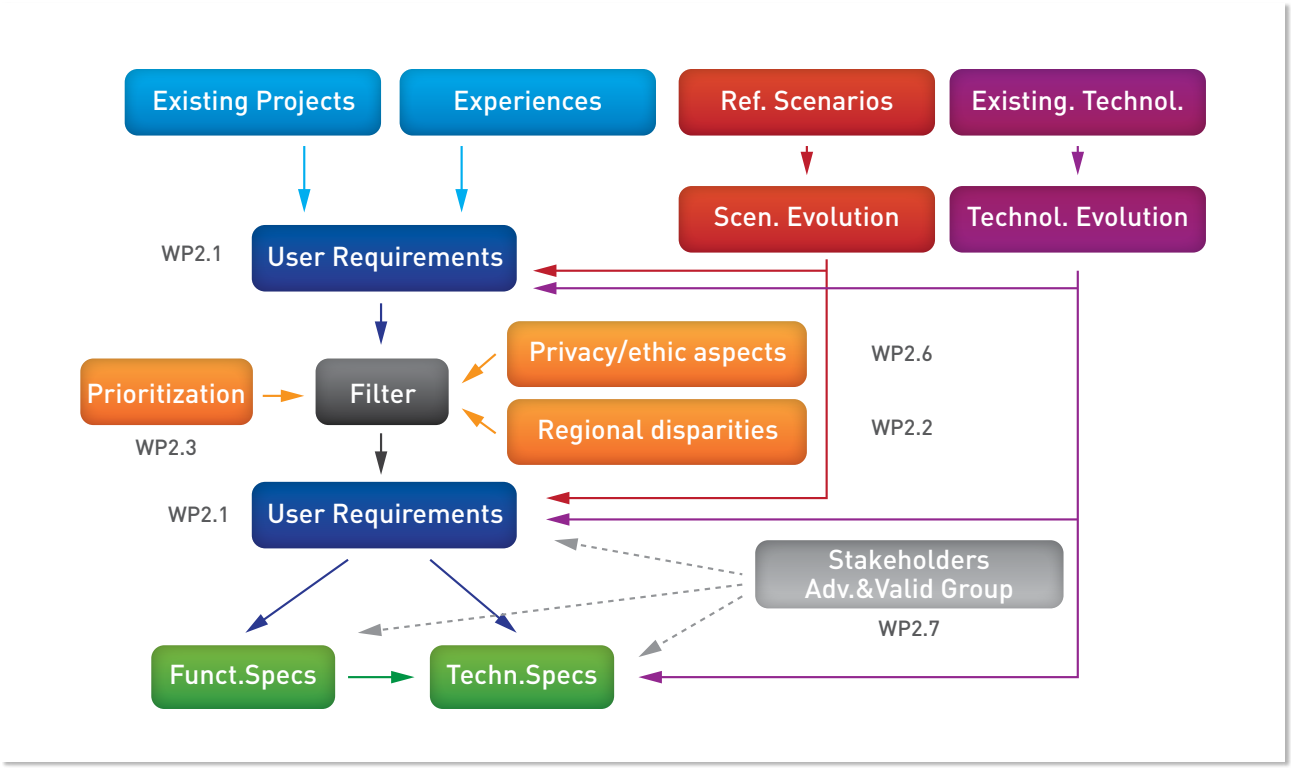
How PROTECTRAIL is structured

For better manageability, PROTECTRAIL splits the global railway security problem into asset specific security problems (submissions) for which it is easier to reach satisfactory solutions applicable and usable in different threat scenarios. Each submission covers significant areas of interest as indicated by a specific risk analysis and from user priorities. The work on these submissions is done in five technical subprojects (SPs): SP2 defines the functional and technical specifications for prevention, mitigation and crisis management. In SP3 and SP4 (for fixed assets and transported assets respectively) the feasibility of solving the identified railway protection submission through an efficient and cost effective integration of technologies is demonstrated. SP5 proposes a coherent architectural and design framework, and SP6 considers the political, economic, and socio-cultural aspects to drive future design for security strategies forward. You can read more about the work done in the 38 work packages and about the achievements of PROTECTRAIL in the following sections of this newsletter. Enjoy the read!

SP2 Functional and Technical Railway Security Specifications

Objective of sub-project2

The main scope of the SP2 is to generate a set of functional and technical specifications which meet the needs and priorities of railway stakeholders and which can help improve railway security policies and privacy rights. The activities of SP2 are spread over the entire life of the project. Like this the requirements



and specification can be modified to take into account possible changes in the environmental conditions or technological evolutions. In SP2 we also collect information and feedback from the European railway stakeholders on the various activities of each SP2 work package. Below you can find all SP2 work package activities and their dependencies.

Main challenge

The main challenge of SP2 is to synchronise all the activities of its work packages in order to obtain a single line of reasoning that would allow, starting from the identification of the stakeholder requirements and their prioritisation, to identify and refine the functional and technical specifications and a set of reference scenarios to be used as a starting point for all the activities of SP3 and SP4 while at the same time respecting all the applicable privacy policies. All the SP2 results are achieved by working closely with the major railway stakeholders both inside and outside the project.

Main findings

Our work in SP2 leads us to the following results: We identified and prioritised a structured set of security-related stakeholder requirements that contain the main current and potentially emerging threats for the railway system; we defined a subset of scenarios which provides details on security issues that were highlighted by the interviewed stakeholders; we conducted a socio-technical functional requirements analysis which aimed to highlight the various functions to be developed in order to satisfy the stakeholder requirements. The focus was put on the relationship between the various functions to explore the complexity of the various PROTECTRAIL missions. We also defined a set of technical performance specifications and technical and operational constraints to complement the identified functional specifications. Finally we analysed the regulation and privacy rights in order to provide guidelines for the implementation of viable solutions that include and respect privacy and the rights of the citizens.

Main benefit to end-users and industry

Our work in SP2 enabled us to identify the needs and the priorities of the major railway stakeholders in terms of security. From this information we derived the 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 that is useful for the implementation of security systems and able to meet the current priorities of the railway world.

Integration of physical assets

SP3

The objective of SP3 is to integrate physical and operational assets for the identified submissions of the overall railway security challenge, with the objective of demonstrating the feasibility of protecting a large set of fixed assets. These large fixed assets include for instance stations, buildings, structures, infrastructures, tracks, command and control as well as communications

systems, and rolling stock clearance at the depot. In SP3 we aim at integrating these technologies in a cost-effective manner into the PROTECTRAIL demonstration, thereby proving that they can be used by operators in Europe too.

Having provided the security technical and functional specifications for PROTECTRAIL, SP3 partners tested all the selected security solutions in labs and managed to give a proof of concept for all of them. After this proof, the majority of these security solutions is tested and validated in the PROTECTRAIL demonstration in Zmigrod. Of course, SP3 worked closely with the SP5 team to make sure the security solutions can easily be integrated and fit the architectural framework of PROTECTRAIL to make an easy integration possible.

We install a number of different security systems for stations and building control in SP3. CCTV services are installed with a unique situation display equipment

PROTECTRAIL

WWW.PROTECTRAIL.EU

for the control room. The CCTV system can deliver information about crowding on the platform. It also works with backward and forward tracking software that is installed and demonstrated. The CCTV system even has the capacity to do face matching and luggage reconciliation. Furthermore, SP3 tests explosive detectors, together with a system assessing the impact of a CBRN-E incident. A day-and-night camera system is installed which can track a suspect around the clock and in all weather conditions. Additionally we have specific capacities for automatic intrusion detection to control the track, tunnels and bridges. Access control also includes a biometric system that checks staff clearance and manages their access right. SP3 also considers issues of IT-security: we test the efficiency of an ICT protection for computer-based signalling systems. An IT-security tool manages the Zmigrod communications networks and shows its ability to detect any abnormal event that could be the result of an IT-attack. In order to allow communication in between all the security solutions, be they on-board or wayside, a high performance wireless broadband network system is deployed and assessed.

The impressive solutions list that is tested as part of SP3 shows that there are many technologies to protect the assets. At the time this article is written, Zmigrod includes already a high concentration of capacities. The visitors can find in a single site all of the proposed state of the art security solutions. A visit at the Zmigrod site therefore represents a unique opportunity for the end-users to understand how to protect the railway systems and to consider what solutions are applicable for their specific challenges in their operational context. To security providers from the industry, a visit is the perfect occasion to demonstrate their ability to integrate solutions in an interoperable manner.

Integration of transported assets SP4

In SP4 we concentrate on the integration of solutions to protect and analyse so-called "transported assets" such as passengers, luggage and freight. Interestingly, these transported assets could be both, targets of potential threats and means to attack the railway system. In SP4 we improve the performance of a number of security solutions and make them available for various use cases.

Passenger clearance control aims at improving detection of threats and abnormal situations on board or just before boarding. Here we work with "face matching and luggage reconciliation through RFID", a technology to re-conciliate a person with his luggage by detecting the luggage, and then verifying if the corresponding person is supposed to carry this luggage. We also work with a system that is made up of two modules: A detector for abandoned luggage that monitors a video stream coming from cameras to try to detect abandoned objects like an unattended luggage. It would also detect removed objects. The second module is a people on-board detector for intrusion and exist detection which monitors multiple video streams coming from depot cameras and tries to detect when a person is leaving the train through

either doors or windows or entering the train when not allowed for example during the night.

In SP4 we also develop a luggage clearance control system which aim at improving detection of threats in ordinary baggage. With current technology it is difficult to control an open-access system like railways because scanning luggage in a way it is done at airports is not feasible. SP4 develops a way to improve the detection of threats without disruption in mass transportation networks. The security solutions of SP4 include a system that detects explosive, chemical and radiological threats without contact and in a non-destructive way through the ULIS system which uses interrogation by fast neutrons with associated particle (API-FNA) and X-ray transmission. They also include a hand-held device to detect explosive gases and toxic gases in a luggage.

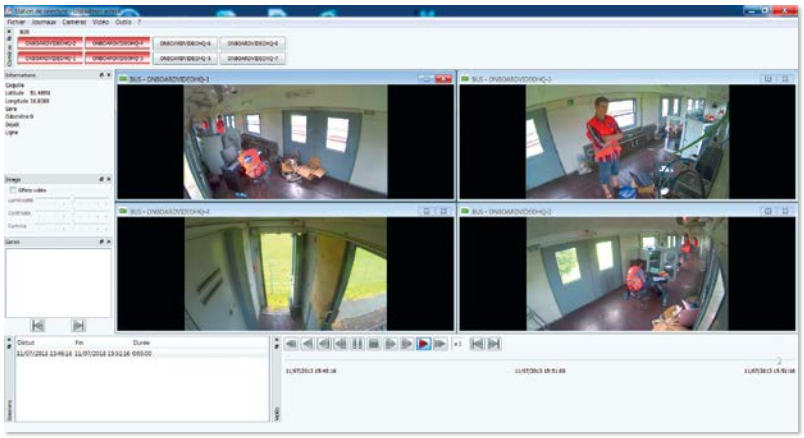
PROTECTRAIL also works on freight clearance control which aims at improving the detection and analysis of threats introduced into transported freight. For this we have a system that can sniff various gases through leaks or small holes in a container and one for gamma radiation detection. We also use a scanner for moving freight trains which detects gamma or neutron emission through X-Ray images.

Tunnel and fast tracks security is crucial in terms of ordinary crime as well as terrorism. PROTECTRAIL has selected several solutions that will be combined in a specific side demonstration focusing on best results in terms of alarms and false alarms rate. These include: CCTV infrastructure for video streams record, alarms management and replay; automatic intrusion detection on thermal images; thermal camera with a ruggedised video analytics device; tunnel entrance intrusion detection system; automatic detection of intrusion in tracks, tunnels and bridges; compact system with artificial intelligence; detection of radioactive, toxic and combustible gases, and a system that detects radioactive agent within passenger areas.

All these solutions were successfully tested in-lab in various representative conditions. They are integrated into the Zmigrod demonstration and on the Villecresnes site.

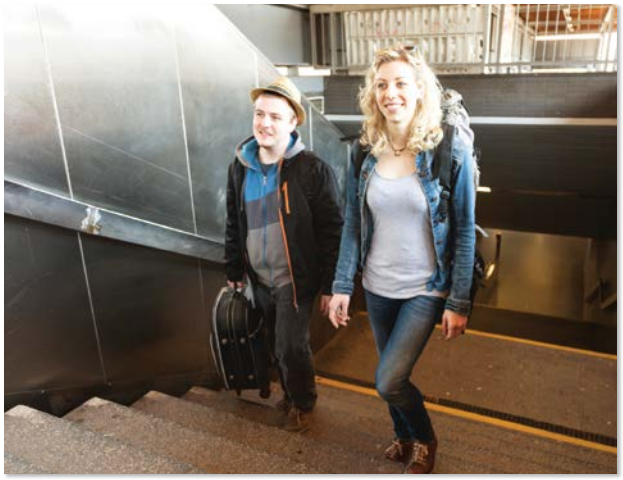
Global integration SP5

The objective of SP5 (Global Integration) is to propose a coherent Interoperability Framework which will ensure that from design to operational field acceptance, the proposed security solutions share the same relevant interfaces and constraints. This will allow a future-proof affordable deployment and demonstrate that complex and distributed security solutions integrating multiple security, communication and electromechanical subsystems from several industrial partners can successfully be integrated at the control and command centre, using modern Information and Communication Technology (ICT) approaches based on a Service Oriented Architecture (SOA).



Main Challenge

The primary challenge in implementing the vision outlined in the PROTECTRAIL project was the acceptance by all of the members to adopt a common design framework based on modern ICT approaches.



Additionally, given the geographic dispersion of the labs of PROTECTRAIL partners, a more agile and virtual approach to development and testing was required. The project team did not have the luxury of building a central lab to house all the equipment of the partners prior to demonstration, so the PROTECTRAIL Global Integration team introduced a secure, cloud-based, continuous integration environment that enabled members to test SOA software interfaces, application interactions, and re-use of various base services (e.g. GPS positioning, time servers, event brokers, etc.) from their own company labs.

Main Findings

The experience of PROTECTRAIL highlighted the need for more ICT enterprise experience in the rail industry. Many of the challenges of integration in the PROTECTRAIL consortia are also representative of the industry as a whole. The wide range of expertise amongst the partners exposed the general knowledge differential on Information Technology (IT) and Software Development domains in the rail industry, which historically has been more electro-mechanical engineering oriented.

This general lack of IT and software knowledge in the railway sector impacts the willingness and capacity to adopt standards and design principles that are commonplace in other industries. Additionally this lack of knowledge impedes the speed with which the industry can adopt new approaches that seek to reduce integration risks and the associated non-recurring costs.

Despite these industry realities, the PROTECTRAIL project team has found that members grew to understand more the advantages of adopting a more "plug-and-play" approach to incorporating new security functions, and are now aligning product and solution roadmaps, as well as influencing industry standards bodies to incorporate the principles of the PROTECTRAIL interoperability framework.

Main benefit to end-users and industry

The main benefit to end-users and industry of the PROTECTRAIL Global Integration activities is the influence and adoption of the PROTECTRAIL interoperability framework into the future product roadmaps of PROTECTRAIL partners, as well as the alignment of the PROTECTRAIL framework with international standards and industry organisations like the IEC, CENELEC, UIC, and UNIFE.

The PROTECTRAIL team has demonstrated that adopting a framework based on a set of existing standards, including standards from other domains, such as ICT, can make a positive impact on easing integration challenges and increasing the available security solutions in the rail market. This increase in available security solutions, which can be more readily integrated into the rail sector, helps drive down costs while increasing the capacity of operators and end-users to address the various threats to the travelling public and associated assets.

Future design SP6

Challenge of SP6

PROTECTRAIL is focused on demonstrating the added value of an integrated and combined approach to security in rail transport using state of the art technologies. However, the three PROTECTRAIL

demonstrations leave three open questions: 1) Can we be sure that the current security solutions will also be useful against future threats? 2) What is the price that we pay for the security measures in terms of social, political, and cultural aspects as well as of the performance of the rail transport sector, for instance for queuing and increasing railway fares? 3) How will today's solutions match a changing railway system with regards to freight and passenger volume and regulations?

In SP6 our challenge is to find security measures that have a good security performance in several possible future scenarios and have a good cost-benefit ratio, do not have (too much) negative influence on business performance, and are acceptable for passengers and society.

Objective of SP6

The objective of the SP6 'Future design for security' is to develop supporting tools that can be used to overcome the abovementioned challenge: We develop a vision of all the stakeholders in Europe on the rail transport sector for the next 10 to 20 years. Evolutions in key technologies, future demands and operational requirements will be considered in which the security constraints can be embedded. We also develop a software-based system consisting of factors that influence the rail transport system and that can be used to assess security measures; and we make a long term assessment of security measures for prevention, mitigation and crisis management. All these will help the rail sector to make informed decisions for their security policies and investments.

At the time of writing PROTECTRAIL had developed a vision on the future rail transport sector, including a large security section, and two methods to map the future complex rail transport system: one on asset level (station, track, train, etc.) and one on (national) rail transport system level. The vision and the two methods are being used for a long term analysis of relevant measures regarding prevention, mitigation and crisis management.

Main benefits

As the vision document was produced with the support of a broad set of relevant stakeholders and PROTECTRAIL partners it is an accurate tool on the future of rail transport and it can be used for planning and policy making. The asset-level method that we developed can be used for instance by a security manager of an asset to analyse a set of possible and relevant security measures for his specific asset. A policy maker or person responsible for a (part of a) rail transport system can use the method to have a structured way to assess all impacts of security measures on the whole rail transport system. Doing this for multiple measures one can get an overview of the pros and cons of these measures, which is the basis for decision making. These models offer the user a structured way (a process) and a tool to think about future security measures and their impact on the rail transport system broader than just security

The PROTECTRAIL Consortium

Name: PROTECTRAIL
Grant Agreement Number: 242270
Total Cost: EUR 21,775,289
EU Contribution: EUR 13,115,064
Start Date: 1 September 2010
Duration: 42 months

Coordinator:
Ansaldo STS S.p.A.
Via P. Mantovani 3-5 | 16151 Genova, Italia

Coordinator contact:
Vito Siciliano
T: +39 010 6552976
E: vito.siciliano.prof110@ansaldo-sts.com

Dissemination contacts:
Marie-Helene Bonneau
T: +33 1 44 49 21 43
E: bonneau@uic.org

Jan Steinkohl
T: +32 2 626 12 69
E: jan.steinkohl@unife.org