Topics in Safety, Risk, Reliability and Quality

Roberto Setola
Antonio Sforza
Valeria Vittorini
Concetta Pragliola *Editors*

Railway Infrastructure Security

Springer

Topics in Safety, Risk, Reliability and Quality

Volume 27

More information about this series at http://www.springer.com/series/6653

Roberto Setola · Antonio Sforza
Valeria Vittorini · Concetta Pragliola
Editors

Railway Infrastructure Security

Springer

Editors
Roberto Setola
Complex Systems and Security Lab
Università Campus Bio-Medico di Roma
Rome
Italy

Antonio Sforza
Department of Electrical Engineering
University 'Federico II' of Naples
Naples
Italy

Valeria Vittorini
Department of Electrical Engineering and Information Technology (DIETI)
University 'Federico II' of Naples
Naples
Italy

Concetta Pragliola
Ansaldo STS
Naples
Italy

ISSN 1566-0443 ISSN 2215-0285 (electronic)
Topics in Safety, Risk, Reliability and Quality
ISBN 978-3-319-04425-5 ISBN 978-3-319-04426-2 (eBook)
DOI 10.1007/978-3-319-04426-2

Library of Congress Control Number: 2015932663

Springer Cham Heidelberg New York Dordrecht London

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media (www.springer.com)

Foreword

September 11, 2001 has been a turning point in world history. The events of that day not only shook the whole world, but also prompted in a new era of terrorism. Firstly, attacks at the World Trade Centre and Washington were not solely an American domestic issue, but had a massive impact all over the world: it appeared that counterterrorism architectures by preventing, addressing, and thwarting further attacks were not adequate. Secondly, the inability to coordinate both information collection and integration among all the several involved agencies led to the failure in identification of actions that might provide attack prevention. Finally, the prosecution of terrorists required appropriate new laws: procedures and techniques of counterterrorism measures have been developed, step-by-step, over the years.

It was evident that terrorists' operations were primarily concentrated on the transportation sector. The reason is evident: destroying a symbol, i.e., an Embassy, is a clear message, but only a message, while heavy interference and destruction in mass-transportation with large number of people and goods lead to severe economic consequences. Accordingly, the development of countermeasures was concentrated in the travel control field: heavier immigration policies and border controls were gradually implemented; vulnerabilities of transportation systems were analyzed; clear awareness of criticalities was examined, and methods able to design, scale, and optimize protection were developed. Consequently, a wide number of approaches, aimed at reducing the negative impact of transportation risks on population's welfare and safety, as well as on national economy, were experimented. This whole procedure has led not just to economical expense but invested society as well: implementing Homeland Security (HS) obviously implies *intelligence*, so that personal *privacy* may be affected.

Terrorist attacks on 9/11 concentrated on the aerospace sector, and this also for the wide international facet of transportation aero-systems, with the result of large resonance on mass media. As a consequence, defense techniques were initially concentrated on airports identified as "main" vulnerable components. The development of security protocols implied the deployment of checkpoints to screen every passenger. However, adopting the same security procedure in mass transportation systems, especially in Railway Infrastructure Systems (RIS), is unreasonable. The reason is that mass transport systems, such as trains and subways, are open and wide geographically deployed assets, difficult to secure by nature. The adoption of airport-style security is impossible in reality. To date, turnstiles, video surveillance, and random checks have been the most common security measures, rather than those used in airports.

However, attacks as those of Madrid (2004) and London (2005) showed dramatically the attractiveness of terrestrial transport as well. Unfortunately, in this case the protection measures are not so simple to find. Indeed, especially for railway systems, one has to consider on one hand the inability to take up screening checkpoints, on the other hand the vulnerable nature of the assets. Accordingly, the study of appropriate countermeasures is an important issue. Even though the achievement of a standard is almost impossible, these studies represent an important starting point to customize specific solutions able to account for these different peculiarities, and are effective in improving the level of RIS protection and security.

In railway security, large attention should be focused on physical protection systems. In general, protection systems incorporate people, policies, and equipment used to secure critical infrastructure assets from malevolent acts. Despite increase in threat awareness and publishing of the best security practices, there is a lack of formal approaches for evaluating the effectiveness of decisions regarding the implementation of physical protection systems. Indeed, current assessment practices rely on compliance (i.e., presence of appropriate equipments) and performance-based approaches (i.e., evaluation of the consequences of successful attacks).

It is evident that Homeland Security is a must in our society, to be strongly implemented over all *system of systems,* with hardware and software complex interaction, which is the functional basis of our society. In this framework, transportation is the backbone of the economy. The railway network keeps people and goods moving across the country and around the world, and the urban subways today are the most efficient solution for the town mobility. While several valuable publications on airport, port, and road security are currently available, specific references about railway security are still very limited. To date, the RIS security topic is usually included as appendix or corollary in essays specifically dedicated to railway safety. In this context, the “Railway Infrastructure Security” book would contribute to fill the gap in the lack of specific manuscripts devoted to RIS security. It has to be noted that the book has been developed in the frame of the MEthodological Tool for Railway Infrastructure Protection (METRIP) project, co-funded by the European Commission, Directorate-General Home Affairs. Its philosophy is to assess issues and problems related to RIS security from the overall point of view adopting an all-hazard approach, hence not strictly limited to terrorist actions. Accordingly, the book can be of interest to a much wider audience.

The main features and the relevant issues of RIS, covered by the book and spread over its 11 chapters, are now summarized, in order to illustrate its knowledge contribution to the sector.

The entire scenario is clearly presented in the book with all the pertinent details. Protection of the critical infrastructure systems is a difficult problem, which has been widely tackled in the last 20 years by experts from different fields: security managers, university researchers, companies, etc. The main aim of the research activity on this topic has been devoted to develop a deeper understanding of the vulnerabilities of these systems, in order to provide efficient and effective strategies to reduce risks and consequences due to improper use and possible attacks. The book is focused on this problem, with specific reference to Railway Systems, which notwithstanding their symbolic and economic value, have not gained proper attention. To this aim, the book collects different experiences coming from international security experts, academic authorities, and leading railway service providers. Although incidents are always possible, in the railway field due to the volumes carried, the density of traffic, and the extent of offered services, the railway system is still one of the safest modes of transport. Unlike other typical critical assets that are equipped with access control (usually with physical barriers), the railway environment usually remains open to the public and clients alike.

Railway transportation exhibits characteristics that make it pretty vulnerable: trains make scheduled stops along fixed routes; their operations depend on people who have quick and easy access to stations and trains, with the result of a large number of access points. In this context it becomes necessary to define the concept of *Security* in *railway* and *metro transportation systems*, in order to enhance their protection level, while keeping their attributes of openness, extensiveness, accessibility, and affordability. This issue is extensively discussed in the book, covering the requirements of security for passengers and personnel at stations and on board, the protection of critical assets, as (but not limited to) the signalling and control systems.

The book continues, presenting an overview of the present challenges for security in railway systems, with a clear picture of the current scenario. The most relevant threats, experiences, best practices, and possible countermeasures are illustrated. Relevant analyses and experimentations are illustrated: starting from the experience gained by Ferrovie dello Stato Italiane that manages more than 23,000 km of rails, which adopted a mix of methodological, technological, and organizational procedures and tools; EAV company that manages a circular railway network in the western metropolitan area of Naples (Italy) analyzed current security problems, and proposed an optimization approach for the improvement of its network security; and Cityringen, a fully automated metro in the heart of the city of Copenhagen (Denmark), which has been planned, designed, and realized in order to satisfy the main security requirements by means of both vulnerability analysis and risk assessment activities.

Mathematical models, computational techniques, criteria, and options for choosing safety and security systems are widely included. A vulnerability assessment via synergic use of Crime Prevention Through Environmental Design (CPTED) and System Dynamics multidisciplinary approach is depicted, outlining the main physical, social, and environmental aspects that provide opportunity for criminality in railway scenario. Results of simulations reproducing different operative conditions are presented and analyzed. The design of a security system, in terms of number and position of the security devices composing it, is one of the main issues tackled in the METRIP project. The proposed tool chain allows to model the RIS infrastructure, attack scenarios, and protection technologies to generate qualitative and quantitative models. These are used to perform vulnerabilities analysis, formulate, and solve optimization procedures to determine the best design choices in the development of physical protection systems. The functional and logical architecture of the tool chain is fully described in the book, including the realization of a prototype to demonstrate feasibility and effectiveness of the proposed approach.

The four editors of the book have large experience in the different fields needed to manage the complexity of RIS security, providing complementary competences and allowing to analyze the problem from different perspectives.

Roberto Setola provides a holistic vision to the problem, exploiting his competence on Critical Infrastructure Protection. He is an associate professor in Control Systems, with large experience in modeling complex infrastructures, and design security systems. He supervised for the Italian Prime Minister's Office the Critical Infrastructures Group, and he has been the coordinator of three European projects on infrastructure security, being also the Director of a post graduate program in Homeland Security at Università Campus Bio-Medico di Roma. He has published seven books and more than 130 peer-reviewed papers on these topics.

Antonio Sforza offers his knowledge on analysis and optimization of networked systems. He is a university full professor of Operations Research, currently working on the application of network optimization models and methods in the field of critical infrastructure protection and smart city planning. The main focus of his latest research activity is on the identification of the critical points of a network, and the design of reliable infrastructures with effective security systems.

Valeria Vittorini contributes with her experience in the analysis of non-functional properties of dependable systems. She is a university professor of Computer Programming and Formal Methods. She has gained long-standing experience in modeling critical systems and specifically railway systems, for vulnerability, availability, and dependability analysis. She collaborated with Ansaldo STS Company in several research projects about railway throughout the last two decades.

Concetta Pragliola provides the concrete vision coming from the design and implementation of several RIS security infrastructures. She is working on railway infrastructure systems security since 2006: during this period she made security assessment on several worldwide railway infrastructures to verify their vulnerabilities, and to design security systems to protect these systems. She is the Ansaldo STS Railway and Metro Security system Manager since 2007. She has led several railway and metro security system design and realizations.

There is no doubt that the book provides detailed up-to-date information about the Security of Railways Infrastructures. The state of the art of research and experimentation in the area is fully covered, with appropriate illustration via citation of real attacks, results of prototype realizations, and improvement projects. The book covers the gap in the methodological and technical literature in this area, becoming fully appropriate for this sector.

Giorgio Franceschetti
Emeritus Professor
University ‘Federico II’ of Naples, Italy

Acknowledgments

The “Railway Infrastructure Security” book has been printed as a part of the METRIP (Methodological Tool for Railway Infrastructure Protection) project (http://metrip.unicampus.it). The METRIP project has been funded with the support of the “Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risk”, European Commission, Directorate-General Home Affairs, under the Grant HOME/2010/CIPS/AG/035.

This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use, which may be made of the information contained therein.

Contents

Introduction

Concetta Pragliola, Roberto Setola, Antonio Sforza and Valeria Vittorini

Abstract Critical infrastructure protection is a very hard problem, which has been widely tackled in the last 20 years by experts coming from different fields (security managers, university researchers, companies, etc.). The main aim of the research activity has been to develop a deeper understanding of the vulnerabilities of these systems, in order to provide efficient and effective strategies to reduce the risk of attacks and their consequences. The "Railway Infrastructure Security" book arises with the scope of improving this understanding with particular reference to the Railway Infrastructure Systems (RISs), which notwithstanding their symbolic and economic value have not gained the proper attention. To this aim, the book collects different experiences coming from international security experts, academic authorities and leading railway service providers. In this context, a significant part of the book is devoted to the presentation of the results achieved during the METRIP project (Methodological Tool for Railway Infrastructure Protection), partially supported by the European Commission, Directorate-General Home Affairs. This project, which arose with the aim of filling the gap observed in the awareness of the RIS security problems, provides methodological tools for the identification of RIS security needs and for the improvements of their protection.

C. Pragliola (✉)
Innovation and Competitvness, Ansaldo STS, Via Argine, 425,
80147 Naples, Italy
e-mail: concetta.pragliola@ansaldo-sts.com

R. Setola
Complex Systems and Security Lab, Università Campus Bio-Medico di Roma,
Via Álvaro del Portillo, 21, 00128 Rome, Italy
e-mail: r.setola@unicampus.it

A. Sforza · V. Vittorini
Department of Electrical Engineering and Information Technology (DIETI),
University of Naples Federico II, Via Claudio, 21, 80125 Naples, Italy
e-mail: sforza@unina.it

V. Vittorini
e-mail: valeria.vittorini@unina.it

R. Setola et al. (eds.), *Railway Infrastructure Security*, Topics in Safety, Risk, Reliability and Quality 27, DOI 10.1007/978-3-319-04426-2_1

Keywords Critical infrastructure protection · CIP · Railway infrastructure systems · RIS · Railway security · METRIP project

1 Introduction

Prevention and preparedness of risks in transportation system is crucial for homeland security. Among other things, it requires a proper analysis of the vulnerabilities of the assets, a clear awareness of criticalities, possible countermeasures and an adequate method to design, scale and optimize the protection. To this end, under the framework of Critical Infrastructure Protection (CIP), wide attention has been devoted to develop a deeper understanding of vulnerabilities and consequently provide solutions to act decisively in order to reduce their negative impact on, among others, welfare of population, national economy and safety.

In this context, mass transportation systems have gained large attention due to their symbolic value and mass media interest because they represent possible targets for criminals and terrorists. Immediately after 9/11/2001, air transportation sector adopted very restrictive and effective counter measurements aimed drastically reducing the risk. However, RIS security has not gained a comparable attention, even if very bloody episodes occurred (Tokyo, London and Madrid, just to cite three of the most famous). The point is that securing national and urban railway systems is a difficult by nature. RIS are generally heavy crowded, characterized by an open structure and are wide geographically deployed. For this reason, the adoption of airport-style security, as passenger screening, is practically impossible.

RIS security has to consider also different problems related to the protection of railways further than terrorism, such as vandalism, predator crimes and recently also the copper stealing problem. Moreover, the planned expansion of high-speed rail systems in Europe, Asia, and North America, with their high symbolic value, represents a strong attractive target for terrorists and criminals.

In spite of air-transport security where a vast and consolidated literature has been developed, the railway security is less considered in the technical field that is strongly focalized on the safety requirements.

This book would contribute to fill such a gap illustrating how to analyze criminal threats, design countermeasures and implement security strategies for RIS. To this aim, the book collects different experiences coming from academia, technology providers and railway operators. In particular, a significant part of the book will be devoted to the presentation of the results matured by the authors in the framework of the EU project METRIP (MEtodological Tool for Railways Infrastructure Protection), which, at the best of our knowledge, represents a first attempt of defining an overall and comprehensive approach to railway system security and network critical infrastructures.

The chapter is organized as follows: the first section briefly describes the problem of CIP, outlying the main policies put in place for CIP after the 9/11 tragic events. The second section focuses on the RIS security problem contextualized within the actual European legal framework. In third and fourth sections a description about the METRIP project, and the contents of "The Railway Security" book respectively are provided.

2 The Critical Infrastructure Protection

National defense, economic prosperity and quality of life have long depended on the essential services that underpin society. These fundamentals, which support every aspect of daily life—energy, banking and finance, transportation, vital human services and telecommunications—are Critical Infrastructures (CI) and in recent years, increasing attention has been paid to protecting them. Specifically, vast attention has been paid to develop a more in-depth understanding of their respective vulnerabilities and consequently provide solutions to act decisively in order to diminish their respective impact.

The USA has been one of the countries that grasped this priority since the mid-nineties. It was for just this purpose that President Clinton called into being the President's Commission on Critical Infrastructure Protection (PCCIP) in 1996 (President's Commission on Critical Infrastructure Protection, Critical Foundations 1997). The objective of the PCCIP was to create a strategy for the protection of the US infrastructures. These efforts were further emphasized after the tragic events of 9/11.

Although the initial PCCIP efforts were applauded, subsequent to 9/11 it became clear that a higher level of dedication in the CIP arena was necessary. A renewed sense of urgency was instilled with the establishment of the "Office of Homeland Security," the "Homeland Security Council" and, ultimately, the signing into law of the USA PATRIOT Act on October 26th, 2001.

The ensuing effects of the 9/11 attacks were not limited to the US. Following the structure outlined by the US, a growing attention towards CIP has begun to take roots across the globe. An example of this can be highlighted by the efforts of the European Union (EU). With an emboldened new approach to combat terrorism, the EU started its counteracts by adopting the Council framework decision 2002/475/JHA. Hardened even further, following the terrorist attacks in Madrid, this maneuver would prove to be the first of many, eventually culminating in the Council Directive 2008/114/EC of December 8th, 2008, focused on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

The 9/11 attacks obviously exposed some main vulnerabilities of the air transport sector. For this reason, in the last few years very restrictive countermeasures and security procedures have been adopted. The newly implemented line allowed a reduction in the number of successful attacks, but also illustrated a high social cost.[1]

[1] Actually, air transportation authorities are planning to relax some regulations (e.g., measures for the carriage of liquid in cabin, etc.).

Balancing the attention paid to all aspects of the transport sector, it continues to be both a priority and a challenge, as demonstrated by the several regulations, directive, reports, law decrees and guidelines issued worldwide.

Although these actions concerned the whole transport sectors, in Europe no specific Directive about the Railway Infrastructure System (RIS) security were established.

While aviation and maritime transportation sectors security are regulated by several acts (e.g., Regulations No 1082/2012, No 2320/2002, No 300/2008 for the aviation security and the recommendation 2010/159/EU, reports COM\2013\792, COM\2009\2, COM\2006\0431, Regulations No 324/2008, No 725/2004, Directive 2005/65/EC for maritime and port security), actually there is no specific European directive about railway security. At the same time, the long-term increase in the number and lethality of terrorist attacks on trains worldwide argues for continued security measures, chasing up the need for new and more suitable measures.

3 The Railway Infrastructure System in the CIP Arena

A brief analysis about European legislation in railway system showed that even though railway safety is regulated by several acts, there is no specific directives about RIS security.

The European Commission, in order to promote a market opening, to improve the performances, the interoperability and the safety of national railway networks, has put forward initiatives in the shape of packages of legislative measures, trying to lay the foundations of RIS safety since the First Railway Package, adopted in 2001 (Directives 2001/12/13/14/EC). Legislation about railway safety was introduced for the first time in April 2004, with the Railway Safety Directive (Directive 2004/49/EC) as part of the Second Railway Package.

The issue of railway safety is also addressed by the European Commission in the directives about transportable (eventually by rail) pressure equipment (Directives 2010/35/EU, 2005/50/EC) and about the transport of dangerous goods (Directives 2010/61 EU, 2008/68/EC, 2006/90/EC).

A change in the field of security legislation has been observed as a result of repeated terrorist attacks occurred since the early years of 21st Century.

Following the attacks in Madrid in March 2004, the European Union has proposed to intensify and enhance its action to counteract terrorism. In those years, the reduction of the vulnerabilities of CI became one of the objectives of the EU. An adequate level of protection must be guaranteed and the detrimental effects of disruptions on the society and citizens must be limited as far as possible.

To this end, the European Council of June 2004 asked the Commission to prepare an overall strategy to protect CI and the resulting outcome was the European Programme for Critical Infrastructure Protection (EPCIP). The EPCIP is a package of measures aimed at improving the protection of critical infrastructures across all EU Countries. The threats to which the programme aims to respond are not only confined to terrorism, but also include criminal activities, natural disasters and other causes of accidents. In short, it seeks to provide an all-hazards approach.

The Commission prepared a roadmap for the creation of a European Reference Network for Critical Infrastructure Protection (ERN-CIP). The aim is to connect existing European laboratories and facilities, in order to carry out critical infrastructure-related security experiments and test new technology, such as detection equipment. The Commission was also developing a Critical Infrastructure Warning Information Network (CIWIN). This Network is a multilevel communication system for exchanging critical infrastructure protection related ideas, studies and good practices. It will also serve as a repository for such information.

A key element of EPCIP is the Directive 2008/114/EC on European Critical Infrastructures (ECI). It establishes a procedure for identifying and designating ECI and a common approach for assessing the need to improve the protection of such infrastructures. Currently, the Directive's scope is limited to the energy and transport sectors in general.

Regarding to RIS field, no legislation and quality control inspection regimes are in place to improve railway transport security. For now, RIS security aspects are included only in two Regulations:

- Regulation (EC) No 1371/2007 of the European Parliament and of the Council of 23rd October 2007 on rail passengers' rights and obligations, in which Article 26 sets in place a "right to security" for passengers onboard trains and in stations;
- RID (Règlement concernant le transport international ferroviaire des marchandises dangereuses), the Regulation concerning the international carriage of dangerous goods by rail.

In spite of air-transport security where a vast and consolidated literature has been developed, the railway security is less considered in the technical field that is strongly focalized on the safety requirements. To date, turnstiles, video surveillance and random checks have been the most common security measure in RIS, rather than airport protocol, which deploys check points to screen every passenger.

Several eminent and renowned transport administration agencies are looking for best practices in order to improve safety/security and increase return on their investment. To mention one, the Amtrak Security Program BASE (Baseline Assessment for Security Enhancements) has been designated in 2012 as a gold standard by the American Transport Security Administration.

Random security measures such as VIPR (Visible Intermodal Prevention and Response team) operations, passenger baggage screenings and canine explosive detection program, were highlighted as leading to the success of the Amtrak security program. Despite these remarkable foundations, a universal global adoption of a golden standard usually represents an almost unobtainable level of security, because vulnerabilities are inherent within the design of the RIS itself.

However, these studies represent an important starting point to customize specific solutions able to account for these different peculiarities and are effective in improving the level of protection and security in RIS. On the other hand, the inability to take up screening checkpoints, the vulnerable nature of the assets, the catastrophic effects (economics, international and national politics, public opinion, media) of possible attacks, can explain why RIS still represent a fashionable target for terrorist assailants.

As pointed out by the Mineta Transportation Institute's National Transportation Security Center (MTI/NTSC) experts, the psychological effect of an explosion on the train would be enormous. A successful attack can deliver high body counts (decidedly greater than in a bus attack), significant disruption, dramatic images and enormous publicity; all highly desired results sought by terrorists. Data provided by MTI illustrate from 1970 to 2011, 2,927 attacks against public transportation systems were committed. Of them, about 48 % were carried out on buses, while 43 % were perpetrated against RIS.

Even though the number of attacks targeting buses is greater than those related to RIS, the lethality is higher amongst RIS targets (5.3 Fatalities Per Attack [FPA] on RIS vs. 3.4 FPA on buses).

Moreover, the planned expansion of high-speed rail systems in Europe, Asia, and North America, (with their high symbolic value) represent a strong attractive target for terrorists. The notes confiscated after the Osama bin Laden raid, which detailed ideas for derailing trains, further confirms the value of RIS targets.

In addition, the open and accessible design, heavy crowds and basic reliance for survival within the cities all serve as contributing factors in deducing why the RIS is considered a soft target for criminals and terrorists. Recognizing these vulnerabilities, it is easy to understand why there is a need for a commitment towards analyzing and improving rail security.

It is also important to consider that terrorists tend to be imitative and subsequently try to replicate attacks (targets, tactics, techniques) considered "successful". For example, the attacks in Madrid, London and Mumbai were considered major terrorist "successes," thereby making the likelihood of copycat attacks more probable. However, terrorism is not limited to emulation. Terrorism is a dynamic phenomenon and has demonstrated an increasing ability to adapt to counter-terrorism measures and political failures. Terrorists are consistently developing new capabilities and improving the efficiency of existing methods (e.g., cyber-terrorism; Chemical, Biological, Radiological and Nuclear weapons, CBRN).

In this context, an effective protection strategy has to be based on the development of tools using quantitative measures of the criticality levels of single assets and/or of the entire system. A clear awareness of criticalities can help to improve existing and discover new and more suitable counter-measures. These efforts compliment the primary objective of METRIP project.

4 The METRIP Project

METRIP—MEthodological Tool for Railway Infrastructure Protection, is a 24-month project (Dec. 2011–2013) cofunded by the European Commission in the framework of the European Programme on Critical Infrastructure Protection (CIPs), addressing the programme theme "Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks".

The project stems from a close collaboration between the academic community and the industry. Ansaldo STS, a leading technology company operating in the global Railway and Mass Transit Transportation Systems business, and the University Campus Bio-Medico of Rome, specifically the Complex System and Security Lab (Coserity) as leading Italian research institutions on Homeland Security and CIP, were partners of the project. Kent Business School and Ente Autonomo Volturno (EAV), a company operating in railway transportation, were associate partners. The Department of Electrical Engineering and Information Technologies (DIETI) of University Federico II of Naples, and specifically the research groups headed by Prof. Antonio Sforza and Valeria Vittorini, where in charge of Ansaldo STS for the development of the METRIP methodologies and prototypal tool.

METRIP project partners shared the idea that the issue of protecting a RIS can be addressed just performing a deep system analysis (in terms of assets, attacks and protections) and using "ad hoc" computer science methodologies for the design of an effective protection system.

Objective of the METRIP project is the development of methodological tools aimed at increasing the protection of RIS, with a specific focus on urban mass transportation. Our belief is that it can be reached by a decisional process composed by activities and tasks related to: statement of the problem, quantitative evaluation of the vulnerabilities and criticalities in RIS, evaluation of the relationships among system assets and attack scenarios, development of smart tools for prevention and detection of attacks.

The different activities and task were arranged into Work Packages (WP), and carried out by the partner's collaboration. A brief description of the activities related to each WP follows:

- WP1, *Data collection and analysis about railway infrastructure protection and related directives*, is devoted to define a framework of the problem under investigation, in terms of European and National (Italian) directives for protection of a RIS, together with the state of the art of the already developed project in the field. Hence, its main aim is performing a gap analysis and identifying best practices and real needs of EC in terms of RIS security requirements.
- WP2, *Analysis of a railway infrastructure system*, is devoted to model the RIS and its assets through a graph/network representation to be used for the quantitative evaluation of vulnerability and criticality parameters. Hence, its main target is the identification of the most critical point of a RIS on which the protection has be to focused.

- WP3, *Classification of threat and attack scenarios*, is aimed at performing a classification of the attacks against a RIS, highlighting the spatial and temporal dimension of an attack. An innovative approach based on a graph/network representation of the attack scenarios will be proposed to evaluate the behaviour of the system. WP3 is also devoted to surveying the protection system to be used in protecting a RIS.
- WP4, *Evaluation of the relationships between railway system assets and attack scenarios*, is devoted to perform a joint analysis of the two networks (railway system and attacks) with the aim of evaluating the interaction between RIS and attacks to evidence their temporal-spatial correlations. The idea is to study the attack scenarios to find the most involved assets and to evaluate simultaneous attacks involving more assets at the same time. One of the output of this study is the definition of cross table for system assets and attack scenarios.
- WP5, *Development of models and methodological tools to support the design of a protection system*, is the core WP of the project. It collects the results of the previous activities to develop a decisional tool prototype able to identify the critical assets within a RIS (or the critical points within an asset) and to choose and locate the protection devices. During this WP, the proposed approach and methodologies will be validated on the real case of an urban railway line in the metropolitan area of Naples, managed by SEPSA, associate partner of the project.

Briefly, the METRIP project addresses the problem of identifying the most critical points of the RIS, defining attack scenarios and detecting them on the base of a quantitative measurement of the vulnerability of the assets and an effective location of the protection devices. The key goal of the approach will be the implementation of prototypal smart decisional tool capable of:

I. Suggesting type and location of protection devices in order to maximize the protection effectiveness according to the available resources.
II. Evaluating effectiveness of a protection system according to the given inputs (RIS and attacks).

5 The Railway Infrastructure Security Book

At the best of our knowledge, there is no book specifically devoted to railways infrastructure security. There are several books on railway safety and railway engineering, and some of them consider, marginally, the problem of the railway security, whereas for other critical transportation infrastructures the literature is more consolidated. Hence, this book could help to cover such a gap.

Our belief is that a monograph addressing key issues in the protection of the railway system, will enhance understanding of the area by key stakeholders and will facilitate further research by offering a consolidated view of crucial areas of interest.

The target audiences for this monograph are researchers and decision-makers in the field as well as advanced undergraduate and graduate students, security managers, law enforcement, railway operators, technology providers interested in critical infrastructure protection or selected aspects thereof.

The book is the results of the collaboration of Italian and international security experts, academic authorities and leading railway service providers, that shared their own competence, knowledge and experience gained through their work in the security field. The book is organized as follows.

Dr. J. Colliard, Head of security division of the International Union of Railways (UIC) is the author of the Chap. 2. It is devoted to illustrate the security issues that affect modern railways systems worldwide. The Chapter will overview the present challenges for security in railway system, illustrating the most relevant threats, experiences, best practices and counter measurements.

The Chap. 3 by Dr. Franco Fiumara, Head of Security Directorate of Ferrovie dello Stato Italiane, illustrates the experience of FSI that manages more than 23,000 km of railways. Dr. Fiumara illustrates how the adoption of a mix of methodological, technological and organizational procedures and tools allowed a concrete reduction of the security related episodes.

Chapter 4, by Università Campus Bio-Medico di Roma, illustrates some interesting results inferred analyzing more than 500 security-related episodes in the railway infrastructure scenario. The data retrieved from the analysis, were after used as input for a simulation model. The proposed model is founded on CPTED Crime Prevention Through Environmental Design (CPTED) approach and System Dynamic method, in an effort to understand which are the elements and features that make railway targets more or less attractive to terrorists.

Chapter 5, written by Eng. Francesco Murolo, consultant of Ente Autnomo Volturno (EAV) and Eng. Arturo Borrelli of EAV, with the support of the operations research group of DIETI, describes a metro system that operates in the metropolitan area of Naples and highlights its security needs.

Chanan Graf of G Team Security Ltd, a leading Israeli consulting firm specializing in mass transit and railway security, writes the Chap. 6. Throughout 2000–2005 the Israel Railways was coping with a sustained threat of suicide terror that was part of the terrorist suicide campaign of the second "intifada". In this chapter the company shows how they responded by developing a security strategy that was designed to allow a continuity of rail services while providing enhanced level of security for the passengers.

The next chapter, Chap. 7, written by Ansaldo STS, illustrates some of the most relevant technologies able to support the design and the implementation of effective railways security systems.

Chapters 8 and 9, by the research group of DIETI, are devoted to the presentation of the methodologies at the base of the tool proposed in the METRIP project. The development of the methodologies presented in Chap. 9 have also seen the involvement of Eng. Stefano Starita of University of Kent.

To this aim, the Chap. 8 illustrates a specific language developed to capture the essence of railways security in terms of targets, instruments and threats.

Vulnerability and protection modeling and related issues in designing for railways security are analyzed. A model-driven approach to critical infrastructure protection and a model-driven framework able to support the automated generation of formal models for vulnerability analysis are presented.

The Chap. 9 considers the problem of optimal location of security devices inside a RIS asset in order to maximize their effectiveness in terms of covered area, taking into account constraints concerning device cardinality, points of interest and multiple coverage of an area.

The Chap. 10, written by Eng. Concetta Pragliola and the research group of DIETI, is devoted to the presentation of the METRIP prototypal tool, implemented as a tool chain which integrates the methodologies presented in Chaps. 8 and 9. The chapter illustrates its functional and logical architecture and describes the realization of a prototype to demonstrate the feasibility and effectiveness of the METRIP approach.

Chapter 11, by The Kent Business School University and Eng. Claudio Sterle of DIETI, is devoted to the application of optimization models to identify, forficate and design a reliable railway system, defined as a set of assets.

Finally, the Chap. 12 by Mr. Lund by Metroselskabet presents the new metro line in Copenhagen, Cityringen. It is a fully automated metro in the heart of Copenhagen and in the chapter the main security constraints and requirements in Mass Transit transportation systems, through vulnerability analysis and risk assessment activities are addressed.

6 Conclusions

The “Railway Infrastructure Security” book addresses the issue of increasing critical infrastructure protection in transportation systems, with a specific focus on RIS. Nowadays RIS, in particular the ones operating in urban area, due to their intrinsic value and to difficulties in guaranteeing their protection, can be considered among the most critical infrastructures.

The idea of this book arises from the awareness that even if much has been done from the research, operational and technological point of view in the field of the railway system protection, much of the studies do not explicitly take into account several important features, such as the correlation among RIS assets and single and multiple attacks. Meaningful impacts in the field of security for mass transportation system could be achieved if our awareness about theses aspects is increased.

To reach this aim it is necessary to put together experiences coming from different fields and build a methodology for the quantitative measurement of the criticality of the RIS assets and the identification of the most critical ones, the definition of a strict intervention strategy and the choice of type, technologies and locations of the protection system.

From this point view, this book could be a starting point for the definition of several guidelines for shared security requirements for RIS at European level.

Hence, in our opinion it will also significantly increase the awareness of railway managers and operators in prevention and preparedness to risk attacks in RIS, so contributing in the future to have safer railway systems and, to increase the sense of safety of urban and national railway system users.

Towards Integrated Railway Protection

Jacques Colliard

Abstract Since their inception, railways have been built upon the need for transport to be as safe as possible. Although incidents remain a fact of life in railway field due to the volumes carried, the density of traffic and the extent of services offered by railways, rail transport remains one of the safest mode of transport. However, another threat is jeopardizing the railway sector: crime and terrorist. Over the past 10–20 years, security issues have increasingly come to the fore, requiring strong sector action. This chapter presents a briefly overview about the present challenges for security in railway system. It provides a clear picture of the current scenario illustrating the most relevant threats, experiences, best practices and possible counter measurements all matured by the experience of UIC, in about one century of activity in the railway sector.

1 Railway: Constantly Striving for Safety

Since their inception, railways have been built upon the need for transport to be as safe as possible. As technical performance has improved and the significance of railways as a mode of transport has grown, rail managers have constantly striven to improve overall safety standards as the bedrock of the rail system's reliability and efficiency, their only limits being technology and funding. Their achievements are impressive, and, although the volumes carried, the density of traffic, and the extent of services offered by the railways mean that safety incidents and accidents remain a fact of life—coincidental multiple occurrences in a short space of time indeed sometimes prompting us to believe that "troubles always come in threes"—rail transport remains one of the safest, if not the safest, mode of transport. Railways' organizational structures, trained staff and, more broadly speaking, human factors approach, and its deployment of ever-better technologies enable more efficient use

J. Colliard (✉)
International Union of Railways, 16 Rue Jean Rey, 75015 Paris, France
e-mail: colliard@uic.org

R. Setola et al. (eds.), *Railway Infrastructure Security*, Topics in Safety,
Risk, Reliability and Quality 27, DOI 10.1007/978-3-319-04426-2_2

of networks and their potential, all contributing towards maximum transport safety. Rules and regulations are already in place and continue to develop, becoming ever more precise and applying to all sector stakeholders, whether infrastructure managers, railway operators or even service-providers and contractors working in the railways.

2 The Emergence of Security

Over the past 10–20 years, security issues—meaning the impact of negative or anti-social behaviour, crime and terrorism on the railways' existence and business—have increasingly come to the fore, requiring strong sector action. Unlike in the field of safety, this action cannot and must not be autonomous, but rather must be in support of and in partnership with the national authorities, which remain in overall charge of the security of people and goods on their territory. It is not a question of the rail sector deputizing for the state in fulfilling the latter's sovereign responsibilities, but rather of the railways integrating a number of constraints, rules, and commitments (in the shape of staff and financial resources) into the way they do business in order to allow an effective partnership to flourish under the state's leadership, ensuring a sufficient standard of security vis-à-vis customer expectations and rights.

The first difficulty arises from the fact that the world of transport is by its nature a world in motion—that is its primary vocation—and that the administration of a state (whatever form it takes: centralised, decentralised, regionally-devolved, etc.) remains the administration of a territory, of geographic areas, of places: the security of these places must thus combine with the security of transport which allows travel from one place to another. Rail transport can only play its vital role forging bonds in the economic, social (urban and regional transport especially) and regional-development (regional, long-distance and high speed transport) spheres if all internal stakeholders fulfil their security roles, in partnership with public authorities and as an extension of the action taken by the latter under the laws and regulations in force. Naturally, this role involves intervention in the event of security problems, but it can also—indeed may most of all—involve the implementation of a policy of prevention, protection and deterrence intended to minimise the number of acts or situations requiring immediate intervention on the ground. These latter points are vital for the rail sector's image amongst the general public, customers, the media, etc.

3 The Transport Environment

From the rail sector's perspective, infrastructure managers and operators agree that the two preceding aspects are vital since they fall under their sphere of responsibility—wholly as concerns safety, and partly as concerns security.

From the customer's perspective, the issue is more complex, since it is not so much a matter of legal liability for the execution of a contract as the idea that once one entrusts or delegates one's transport to a company or organisation, this latter must fulfil its task faultlessly. To this extent, the rail sector also needs to take on board other customer expectations, such as allowing for and managing random external events for which there may be no malicious intent or culprit, e.g. extreme weather conditions or meteorological hazards impacting on infrastructure or operations.

The sector must adopt an "all hazards" vision since that is what customers demand, even though the sector can and may only act in response to certain aspects. In this regard, it is vital to communicate prior to, during, and after operating incidents with a bearing on safety, security or other factors.

Crisis management and resilience

All the efforts deployed by the sector are intended to reduce as far as possible the number of incidents and accidents, whether intentional or random. Since it is self-evident that no blanket guarantee can be given that nothing will happen, the sector must nonetheless make preparations to manage situations disrupted by these incidents or accidents and ensure the resilience of the rail system in order that services may resume as soon as possible, even if they temporarily run at a reduced or downgraded level pending a definitive return to the normal situation.

Even if it is conceptually difficult both to organise things such that adverse events do not happen and simultaneously make provision for how to respond when they do, this two-pronged strategy is nonetheless vital.

Regularly conducting drills with the emergency and first-response services is essential for various reasons. The first is to teach different organisations, each with their specific rules and mindsets, to communicate effectively and act without delay in joint or at least joined-up fashion when responding to an emergency. The second is that the rail environment presents hazards for the uninitiated and those untrained in its constraints and particularities.

What is railway infrastructure security?

The definition of security as the rail sector's response, in partnership with the public authorities, to malicious intentions or acts, is a very broad one and covers extremely disparate realities and constraints, between which a choice must be made or which must be combined in an overall strategy to offer customers and staff the responses they expect.

4 Everyday Security in the Railway Scenario

When we think of security, we mostly think of terrorist attacks targeting transport—whether everyday commuter services or high speed trains—as a way of destabilising governments. However, we must not neglect everyday offences such as graffiti, vandalism and antisocial behaviour, which create delays and disruptions and which harm the image of public transport, preventing those who most rely on it from using it to remain connected to the rest of society.

Security is very often to the forefront of people's minds when choosing a mode of public transport for a journey, and this concern needs to be taken on board, since for many people the fundamental freedom to come and go as they please is underpinned by the ability (whether subjective or objective) to use public transport. Alongside long-distance transport and the high speed systems developed in various countries, everyday transport represents a social and economic challenge of the first order.

The matter becomes complicated when we start trying to distinguish between objective security and feelings of security. A UIC study conducted some years ago into major stations (in London, Paris, and Brussels) highlighted some remarkable aspects. When asked to define what they considered a particularly secure place, a place where nothing could happen, most travelers cited military bases, embassies, etc., that is places where the coordinated deployment of technical and human resources to protect and monitor on a massive scale (with all the associated constraints) rendered any security breach or attack impossible or so unlikely that it was unworthy of consideration. However, when the same travelers were asked to name a place in which they felt particularly secure, they mentioned their home, where they went on holiday—places where there were no specific external constraints in place but where they did not imagine anything could happen to them.

Railway companies' security policies must distinguish between what is more a matter of objective security (video protection, specialist uniformed staff, technical monitoring systems, etc.) and what is more a feeling of security (cleanliness and agreeableness of facilities, customer service staff in company colours, etc.). Of course they have to involve themselves in both, level of security and feeling of security, and remain in touch with the clients in order to define the priorities accordingly to their requests.

In addition, all the measures taken—particularly when they result in constraints on customers—must be understood and accepted by customers: no security policy can survive if the measures it provides for are not accepted by customers. Beyond this, the effectiveness of security policies will be boosted if the travelling public backs them and plays an active part in ensuring its own security: remaining vigilant, reporting unusual situations, unattended objects, etc.

5 Personal Freedom and Collective Security

Introducing security restrictions for passengers, particularly in publicly-operated urban or other everyday transport systems, also raises a problem of principle, one which is variable according to the political and institutional make-up of each country, that is, the balance between personal freedom and the need for better collective security.

Whereas a demonstrable terrorist threat may necessitate the taking of strict emergency protective measures, which may be coercive in their application, everyday security must for its part be underpinned by clear principles where each party's rights and obligations are defined.

This issue has arisen in particular with regard to video protection systems, specifically the permitted retention period for recorded material, the authorised viewers of this material, and under what circumstances and with what controls it may be viewed.

It also arises in the legal and technical division of labour between the public authorities in charge of security and their various partners such as railway companies' in-house security services and private contractors allowed to work on or monitor railway property.

6 The Terrorist Threat

Their extent, complexity, and impact on everyday life mean the railways are a target for domestic or international terrorism, and we do not need to recall the attacks in Madrid Atocha, London, the Russian Federation, India, and elsewhere. Constant allowance must be made for this threat, and only close collaboration between the services of the state, particularly intelligence services (which are tasked with gauging the threat to the country) and railway companies (which are aware of their own vulnerabilities) can allow any headway to be made.

A probability-based analysis such as may be used in safety management cannot apply in the same way when the task is to counter the acts of individuals or groups with significant intellectual and financial wherewithal, whose singular determination is deployed in support of a strategy which evolves in tandem with the policies developed to protect against it.

Though anti-terrorist strategy feeds off past experience, it must constantly take account of new threats and adapt to them.

The particularity of the railways, given their extensive infrastructure and the significant traffic flows they carry, requires them to develop their own strategy, since the examples of other transport modes (airlines, for instance) can only be followed to a limited degree and in very specific circumstances, otherwise the efficiency and capacity of rail transport would be compromised. The question arising is whether significant flows can be securely monitored without jeopardising the atmosphere, duration or cost of carriage by rail.

7 The Cost of Security

Since security does not obey probability-based reasoning, it is difficult to assess the efficiency of security measures, impossible to establish a direct mathematical link between the money spent and the outcome in terms of the number of offences committed, culprits arrested, etc. It is difficult enough even to gauge the real cost of security, beyond the cost of the staff and infrastructure directly allocated to this task.

It is particularly difficult to gauge the effect of prevention policies, the goal of which is to avoid malicious acts being committed.

It would perhaps be useful to reason in terms of a feeling of security. That would involve, as some railways do, regularly questioning both customers and those reluctant to travel by train to assess how important feelings of security or insecurity are in their decision and in the image they have or will retain of their journey and the rail-sector stakeholders which executed it.

In any case, it remains to be clarified what is the carrier's responsibility and thus included in the cost of carriage as paid by the user, and what is the public authority's responsibility and paid for by the taxpayer. Here again, the challenge is also the terms of competition between transport modes.

8 Security of Stations: The Challenge of Joined-Up Thinking

Stations are set to play an increasingly complex role. Initially solely transport-focused, over time they have become places where people live their lives, and form part of the urban environment. Their long opening hours mean that at some times of day they are the only building open to the public when all others are shut, and are thus frequented by various groups and categories of people, whose goals in using or occupying them are not necessarily the same. The development within stations of bigger and bigger retail areas, of which high-street shops are a particular feature, creates other everyday security issues, and suggests we need to clearly define the roles of the various security players for each area of the station affected. It is logical that a security guard working for a railway's in-house security service should come to the aid of passengers on a platform, though the police of course retain jurisdiction, but what about being called to assist with a security incident in the retail area of a station—perhaps between people who are not even there to catch a train?

Moreover, major termini are also multi-modal transport hubs served by various transport companies at any one time—these may not share the same view or analysis of their security commitments in terms of policy or financial outlay, which may again raise issues of consistency.

Lastly, within the European Union, the ongoing development of community law and the adoption of the Fourth Railway Package mean that 1 day, even within "the railways" in the narrowest sense, stations could 1 day simultaneously host trains from different companies, of different nationalities, incumbents or newcomers. There are already an increasing number of such players operating in the same place at the same time, a number set to increase further under the Fourth Railway Package given its emphasis on boosting competition between rail-sector players. The challenge will be to ensure consistency between their operations and security policies, and to avoid security becoming or causing a distortion of competition between them.

Consistency in managing the security of a space comprising various locations, each of which obeys its own logic, and playing host to stakeholders who alternate between being collaborators and competitors, is becoming a major challenge, since stations, as well as being multi-modal, are also increasingly multi-stakeholder.

9 Consistency at European and International Level

The issue of consistency already raised with regard to stations also extends to international traffic, which is certain to prove a source of traffic and railway business growth, particularly due to the development of high speed systems.

Guaranteeing a "sufficient" level of security throughout the journey in international traffic may convince people to travel by train rather than another mode.

Alongside this "commercial" argument, within the European Union there are the provisions of Regulation (EC) No 1371/2007 of the European Parliament and of the Council of 23 October 2007 on rail passengers' rights and obligations, published on 3 December 2007, article 26 of which makes the following provision: Personal security of passengers: "In agreement with public authorities, railway undertakings, infrastructure managers and station managers shall take adequate measures in their respective fields of responsibility and adapt them to the level of security defined by the public authorities to ensure passengers' personal security in railway stations and on trains and to manage risks. They shall cooperate and exchange information on best practices concerning the prevention of acts, which are likely to deteriorate the level of security."

Here again, then, consistency needs to be sought, in a shape which remains to be defined, in order to guarantee the involvement of domestic and international players throughout the journey; this consistency cannot merely be limited to an array or succession of bilateral agreements such as those developed for specific infrastructure (e.g. the Channel Tunnel, etc.).

10 Specific Aspects of High Speed Systems: Risks and Opportunities

What has been said for major stations and international traffic is naturally also true of high speed systems, with some specific aspects and limitations.

As regards terrorism, though the most notorious recent acts have tended to strike at urban networks, high speed rail definitely offers an attractive target, given what it represents.

Firstly, it is an important symbol of technological development in industrialised countries, attacking which guarantees immense political attention and media coverage of the acts perpetrated and the culprits thereof (or those claiming responsibility).

Beyond that, any safety-critical consequences of such acts risk being magnified by the speed of the train (obstacle on the track, potential derailment, etc.).

Travellers on high speed services have a legitimate demand for high-quality service due to the highest price.

If a local train is graffitied or looks the worse for wear, the least-worst solution for the operator may be to continue running it nonetheless, as long as it does not present a safety risk, since cancelling such services would create chaos in terms of service punctuality. At the same time, travellers will use such trains because they do not really have a choice, even if they feel uncomfortable doing so, that is, they feel the opposite of a feeling of security.

What passengers will tolerate for local services they will not tolerate for high speed.

Set against this, the high speed rail system also offers helpful opportunities: the speed with which it is developing means there is always new-build or upgrading going on, allowing security of operation to be integrated upstream as one factor in quality of service, rather than adding-on measures or operating restrictions post-fact.

A complex balance must therefore be struck. Railway security, preventive action and anti-terrorism form a whole: passengers have a right to travel in security both in daily travel and on high speed services. However, the high speed sector presents specific risks calling for a specific and tailored response. High speed rail represents a very significant investment by society and thus requires protection. At the same time, the rapid roll-out of high speed services in many countries means that security issues can be integrated upstream in the design and management of such systems, bringing maximum effectiveness at an optimum cost: security is one part of service quality, not an additional constraint imposed post-fact.

11 UIC Involvement

UIC was founded in 1922 by governments seeking to "create a permanent conference of railway administrations to harmonise and improve the conditions governing the establishment and operation of railways with regard to international traffic".

UIC currently has almost 240 members on 5 continents, including integrated railways, infrastructure managers, rail and intermodal operators, and service companies.

UIC's chief task is thus to:

- promote rail transport at world level,
- promote interoperability between rail systems,
- develop and facilitate all forms of international cooperation between its members,

- support its members in their efforts to develop new markets and new areas of business,
- propose improvement pathways for the technical and environmental performance of railways to improve their competitiveness.

Since 2009, UIC has been structured on the basis of four technical departments: passenger, freight, rail system (infrastructure and associated aspects), and fundamental values. The latter department brings together railway protection and promotion of its social and environmental credentials: security thus sits alongside safety, environment and sustainability, training, and research.

Alongside the action taken by UIC member railways, UIC itself has addressed the subject of security, developing activities in various shapes and forms since the late 1990s and focusing particularly on the development of the terrorist threat following the 11 September 2001 attacks in the USA.

The idea is to share experience and best practice and to define shared ways and means of action so that members can learn from and successfully apply lessons from elsewhere when developing their own strategies, in partnership with their national authorities and, potentially, in accordance with a general international framework.

11.1 UIC Fundamental Values

Alongside its three "technical" departments—Passenger, Freight and Rail System—corresponding to the business units conventionally used in the rail sector, UIC has also created a "Fundamental Values" department bringing together various subjects which cut across the traditional lines but which also serve to protect the rail sector or spotlight its economic and societal benefits.

Security and safety are thus part of this department, alongside sustainable development, international training, expertise development, and research. As regards security, this serves as a reminder to the rail sector that its security policy must be designed in the service of its various businesses, alongside and complementary to the vital role played by the public authorities, not as a substitute for them. The security priorities of the sector and those of the authorities may thus differ, but must remain consistent and a source of synergy.

11.2 UIC Security Platform

Both in its working groups and at its annual congress, the Security Platform brings together UIC members from across the world wishing to make headway on the subjects they consider vital priorities.

The Steering Committee is attended by representatives of the various rail business units (passenger, freight, rail system), representatives of the UIC regions

(Europe, Asia, Middle East, Africa), representatives of the major industry, technical and institutional partners, and by the chairs of the working groups, guaranteeing that the needs of each party and of the rail sector in all its complexity are optimally attended to.

Overseen by the Security Division, which also acts as a centre of expertise and think-tank, the platform acts both as a standing venue for exchange between members and as an arena for partnership with the various European and international institutions and bodies with responsibility for railway security.

Chaired by a European and a non-European on a rotating basis, it has a global dimension, which goes beyond regional particularities.

The platform holds an annual world security congress on a mutually-agreed subject which is defined based on members' needs; the 9th such congress is set to be held in Paris on 13 and 14 November 2013, and will be organized jointly with SNCF on the overarching theme of: "Security policy: which strategies, regulations and partnerships for railway companies?"

Meanwhile, the working groups continue to address: three "constants", developed by UIC, which form the core planks of security policy: human factors, technologies, strategy and regulations. The idea is to develop these three aspects in parallel: an effective security policy starts by supplying frontline staff (human factor) with the information and decision-making support they need (technology), all within a legal or regulatory framework in partnership with the public authorities (strategy and regulations). Two priority subjects, requested by UIC members in the light of current events and the problems encountered on the ground: metal theft, and border crossings and security of international transport corridors. Metal theft represents an intolerable burden for railway companies both in terms of the direct costs caused by theft (replacement, repair, etc.) and in terms of the indirect costs (compensation for delay, damage to company image, etc.). In terms of the second subject, developing international traffic is assumed to bring time savings and ensure the end-to-end integrity of convoys: in this context it has been deemed a priority to conduct a pragmatic examination of security conditions on international routes (predominantly Eurasian freight corridors) and of border crossings en route (customs, compatibility between systems, etc.), in order later to define a shared method of analysis and a joined-up response, where necessary, along the whole route.

In addition, the Security Division provides various services, either at the request of the technical departments (e.g. the aforementioned work under way on a handbook on security in high speed systems, in collaboration with the Passenger Department), or at the request of UIC members (participating in studies, organizing working seminars, disseminating results and documentation, etc.).

11.3 UIC Research Focuses

In the areas of security, prevention, and combating crime and terrorism, perhaps even more than in other fields, tomorrow's challenges will not be met with today's solutions. The threat is ever-evolving, and the response must develop at the same pace, at least.

UIC is thus involved in various research projects, including those funded by the European Commission, focusing on the general protection of the rail system (stations, infrastructure, rolling stock), and on the reduction of suicides and trespass, protection of the most vulnerable infrastructure against threats of all kinds, etc.

One output of the PROTECTRAIL project was a general demonstration of the project proposals in Zmigrod (Poland) in October 2013; the project will conclude at a final conference to be held at UIC in Paris in June 2014. The goal is to coordinate the various useable security technologies within a consistent architecture, providing railway undertakings with solutions and standards for the security issues they encounter, whether these are objects blocking the tracks, unattended items in stations, identifying those responsible for risky behaviour, etc. The project takes a modular approach to the various aspects, and developments in problem-solving technologies can be included and integrated within the whole without adverse effects on the rest.

The RESTRAIL project (Reduction of Suicides and Trespass on Railway property) for its part aims to produce a toolbox for decision–makers in order both to reduce the number of suicides and trespass incidents and to mitigate the consequences of these acts. Some of the various measures identified and examined come under education and communications policy; others draw on early-warning or infrastructure-protection technologies. The most promising solutions are being field-tested during the second half of 2013, and the final toolbox should be available by the end of 2014.

The other projects underway include, in particular, those touching on cybercrime, which is undoubtedly a future threat.

Beyond the inherent value of these projects, they offer opportunities for partnership and joint thinking between disparate communities: railway companies, research centers, universities, specialist consultants, technical service-providers, etc., and allow us to broaden the scope of our enquiry, compare and contrast our analyses, and obtain a broader view of the roles, capabilities, and rights and obligations of the various potential players.

12 Conclusions

The rail sector has had to learn to live with a number of external constraints, which affect its environment, beyond the internal safety constraints, which are a constant of its business. This is the challenge to be met by the security policies to be developed. The challenge is complex since it involves taking on-board external systems of thought, which need to be joined up or synergized with those within the railways. Nevertheless, the challenge is also to meet the expectations of customers who wish to be able to travel undisturbed and of staff who wish to work without undue risk: this is the legitimizing basis for railways' actions, whether they are infrastructure managers or operators.

The task is simultaneously to construct a set of principles, which may require updating or strengthening by legal texts defining the rights and obligations of each party and its role in the process, and to develop constant awareness of security amongst the various players—including customers.

Customers expect their transport to be secure, but also that transport operators allow for all their various concerns, and for the random events which may disrupt their journey. Their vision if one of integrated protection for rail transport, to achieve which each component part must be integrated. This is no easy task, but to quote the philosopher Seneca: *It is not because things are difficult that we do not dare, it is because we do not dare that things are difficult.*

The Railway Security: Methodologies and Instruments for Protecting a Critical Infrastructure

Franco Fiumara

Abstract This chapter illustrates which are the methodologies and instruments for protecting one of the most critical infrastructures: the railway network. After a comprehensive overview about the potential threats, the chapter describes the security strategy, technologies and cooperation with Public Authorities which should be put in place to protect the railway infrastructure in a complete and effective way.

1 Introduction—Why Security?

Safety and Security have always been important needs for humanity.

Each human community—from the simplest to the most complex—has shown the will and the need for rules or organizations to regulate deviated or antisocial behaviours, in order to develop.

Overlooking the historical details, nation states took over security management, and left to private companies only a few sectors of autonomy, especially in the field of private property rights (e.g. real estate protection).

Social, economic, trade and transport development, and the impact of risk factors on strategic areas (e.g. energy, telecommunication, transport, bank), led to the development of "private security" activities.

Each company needs security systems to guarantee the protection and integrity of information, assets, and core business, regardless of its dimension or field.

Modern security organizations have extended their previous activities of surveillance and protection, to Business Intelligence, Competitive Intelligence, Crisis Management, Risk Management, and Information Communication Security Technology: in other words, they now prioritize the protection of any relevant information,

F. Fiumara (✉)
Ferrovie dello Stato Italiane, Rome, Italy
e-mail: r.setola@unicampus.it

R. Setola et al. (eds.), *Railway Infrastructure Security*, Topics in Safety, Risk, Reliability and Quality 27, DOI 10.1007/978-3-319-04426-2_3

about technology, organization, marketing, or production—which can represent a competitive advantage for the company.

Presently, the rail transport corporations require, depending on system complexity, a high-level integration of technological components and security procedures.

2 The Security in the Railway Transport

The first private security activity in the world actually appeared by happenchance in the railway field itself.

In response to frequent assaults and robberies from bandits, in 1850 the USA West Railway recruited the first private security company, under the command of the legendary Police Inspector A. Pinkerton.

Beyond the historical notice, because the railway was the first source of mass transport for remote areas, it was necessary to develop a security activity, in addition to the industrial and service ones, to guarantee its survival.

Building upon those foundations of railway security, today almost everywhere in Europe special units of Railway Police have been created.

Unlike industrial companies, who may decide and control the access of production and storage locations (usually with physical barriers), the railway environment must remain open to the public and clients alike.

As the most extended national network infrastructure, the railway system is open to many security-related vulnerabilities, in addition to the widest issue of the railway traffic safety.

The large city stations are authentic control centers of urban traffic, and crucial hubs of mass transportation intermodal flows. They represent the connection between airports and economic and cultural centers within countries, and between national and regional/metropolitan traffic systems.

As an open system, the railway is obliged to seek for robust relationships with the “external” world. First of all, it establishes relationships with the Institutional Authorities in charge of security, public order, and emergency management. Secondly, it builds a relationship with private companies and providers working in the same field, as well as with clients. The latter being the target of each activity meant to improve the offered service, in order to understand their awareness and perception about the security issue.

The security concept generates activities with different contents and action instruments, but deeply connected to the end-goal: “guarantee to the company the integrity of resources needed to perform the productive processes”, beginning with its clients.

3 Railway: A Critical Infrastructure

Development, security, and quality of life in industrialized countries depends on the continuous and coordinated operation of a set of infrastructures, universally referred to as critical because of their importance.

The term "critical infrastructure" describes a system, a resource, a process, or a set, whose destruction, interruption or temporary unavailability, has the effect of significantly affecting the efficiency and the regular operation of a Country, as well as the security and the economic and social system, including central and local public administration institutions.

The following resources are related to the critical infrastructures concept:

- Telecommunication
- Water supply systems
- Transportation
- Credit and finance
- Energy
- Emergency services

The importance and the significance of these infrastructures in our society have considerably increased in the last decade, with a consistent progression of available services.

Due to economic, social, political, and technological reasons, these infrastructures are becoming more and more complex and interdependent. Not only has their technical complexity risen remarkably, but also the decrease of monopolies has created articulate markets with many actors.

The increasing employment of innovative and powerful information and communication technologies has exponentially raised the interdependence of critical systems and infrastructures.

On the one hand, the quality of the distributed services has improved and the costs have decreased. But on the other hand, the information technology has introduced new and unexpected vulnerabilities in these infrastructures. Technical faults, natural disasters, and malicious actions would produce devastating effects. These events represent real dangers for the development and the social welfare of a country, and they seem to have increased as a consequence of the climatic phenomena exacerbation and the afflicted world socio-political situation.

4 CIP—Critical Infrastructure Protection

Governments are developing projects and precautionary measures to decrease the risk of critical infrastructure operations being interrupted due to wars, natural disasters, employees strikes, vandalism or sabotage.

The European Union is firmly involved in this topic, supporting scientific and technological research activities, and supervising the EPCIP (European Programme on Critical Infrastructure Protection) proposal from the regulatory point of view.

On the 8th of December 2008, the Council of the European Union adopted the 2008/114/EC Directive, aimed to identify and define the European critical infrastructure and to satisfy the related demand of better protection measures.

Though related to European critical infrastructures and limited to energy and transportation fields, point (a) of Article 2 provides a definition of critical infrastructure as follows: *an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions*.

Thus, the transportation and railway domain should definitely be categorized as a critical infrastructure, whose defense and protection is necessary and expected on behalf of the country government and management companies.

Methodologies to reduce vulnerabilities and face new threats against these complex systems must be developed by the management companies, since current welfare and security for a country strongly depend on critical infrastructures.

Italy adopted the 2008/114/EC Directive of December 8th, 2008 with the Legislative Decree N. 61 on the 11th of April 2011, related to the identification and the definition of European critical infrastructure and to protection requirements assessment. The legislative decree entered into force on the 5th of May 2011, after the publication on the Official Journal (GU n. 102 on the 4th of May 2011).

5 Threats in Rail Transport

The picture Fig. 1 summarizes the main and most frequent threats in the railway infrastructure.

Some of these threats come under the security incidents group, i.e. those events which anyhow endanger the railway traffic. It is important to note that potential risks for railway traffic also qualify as security incidents.

Examples of security incidents:

- Vandalism to the detriment of equipment connected to the railway traffic;
- Intrusion/interference of unauthorized individuals who alter the equipment operation for the railway traffic controls (signals);
- Placing heavy objects on the platforms (tracks, rails).
- Railroad switches operations on wrong routes which have impacts on railway traffic;
- Drivers inattention to give way at unmanned level crossings, which cause a collision with the transit train.
- Allow herds to reach the tracks.
- Dangerous substances incidents.

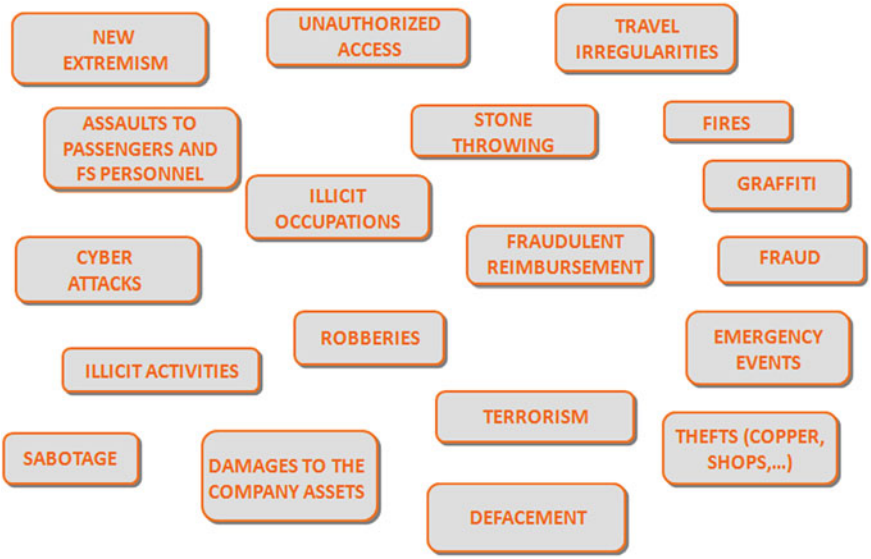


Fig. 1 Main and most frequent threats in the railway infrastructure

In the last years, two heterogeneous phenomena have gained importance:

- The terroristic threat;
- The theft of copper.

5.1 The Terroristic Threat

The terroristic threat is spreading all over the world with increasing intensity and violence.

It is an "asymmetrical" war, involving any means: Mass murder, the employment of non-conventional weapons, the destruction of an "enemy's" physical and logical infrastructures, the recourse to disinformation and media manipulation, and the evil use of *social networks*. All the above are elements to be considered in this war. Combined with destructive intents, these elements reveal vulnerabilities to collective security driven by new and alarming potentialities.

The risk that civil and economic targets could be attacked increases as people, society, and economics rely more heavily on infrastructures, public utilities, transportation and communication.

The attack at the heart of America has gravely affected Occidental population's fears. Since then, the raising level of the international terroristic threat has required an increased attention threshold towards strengthening the security instruments and the general prevention measures in each national field.

The attacks at the London underground and buses in 2004 have called into question the security of normal life of citizens during their daily activities—at the underground station, the bus stop, on the escalator, in the railway carriage, going to work, to school, reading a newspaper. The general fear of wide-open spaces (especially airports, railway stations, etc.) as potential terrorist targets has increased the focus on security issues and heightened public awareness.

Regarding the internal terrorism, the aggressiveness level is documented. The "new" Italian terrorism is composed of forces acting with explosive or combustive devices, addressed towards institutional targets and railway structures, in order to sabotage the "arteries of power". Handbooks with detailed information actually instruct how to damage electrical, overhead lines, signage or the tracks.

Therefore, it is necessary and important to devise new and dynamic methodologies to guarantee the security.

There is an innovative, non-static idea of security, very distant from the deaf and static *Moloch*, which quickly adapts to social changes and responds to the often unexpressed or misunderstood demands of collective security. Therefore, in order to allow the habitual levels of everyday life to occur, a structure is necessary which is capable of revealing the weakest signals limiting damages of "successful" attacks, and restoring the technological and infrastructural defense in the shortest possible time.

It is critical to build new stations, airports, and public places according to criteria and services layouts which take into account both the expected and the necessary levels of security.

5.2 Theft of Copper

After silver, copper is the best conductor of electricity on the market. It is corrosion resistant, recyclable, and widely utilized in the rail infrastructure and in telecommunication systems.

Because of the large employment at international level, the copper demand as a rough material exceeds its production, causing the rise of its stock price—which has tripled in the last decade—subsequently multiplying the thefts, especially penalizing the public services companies and causing remarkable delays.

Railway men and police forces are involved daily in combating the thefts. However, even with line controls at night, the phenomenon has reached such dimensions that structured actions must be taken. The illicit trade of copper is one of the most considerable source of capitals for criminal organizations.

In February 2012, in Italy the National Observatory for Copper Theft was created by the Ministry of Interior, within the Public Security Department. The Observatory has promoted the Law 119/2013, introducing from the 15th of October stricter penalties for copper thefts which damage Entities supplying public services. This countermeasure is considered as a deterrent by experts in the field who participated in the National Conference on theft of copper on November 22nd 2013, supported by the Observatory and presided over by the Chief of Police.

During the Conference, the Ministry of Interior reported that:

- the theft of copper from 2006 to 2012 had a fluctuating trend;
- in 2012 there were 19,701 thefts of copper, with a rise of 6.9 % compared to 2011;
- in the first semester of 2013, there were 11,040 thefts with a rise of 12.1 %, compared to the same period of the previous year.

This statistic, provided by the SDI (Service for the Interforces Informative System), includes the theft of copper both in public companies and in private citizens utilities.

In 2012 the most affected regions were, in order: Lombardy, Puglia, Sicily, Campania, Lazio, Piedmont, Tuscany, Emilia Romagna, Veneto and Sardinia. However, in these regions the police force had considerable results in opposing the phenomenon. In particular the number of reported and/or arrested subjects in Lazio increased 48 % compared to the previous year, 38.7 % in Sicily, 65 % in Emilia Romagna, 4.5 % in Tuscany, 21.2 % in Veneto, and 79.5 % in Calabria (Figs. 2 and 3).

On the Italian initiative, this topic was pointed out to the COLPOFER, the international association of the railway police forces and the security structures of the European railway companies. The association discussed the tendency analysis and the additional possibilities to oppose the phenomenon in the international meeting in Rome on 5 and 6 December 2013, due to the serious damages in the rail infrastructure. Fortunately, the safety risk for the passengers is excluded.

According to the European point of view, the theft of copper is considered a cross-border crime, which has a significant impact on people's lives and on national economies, and in general on free circulation of citizens.

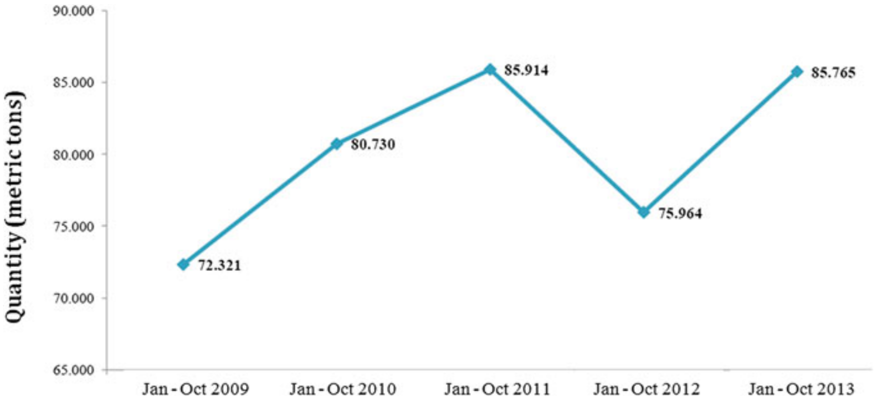


Fig. 2 Copper waste and remains exportation expressed in metric tons from 2009 to 2013—Italy's outgoing flows. *Source* COGNOS database—customs and monopolies agency

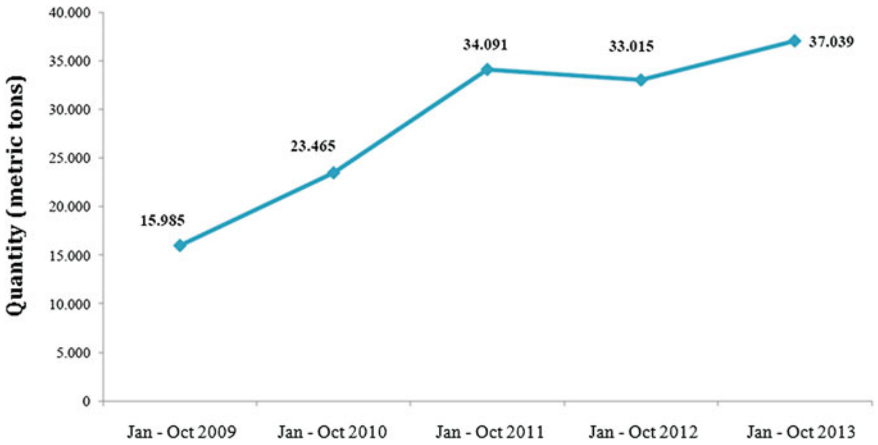


Fig. 3 Copper waste and remains importations expressed in metric tons from 2009 to 2013—Italy's incoming flows. *Source* COGNOS database—customs and monopolies agency

Therefore the EU institutions and the associations of the field (COLPOFER, CER, and UIC) are paying increasing attention and are requiring more coordination between the Police Forces in order to contain it.

For this purpose, EUROPOL organizes annual conferences (the last one was held in April 2014), which allow Police Officers and essential services providers to share opinions and find concrete solutions to this problem.

The German railways reported 2,848 thefts in 2012 and 1,557 in 2013 (this data was collected until November), whereas in Poland about 4,600 thefts have been registered in 2012, and 3,542 in 2013 (this data have been collected until October).

6 The Security Structures in the Main European Railway Organizations

A brief description of the Security sector in the most important European railways is shown below.

6.1 France (Société Nationale des Chemins de fer Français—SNCF)

Throughout 33,000 km network, SNCF Security is responsible for the security of customers and employees, railway operations and railway property. The organization ensures coverage of the whole French territory through a national central command and 11 Security zones. The SNCF is composed of a specialized SNCF railway

Security service (SUGE) and 400 Security specialists based in SNCF regional directorates and operational establishments. The security at the SNCF is moreover based on partnerships and cooperation with the authorities at both national and local level and cooperation with Security companies. This cooperation exists at European level when the expertise is shared with the other Security services abroad.

More precisely the SUGE is an armed force of authorized railway Security officers with 2800 agents who are in charge of controlling potential violations of law if committed within the SNCF railway structures, according to the French legislation on Security guards.

They have police powers in the fields of crime prevention, ensuring the security of staff, customers and property on railway premises, powers of arrest when a crime is committed on railway premises.

6.2 Spain (RENFE)

The Security Department direct, coordinate and organize the plans and actions for safety/Security of Renfe, in order to preserve the safety of persons and company assets and to implement Civil Protection and Risk Prevention policies. The main goal is to guarantee the safety and health of travelers and employees, all in accordance with current legislation and Renfe guidelines.

Renfe Security department deal with natural (snow, floods, etc.), social (demonstration, terrorism, strikes, etc.) environmental risks and internal risks (hazards for transportation of dangerous goods, etc.).

6.3 Poland (PKP Polskie Linie Kolejowe S.A.—PKP PLK S.A.)

The Railway Security Guard was established in November 1918.

Currently, the Railway Security Guard functions within the frame of the rail infrastructure manager PKP Polskie Linie Kolejowe S.A.

Railway Security Guard tasks defined in the Act of 28 March 2003 about Railway Transport

- Monitoring of compliance with order regulations on railway premises, trains and other railway vehicles,
- protecting people’s lives and health as well as their property on railway premises, trains and other railway vehicles.

While executing his duties, Railway Security Guard Officer is entitled to:

- Identify individuals (check one’s ID card)
- Incapacitate and transfer power to Police over all individuals who behave in the way that go beyond the permission of Railway Guard

- Stop and check individuals' cars
- Clamp sanctions in the form of penal ticket
- Conduct explanatory activities, move proposal to court with application for punishment, accuse in front of the court
- Use the means of direct coercion
- Using PESEL* database

*PESEL—Universal electronic system of the population census

Dog units (98 dogs) are used to achieve the SOK institutional goals. Following a specific training, the dogs can be utilized only by SOK officers.

6.4 Switzerland (Schweizerische Bundesbahnen—SBB CFF FFS)

As stated in the federal law SR 745.2 of the 18th June 2010, there are two types of security organizations in Switzerland: the security service and the transport police.

The transport police and the security service differ by:

- Additional tasks (Article 3 section 2);
- Additional powers (Article 4 section 2);
- Obligation to pledge (section 5); and
- Obligation to wear the uniform (section 6).

The security service and the transport police are entitled to:

- Question people and check entitlement documents;
- Hold, monitor and expel the individuals who do not respect the regulation;

The transport police is also entitled to:

- Temporarily arrest the held people;
- Seize objects.

The Transport Police works at the Swiss railway company SBB CFF FFS, under the supervision of the Federal Department of Transportation.

6.5 Italy (Ferrovie dello Stato Italiane SpA—FS SpA)

The Railway Police has the institutional duty to prevent and repress crimes, safeguard the public order and ensure the security of citizens in the railway environment —both on running and standing trains, and in stations and other premises of Ferrovie dello Stato Italiane.

The Railway Police was established in 1907. The Ministerial Decree n. 1211 of March 30th 1920 established thereafter the regulation for the public security service in the railway environment. Moreover this regulatory document has imposed on the "FS Company" all the necessary costs for the railway police service (as restated in the following Legislative Decree 687/1947 and in the Law 150/1985). The M.D. of August 2nd 1977 adjusted Polfer functions and duties and redefined its organizational structure.

The law n. 121 of April 1st 1981 regarding the Public Administration Security reform has qualified the Railway Police, the Traffic Corps, the Postal and Communications Police and the Border Guard, as a State Police "Specialty". The subsequent definition of the organization was regulated with the M.D. of the March 16th 1989.

Today the Railway Police is present in the national territory with 15 districts, in which there are 17 sections, 27 subsections and 153 Railway Police posts.

Within FS there has been a Company Security structure since 1991; this structure has been existing at central level until 2001. After the privatisation of Ferrovie dello Stato and the creation of Trenitalia S.p.A and of Rete Ferroviaria Italiana S.p.A., the Company Security structure reorganized. To date, two different structures have been created, one belonging to Trenitalia and the other to RFI, both coordinated by the Security Directorate of the Ferrovie dello Stato Italiane Holding.

Local security offices are created and located near regional railway directorates.

The security activities are planned at the headquarters and they are put in place by the personnel at the local security offices throughout the entire national territory.

7 International Organizations Involved in Railway Security

At international level, three associations allow the cooperation between public and private authorities in the security field:

1. Colpofer
2. Security Platform in the UIC
3. Brenner Group.

7.1 Colpofer

In the sphere of the European rail transport, many organizations are involved to ensure the public security of travelers and goods belonging to the railway companies. These organizations have developed appropriate methods and techniques to oppose certain kinds of delinquencies, nevertheless the implemented approaches differ from country to country.

Therefore, in 1980 the main West-European railway companies decided to found COLPOFER (Collaboration des Services de Police Ferroviaire et de Sécurité), an association aimed at the cooperation of railway polices and the company structures of railway security. Common principles, procedures and methods have been developed to allow information exchange and unified approaches to particular issues. The members can share their experiences and know-how in the area of interest, especially concerning the fight against crime within the rail environment.

COLPOFER operates independently and is associated with the International Union of Railways (UIC) whose headquarters are in Paris; COLPOFER is referred to in UIC as "Special Group". Its members are railway company security managers, authorities and police force representatives of 24 Countries.

7.1.1 The Method

COLPOFER has developed a common approach to deal with different security issues, in order to promote the international cooperation and the development of the European unification. So far this joint approach has been utilized for the following rail security issues: football supporters, sabotages, terrorism, unpaid train tickets, fraud and ticket forgeries, freight traffic thefts, thefts on international passenger trains, criminality in urban transportation, vandalism and graffiti.

Common principles have also been devised in regard to: environment and security perception in the rail sector, commercial railway company security, railway police function and position (ranking), and crime prevention on urban transport.

7.1.2 The Mission

- Exchanging experiences and information about methods and systems concerning prevention and fight against crime in rail environment
- Exchanging information about important issues in the rail security sector
- Defining a common strategy in regards to railway security
- Improving the results of the international security measures thanks to cooperation among members
- Analysis of methods and systems to enhance security in rail transport
- Elaborating on recommendations aimed at improving security levels in the international rail environment
- Consulting and supporting rail transport security operators.

COLPOFER activities are arranged into appropriate Working Groups, i.e.:

- Graffitis
- Fraud/Ticket forgery
- Cyber Crime
- Antisocial behaviors

- International Freight Transport
- Terrorism and extremist activities
- Pan-European Corridor X[1]
- Big Events (“Control Rooms” Sub WG)
- Metal Theft monitoring cell.

7.2 Security Platform UIC

The *Security Platform* was instituted in 1997 and rearranged in 2008 as the UIC (Union Internationale Chemins de Fer) structure aimed at developing the security policy for people, trains and railway employees. The Security Platform members include world-wide Transport Companies who define international strategies, examining several topics in specific Work Groups. Its meetings are attended by the associations CER (Community of European Railway and Infrastructure Companies) and EIM (European Rail Infrastructure Managers). Specifically CER activities are aimed at protecting the interests of its members, transportation companies and infrastructure managers, with regards to the EU Commission, the European Parliament and EU decision-makers in general.

COLPOFER and UIC have promoted, at a specialized level, the rail environment security through international Forums. The meeting of October 2002 in Rome is noteworthy, since it involved 200 participants among Police representatives, Railway Industry managers and experts from different countries. The objective of the “Rail Security Forums” is to promote “experience sharing” and for the rail transport actors to cooperate, taking into account each other’s security elements. Security is indeed a strategic factor for the railway enterprises, and its aspects are crucial parameters in the service quality, company operation and image.

The II World Forum on Railway Security, held in Rome in 2002, presented the new operating background for railway companies, and restated the importance of such joint platforms as a part of the overall railway product.

The last forum held in Rome (22–23 September 2011), was the UIC World Security Congress, promoted by the Ferrovie dello Stato Italiane Group with the *Union Internationale des Chemins de Fer* (UIC), and involved the protection of the railway infrastructure and trains against international terrorism and micro-criminality.

During the congress, security managers of the main international railway companies exchanged views about several issues within the security field: prevention methodologies, global risks, changes introduced by the liberalization, use of more sophisticated technologies, etc. It was concluded that the concept of security must

[1] The Corridor X is one of the pan-European corridors. It runs between Salzburg in Austria and Thessaloniki in Greece. The corridor passes through Austria, Slovenia, Croatia, Serbia, Macedonia and Greece.

be considered from the inception of the station design. Therefore, it is necessary for the security field to interact with the representatives from architecture and town planning. Additionally, the construction of rolling stock should comply with this approach.

Besides the preventive measures for possible international terrorist acts to be precluded, the Congress took stock of the situation concerning the world phenomenon of the theft of copper and the micro-criminality episodes on trains and in stations. During the international Congress the records of each Country and the adopted prevention and protection measures were illustrated. For example, the Italian Railways have already increased the number of inspections in the most affected areas in order to restrict the phenomenon. Moreover Ferrovie dello Stato Italiane is gradually replacing, where possible (prioritizing the high-risk lines of the 16,700 km national network), the copper with other metals (aluminum, aluminum-steel, alternative materials), which are less precious and attractive for criminals. Otherwise, the copper is isolated with cement "cages", especially in the regions, which suffer the most the "red gold" theft.

During the Congress, it was expressed that technology should play a more active role in order to accomplish the desired security tasks. Projects aimed at the development of an appropriate architecture were illustrated; they devised to achieve integrated security systems starting from current technological products integrated on a common platform which could be combined and re-modulated depending on the end user's needs. In particular, research activities aim to identify integrated systems (CCTV systems, access control, perimeter and volumetric anti-intrusion systems, radar systems, building automation systems) to protect the main rail assets (stations, electrical power substations, tunnels, bridges and flyovers, etc.), using software platforms with SOA communication protocols.

In conclusion, it was pointed out that each aspect of our current life, i.e. economic, social and political, is deeply affected by the rise of Eastern Countries' economic power with regard to the West. The railway companies, the infrastructure itself, the habits and needs of customers, and of course the security field, all feel the consequences of those changes, both in the public and private sectors. Many challenges arise from the attempt of companies to expand into other world markets, especially the emerging ones, e.g. additional risk elements, increased types and number of threats, less economic power to have the necessary resources available to meet the increased need of infrastructure protection, and fewer investments to let the companies grow and recover in the economic drop. Because of dealing with new social, economic, and regulatory rules, those engaged in the security field must be able to broaden their competencies and deepen their tools for the risk analysis and emergency management. For example, the recent need for many Italian companies to evacuate their employees working in North Africa (Egypt, Tunisia, Libya), where in a limited amount of time the masses have strongly altered the political condition of the current decades.

It is necessary to employ reliable and effective technologies, to contain the maintenance costs and arrange focused investments and accurate strategies, in order to optimize the tasks for the operators and reduce the waste. Therefore, the search for the right mix of "innovative" and "mature" technology is a complex algorithm, which needs to be continuously updated depending on the technological variations and appearances of new threats.

7.3 Brenner Group

Founded in 1985 as the seat for the information exchange between the Railway Police Department of Verona and the Austrian Police, it has become a regional group of the Alps.

The Group promotes information exchange and the adoption of security measures in a well-travelled international area. Since the number of participant countries is limited, the group is able to effectively deal with operational issues with immediate effect implementations.

8 Infrastructures Security: A General Survey Regarding the Current Regulation

Until recently, the security of large national air, naval and rail companies were managed by the Institutions: i.e. the Border Police—Coast Guard—and the Financial Guard. The Law 217/1992 established—for the airports- the transfer of the management responsibilities from the State to the economical operators, leading to their privatization and liberalization of the ground services. The transfer of the management from the public to the private sector involved the activation of private security services to monitor people and luggage, as stated in the Article 5 of the aforementioned law, and in the following MD 85/1999 regarding the implementation in matters of concession entrustment of security services.

Moreover, a dedicated inter-ministerial Committee was instituted for the security of air transport and airports (CISA). The Committee is in charge of elaborating and updating the National Security Programme against illicit actions in the civil aviation field, in accordance with the guideline of the Interministerial Coordination Committee for the security of transportation and infrastructures.

In the matter of port infrastructure, the Law no. 84 of 1994 attributed the port management to private subjects. After the 9/11/2001 incident, port security standards experienced profound transformations with regard to the trade relations with the U.S. (freight transport and containers). In December 2002, the International Maritime Organization (IMO) issued the "International Ship and Port facility Security code", better known as ISPS, as a model for the security management on ships and in ports. It is a risk assessment aimed at identifying the vulnerabilities and weak points, and then defining the infrastructural and organizational measures to secure such assets. This concept of security was previously unknown in the port field, except for the cruise sector.

Italy participated in the U.S. project named "Container Security Initiative" (CSI), which expected U.S. Customs executives to reach the major world ports (including Genoa, La Spezia, Livorno and Naples) with the purpose to monitor the U.S. bound containers alongside local customs officers. Another U.S. security initiative is the standard "Customs Trade Partnership Against Terrorism" (C-TPAT). This voluntary standard for main carriers and exporters is aimed at assuring the security of the overall logistic chain in return for reduced inspections.

Additionally the port field includes a dedicated Committee (International Committee for the Security of Maritime Transportation and Ports), in charge of establishing the guidelines for port security, updating the Security and Anti-terrorism National Programme and keeping in contact with the responding international organizations.

Recently, the decree n. 154 of 15 September 2009 was issued. It introduced a procedure to regulate the services of subsidiary security in ports, railway stations, underground stations, and of the related means of transport and depository, which do not involve public authority intervention (as stated in Article 18, clause 2 of the decree-law no. 144 of 27 September 2005, converted into law no. 155 of the 31 July 2005). The control services requiring public authority intervention or the employment of Police forces are excluded from the application of the aforementioned procedure.

The subsidiary security activities aimed at preventing damages or prejudices to the free provision of goods carried out by private subjects, that the law does not attribute public forces (so they can complete the operation of public security and judicial police officers duties).

In the mentioned facilities, the port management companies, the railway companies or the transportation services in concession systems, or private vigilance services/security guards all have the possibility to take care of the following services:

- Vigilance service for property goods or in a concession system, to protect the company assets, and the equipment of the personnel on board;
- Video surveillance and tele alarm services;
- Radioscopic control or use of other instruments, of freight, luggage, and courier parcels;
- Catering material and provisions on-board monitoring in the production and packaging area;
- Vigilance of luggage deposits, freight, mail and catering;
- Escort for luggage, freight, mail, catering, and provisions on board to and from carriers (ships and trains);
- Vigilance for standing means of transport—ships, boats, trains, carriages, buses, etc.—in the respective depositories and on board access control;
- On board control aimed at revealing security risks (abandoned luggage, dangerous objects, etc.—and possible critical situations);

- Authorization monitoring, examining port cards, badges, travel documents, which allow access to the port area, the port personnel and to any individual who needs to access those areas;
- Any other monitor or vigilance service, which does not need public authority intervention or the employment of Police forces.

According to the Regulation 725/2004/EC and the Legislative decree no. 203 of 6 November 2007, plans including vigilance services and control exerted by the public force in the port and railway field, are allowed to directly commit the following activities to private vigilance institutions or security guards:

- Checking of hand luggage and objects brought by passengers through walk-through metal detectors (WTMD) and hand held metal detectors (HHMD), spot-checking with radioscopic controller, pat-down checks, use of explosive trace detectors (ETD) and dog units;
- Radioscopic checks or use of other types of instruments for checking hold luggage, wares, and the express courier parcels;
- Control at driveways and crossovers of the port area, of railway stations bus services in concession and of the relative depositories, including the access control for the single areas, where required;
- Vehicles control at boarding;
- Vigilance at passengers and freight terminals.

The aforementioned services are accomplished under the supervision of the police force in charge, according to the directives in force on the subject.

The security guards on trains or ships can also cooperate with the onboard personnel, for on board services protection and maintenance, (this excludes rail police activities and navigation).

All the private security facilities and the specific security guards who operate in the environments depicted in the 203/2007 must safeguard the citizens' security and must:

- Equip their operative centers with appropriate systems to rapidly exchange information and communicate with the police force in charge;
- During vigilance and control activities, report to the police force in charge the remarkable events about the public order and security, according to the Public Security Department directives;
- During video-surveillance and tele alarm activities, keep and make available for the public security and the judicial police organizations, the technical supports containing sensitive data for the prevention and suppression of crimes, according to the Public Security Department directives.

9 Corporate Protection in Rail Transport Companies

The Railway Security operation is involved in peculiar activities for both Railway Infrastructure Managers and Railway Undertakings[2] (Passengers and Freight)[3]:

1. Railway Infrastructure (systems involved in the railway operational activities: tracks, signaling systems, circulation management systems, electric power supply systems, telecommunication, stations, train depots);
2. Passengers and freight transport (rolling stock, on board and assistance personnel, stocks, dangerous goods in transit, maintenance structures, plants).

9.1 Tasks

In each railway security organization, it is possible to find the following areas of expertise:

1. *Property protection*:
   - Definition of strategies, policies and security standards;
   - Fight against fraud and tariff evasion;
   - Inspection activities and assessment of the compliance to the company instructions;
   - Inspection by third parties of facts, circumstances and behaviors which could damage the company interests;
   - Analysis, study and definition of technological systems;
   - Design, achievement and definition of technological systems for information security;
   - Design, achievement and definition of technological systems for physical assets security.
2. *Supervision and risk analysis*
   - Dynamic supervision and data collection regarding critical situations of railway service;
   - Company assets risk analysis;
   - Awareness and education projects in the field of company security.

[2] Any public or private company which provides services for the transport of goods and/or passengers by rail

[3] The CEE Directive no. 440/1991 laid the foundations to rearrange the European railway system. According to the previous structure, a national railway company (monopolist) often worked for the Ministry of Transport supported by private companies in charge of minor lines in concession regime. The Directive has imposed the accounting separation between the infrastructure management and the transport services, promoting the liberalization and the competition in rail transport trade.

3. *Emergency management*
   - Operational management and overcoming of critical events, including the activities of civil protection.
   - Training activities of civil protection and defense.
4. *Institutional relationships*
   - Law Enforcement;
   - Governmental authorities;
   - Civil Protection Authorities (Department and local divisions);
   - Other International Organizations (COLPOFER, UIC, Europol, Security Platform UIC, etc.)

9.2 The Organization of the Security Function

When "building" the Company Security structure, it is necessary to maintain compliance with the needs of the overall corporate organization, meeting the different "interests" of the internal stakeholders according to systematic and economic criteria.

The security function must be arranged as a central structure able to develop security strategies, manage the economic investments and cooperate with the crisis units (both institutional and within the company).

Considering the organizational chart, the afore-mentioned activities can be arranged in the following structures:

- *Industrial security*: in charge of the procedures and security regulations design, for the protection of trade secrets (know-how, information), and to comply with the regulatory requirements in the matter of National Defense and Civil Protection (military transport coordination, civil defense committees, etc.).
- *Railway Infrastructure/Railway Undertakings security*: in charge of the coordination of the local offices' activities and for the organization and the achievement of strategies and operational plans approved by the Security Manager.
- *Engineering Technical Area*: responsible for proposing investment plans, defining the needs and the implementation of technological means for structure protection, design and installation.
- *Information System Security*: in charge of the protection measures management, the integrity and the availability of the company information and IT assets. The knowledge of this information is a basic factor for the development and the maintenance of the business objectives. The development of information processes and systems that characterize the company leads to rapid changes in the possible risk scenarios.

- *Territorial Departments of the Security*: several local units must be present to consider the territorial distribution of corporate property and activities, aimed at monitoring the territory, managing relations with the Law enforcement and territorial governmental organizations, and supporting the emergency and crisis management units.

This decentralized model allows the effective protection of the local assets, such as timely interventions and the possibility to have operational cooperation with the referential law enforcement.

10 Human Resources

A relevant aspect in the security organization phase is the fact that a Security management system within a company is based on many different subjects, some humanistic (sociological, psychological, legal), some more technical (information technology, electronics, magnetism and physics), and some related to math and logic (cryptography, risk analysis models).

Although it is not possible to expect that security officers are experts in all fields simultaneously, there are a number of distinct sectors, each one requiring a specialized group:

- Security operational aspects
- Technical knowledge of the railway infrastructure
- Social and intelligence aspects, including the promotion and the communication of security aspects
- Legal regulation and certification standards
- Risk analysis methodologies
- Physical, information, and cryptographic technologies
- Security procedures

It is also necessary to appoint a supervisor for the entire sector, and for companies, which have local department, there should be a responsible for each decentralized office.

10.1 Recruitment

The personnel, mainly the regional one, has a crucial role in the prevention and management of crimes committed against the company, therefore it will be selected on the basis of:

- Reliability and confidentiality
- Respect of rules
- Flexibility

- Aptitude in working in team and ability to share objectives
- Aptitude in interpersonal relations

The resources could come from the company itself, from the Academia or from public or private security sectors.

The recruitment should occur through different assessment processes for each role, able to measure the professional level, the resources management competences and the aptitudes.

The know-how acquisition is conducted through the employment of external experts with a public (law enforcement) or private security background with a deep knowledge of public order, personal security, and specialized personnel management techniques.

10.2 Training

During the first months after recruitment, an appropriate "culture of security" for the personnel should be achieved with both education courses and on the job training.

The topics of the training course should be:

- Scenarios, fundamentals and the reference regulatory framework for security
- The security organizational system they will be working in
- The operational and management instruments of security
- Interpersonal communication

Due to the preponderance of front line activities, the last module is fundamental to strengthen the trust between colleagues, in order to enhance a "team working" environment, and to provide each other with communication models and theories to approach the habitual interlocutors of the railway field.

For the "expert" personnel, specialized education courses must be periodically organized, such as:

- Courses for operational management of security-related railway emergencies
- Civil Cooperation and Civil Protection courses
- Master's programs in corporate security.

It is also necessary to establish an educational path aimed at certifying the personnel's know-how regarding the different rail sectors (plant and line security, equipment, telecommunication, electrical system, implementation means) and the related updates.

The afore-mentioned features characterize the personnel in charge of two functions, which represent the "core business" of the railway security: crisis and risk management.

11 Crisis Management

During crisis management, an organization deals with the risk that a huge event could potentially damage the organization, its stakeholders and the public in general. The project arrangement and design require a deep knowledge of the single company processes and their development.

The crisis management plan should always take into account the company and human dynamics affected by the malicious event. After its design, the crisis management plan should be periodically updated, and not left aside, waiting for the undesired event to occur before its application.

The crisis management plan should not be considered "unchangeable" and when prepared it should not be left languishing and waiting for the event to happen. Those who wrote the plan (which is mainly a collegial product and shared among company functions) and those who manage it should take care of it as the oil for bicycle.

Obviously, the crisis management process will be only as effective as the company social environment is strong and characterized by valuable human relationships, and valid professional experience. In most cases, the crisis management plan is achieved with the cooperation of all corporate functions.

It is sometimes possible that a critical event reveals the latent conflicts between corporate managers or functions, worsening the potential consequences affecting the company. Thus, it is necessary for all the corporate structures to manage these conflicts and convey only positive efforts towards the crisis passing.

For the "learning skills" of the company personnel, the following aspects should be of utmost importance:

1. The will to investigate the causes of the crisis (to identify personal responsibilities), in order to remove the basic prerequisites;
2. Competence of the crisis manager, who should continue to work on the plan even after the crisis stops spreading its potential harm, focusing on the gaps found in the crisis management system.

The rail transport is often affected by national events regarding the crisis management, produced by natural, anthropic or technical causes. In such occasions, it is necessary to manage several criticalities, such as mass transfer and external threats including a terrorist one.

12 Risk Management

The risk management process identifies, measures and estimates the risk, and further develops, examines, and updates the methodologies to manage it.

In general, the risk management process is considered as the need to sustain a certain cost as a consequence of potential losses, therefore this need could be postponed.

The risk management process minimizes the total cost of risks and maximizes the company utility. The aim is the achievement of company profits and competitive advantages through the employment of a mix of optimal strategies and appropriate instruments to reduce the global cost of risk.

12.1 The Italian Case of Risk Management by Rete Ferroviaria Italiana SpA, within Ferrovie dello Stato Italiane Group

Rete Ferroviaria Italiana (RFI) SpA performed a technical/regulatory Security Risk Management system, in order to obtain the ranking of risks related to each RFI business process and to corporate resources, in addition to the elaboration of an Incident Report for each company asset.

This project, called Enterprise Risk Assessment and Security Management (**ERA$^{\mathbf{SM}}$**), is an open information system, adopting brand new methodologies, risk-related data elaboration, and consequent dynamic analysis of threats as wide as the extension of the infrastructure on the national territory.

According to this approach, the system adopts a qualitative/quantitative methodology for all the 14 large stations, 103 medium stations, and to the 2,700 small stations, to bridges, viaducts, and to the remaining 25,000 assets of the infrastructure (tunnels, lines, rail crossings, etc.).

ERA^{SM} makes available information related to potential threats towards the single asset, and the dynamic evaluation of the actual risk, indicating the most effective countermeasures and the procedures to be adopted by the operators.

Another relevant element of this project is the strong integration with the other RFI IT systems for maintenance and railway traffic management on geographic information layers.

The system is devised to be utilized daily by a huge number of Corporate, Railway Police and Civil Protection operators. Further, it allows an accurate and precise detection and recording of security events occurring in the whole infrastructure, upholding the track record; all operators on the territory utilize this function to include information in electronic format related to denunciations to Railway Police, supplying and updating in real time both the statistical data and the exposure level to several risks.

ERA^{SM} is a very innovative project, conceived from the fusion of the technical expertise of the railway security personnel and that of information engineering. RFI has collected all the issues raised in international security forums among Critical Infrastructures managers. The system is highly complex because of the alchemy between information engineering and advanced security methodologies in the information selection phase and in the interaction with the territory and the environmental context.

The complex amount of information, depending on the large extension of the related infrastructure, and correlated to automatically calculate the risk level, has required the design of an intuitive system for the operators.

The objectives for the design of the system according to the Corporate Protection structure are:

- Definition of the security risk ranking for each corporate asset located on the territory;
  - Elaboration of Incident Reports for RFI corporate processes;
  - Update of damage assessment elements;
  - Agreement on risk management methods with other corporate functions;
  - Collection of requirements and identification of investments budget;
  - Management of security incidents signals;
  - Provision of a local Incident Report;
  - Update of risk database;
  - Census of security measures and their effectiveness;
  - Identification of protection measures' needs.

The system is divided into main operational fields:

- Security Management
- Event Management
- Report and Analysis (Fig. 4).

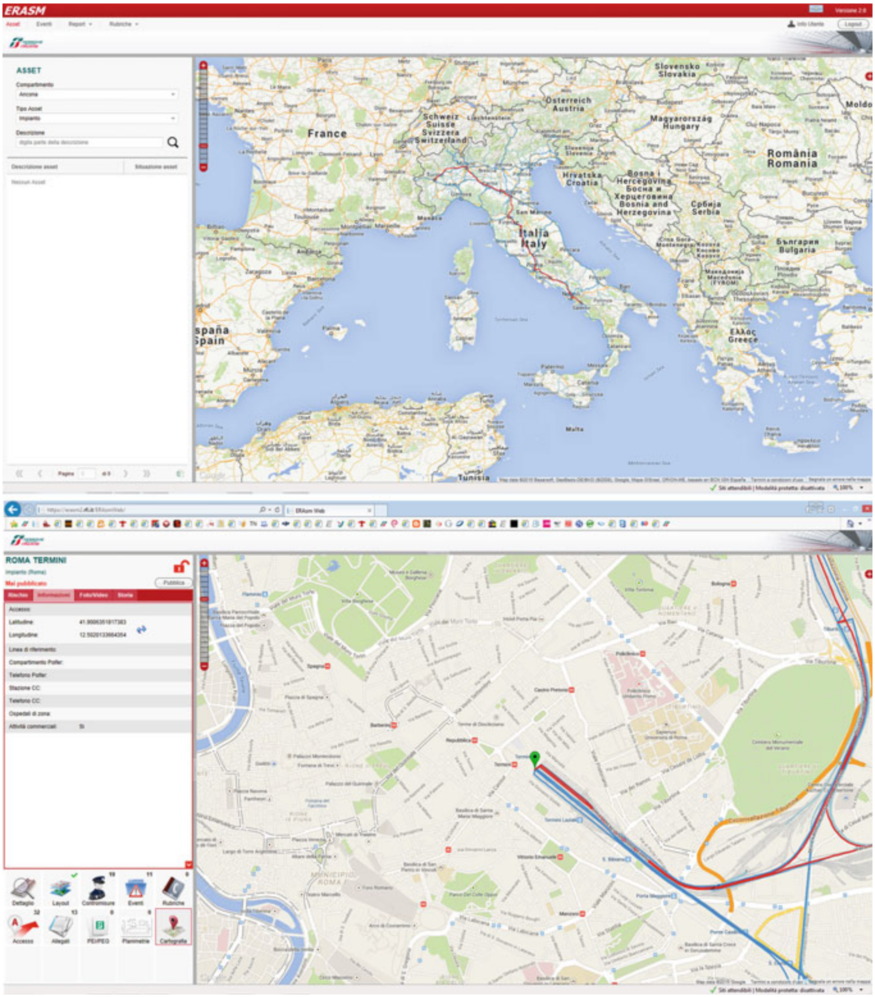
In the *security management* environment, information regarding the asset, the station "actual" structure, the risk indexes, the frequency of security events and incidents, the camera position map, the emergency plan, and the closest emergency and hospital structures are present. Further, a suitable set of concurrent countermeasures (CCTV, vigilance, fire prevention, lighting, etc.) allows the operator to immediately perceive the type and level of asset security system functioning.

Finally, thanks to a dedicated *simulation environment*, it is possible to evaluate the changes in the risk level depending on both the asset state (structure or layout) and in security measures, and the cost/benefits analysis formulation.

All the security incident signals or malicious acts against the infrastructure assets are conveyed in the *event management* section of the system, and they can be processed to produce reports. The "Webrisk" function allows the warnings report in real time to the appropriate operators.

The reports accomplished in the *report and analysis* environment are one of the most employed functions in the security operational activities: they have a tab or graphical format (e.g. pie graphs or histograms) and they are elaborated based on the threat, the time band, the location or specific needs, thanks to the custom features of the selected information tool.

In the System all the information collected by the Corporate Security personnel is stored and organized, such as asset plans, schemes, emergency plans, etc.



Compartimento: Ancona

Tipo Asset: Impianto

Descrizione: digita parte della descrizione

ROMA TERMINI

Impianto (Roma)

Mai pubblicato

Accesso:

Latitudine: 41.9006351817383

Longitudine: 12.5020133664354

Linea di riferimento:

Compartimento Polfer:

Telefono Polfer:

Stazione CC:

Telefono CC:

Ospedali di zona:

Attività commerciali: Si

Fig. 4 ERA^{SM} Screen shots

Since ERA^{SM} is a tool which supports the security operational activities of Ferrovie dello Stato Italiane, the system includes the instructions and the procedures the Corporate Protection should follow if thefts, personnel assaults and other events occur.

Obviously, the physical access control systems and the whole information system framework have been developed with the aim of assuring the confidentiality and the integrity of the information in the database; in this, the data can be accessed only via strong authentication systems, in compliance with the privacy regulation.

13 The Information Security

Thanks to the technological progress, it is possible to have more readily available a huge amount of information, such as the exponential use of e-mails or messaging services in the last years. In the industrial field it is also common to consider the information available in the network, both internal and external, a necessary source of information to increase the performances and reach the business objectives. A fundamental role is played by the information protection, which usually includes trade secrets, strategy plans and also communications between top managers or institutions.

The information systems security is an important element for the protection of the personnel or of business issues, in some cases connected to this specific context. This is the case of the Critical Infrastructures, as both the information regarding the circulation systems and those of the passengers who often buy their tickets online, are available.

In the last few years new advanced and dangerous threats have led the Critical Infrastructures to adopt specific security units for the protection of information systems and information, supervised by the security manager and/or the corporate protection directorate.

Those organizations are dedicated to manage every kind of IT threat, both internal and external towards company information asset.

The objectives are reached through:

- Matching of the information security with the business strategies;
- Defining guidelines and general methodological, functional and technological rules in matters of information security;
- Risk management in activities connected to ICT development and operating processes;
- Development and definition of dedicated information security solutions;
- Supervision of information security activities;
- Specialized assistance and support;
- Promotion of communication and education programs to enhance the company awareness regarding information security.

Due to the development of threats and theirs sophistication, methodologies for software analysis and data traffic have been designed, in order to identify in the least possible time potential malwares which are often aimed at stealing or sabotaging information.

Therefore the dedicated structure should work on three aspects. The first aspect is the strengthening of the proactive analysis measures and techniques, in addition to malware analysis or code analysis; the second aspect is the strengthening of communication infrastructure security measures, via the adoption of specific technologies for data and network segregation; the third and last aspect deals with the security in the application of development methodologies for software quality and the creation of vulnerability assessment to monitor the robustness.

Finally, but not of less importance, as in every Critical Infrastructure, specific agreements with institutional authorities establish a direct connection to constantly share information regarding threats/attacks and the methodologies to limit the consequences.

14 Assets Protection Technology in the Railway Field

Today the corporate security is increasingly oriented towards technical aspects in order to study and accomplish strategies, policies and operational plans aimed at preventing, managing and overcoming unexpected events which can affect material, non-material, human resources and processes the company possesses and needs to reach good performances in the short-, medium- and long-term.

The projects aimed at guaranteeing the security of "strategic" railway assets consider the protection of:

- Stations, electrical substations, buildings critical for the railway circulation, tunnels, bridges and flyovers;
- Rolling stock;
- Ticket office and self-service machines;
- Stocks/structures;
- Ships and road schemes.

The following technological systems have been implemented to safeguard customers, staff, and company assets, together with physical security intervention where necessary:

- Passive security measures;
- Anti-intrusion and access control systems;
- Video-surveillance systems with local and/or remote management;
- Software systems for the video analysis;
- Building automation systems;
- Rescue request systems (SOS column);
- New technologies used according to the characteristics of their application.

The security strategy implementation is completed through:

- The definition of organizational procedures for access;
- The issuing of guidelines and technical requirements for the security system design;
- The occasional utilization of concierge services.

The Corporate Security structure should also include a technological *scouting* department, aimed at identifying the most suitable and innovative solutions in the market for railway asset protection.

14.1 The Components of a Security System

A security system is an integrated structure for the centralized monitoring of CCTV systems, access and anti-intrusion control from one or more monitoring centre.

The anti-intrusion detection subsystem is based on a central unit located in a protected area and aimed at the supervision of the whole system and reporting alarms and messages (auto-diagnosis messages included) to the local server, to the local station and to one or more remote stations.

The hardware and functional characteristics of the access control subsystem should manage the access of heterogeneous personnel to specific areas which are considered sensitive for the railway structure, both for the activities and the membership department.

In addition to guaranteeing the main typical performances of security systems, the subsystem should be able to acquire, manage and rule the functions of the different present elements. Therefore, it should possess the following requirements:

- Management of access control depending on user class and access levels;
- Badge reader management (magnetic, proximity or other type of identification systems);
- Management of the database utilized for the configuration of each way through or each consumption (user classes, access authorization level);
- Management of transit, alarm, malfunction messages and badge reader condition;
- Minimal response time of the system between event, alarm and display on the terminal of the remote control station and, if present, on the terminal of the local station.

The video-surveillance subsystem is made up of a set of cameras permanently connected to the control rooms of the main stations on the national territory, equipped with one or more monitors and sometimes with video walls. Each room is in charge of prearranged monitored areas, near the control room or, nevertheless, included in its “area of control”.

The type of reference system for the design of new CCTV systems is based on the transmission of images in digital format on the Ethernet network. It is a star architecture network with a high-performance and redundant central switch, entitled to the management of communication between cameras, users, recording servers, and monitors to display the images and their transmission on the geographical network in order to display them in the remote stations.

There are also IP cameras or analog cameras provided with codec in order to digitalize the signal and to send it to the local network through the Ethernet protocol.

Every signal originating from the video-surveillance system (auto-diagnosis included) is sent to a remote workstation in the local supervision center, in case of specific events, periodically or after a specific query. Moreover it is possible to send in parallel the signals from the video-surveillance system to other remote stations.

The images are stored in a local server which keeps the data for the maximum period of time established by the current regulation on personal data treatment.

The access to the recorded images, both local and remote, is password protected and available only for the authorized personnel, also in compliance with the privacy regulation.

As a general rule, some precautions should be kept in mind when installing cameras:

- use vandal-resistant cases;
- place cameras as much as possible in a way that they face each other;
- place cameras at least at 3 m high, where possible, to avoid them being vandalized;
- place protective films on glass cases to protect them from being spray painted;
- install external cables in cut-resistant materials.

Currently the subsystem of general alarm (SOS) is placed in those stations which are considered critical for security. It is composed of a rescue call column, being placed in numbers of two for each public-open platform and in the hall/ticket office, in the appropriate position to activate a videophone and alarm between the user (in case of assault, theft, threat, etc.) and the control post in the same station. If the station is not controlled, the call can be remotely sent to the appointed order forces. The system is also able to simultaneously record audio and video of the call. The main features of the column are the push-button panel for the rescue call (emergency call), the camera, and the audio equipment.

14.2 Security Logic

The complexity of the security system and the number of sensors or cameras employed depend on the characteristics and the dimensions of the protected area. In the railway sector, security logics and topological reference schemes are adopted for:

- Stations and stops;
- Electrical substations;
- Rooms or buildings considered sensitive for the railway circulation;
- Tunnels, bridges and viaducts;
- Parking areas;
- Rolling stock;
- Ticket offices and self-service machines;
- Maintenance offices;
- Other non-instrumental assets.

In general, protective measures for technical premises depend on the strategic level of importance, the analysis of the specific socio-environmental context of the area and on the following other criteria:

Table 1 Security Measures

	Critical level	Attended h 24	Not attended		
	Security measures		Low	Medium	High
CCTV system	Fixed dome on wall of premise			×	×
	External fixed camera				×
	Internal camera				×
Intrusione detection/ access control system	Magnetic contact		×	×	×
	Badge reader/electric-mechanical locks				×
	Volumetric sensors			×	×
	Inertial sensors				
	Acoustic device		×	×	×
Physical measures	Security door				×
	Gates				×
Alarm management	Phone dialer	×	×	×	×
	Control room			×	×

- Confidential documentation inside the premises;
- Core business technical equipment, (such as rail traffic controls);
- Unattended premises.

For example, Table 1 shows protection measures to be taken into account, considering if the asset is attended by security staff or unattended. In case of unattended assets, it is necessary to increase both technological security measures and remote controls.

In the following section, the security logics of the afore-mentioned assets will be described.

14.3 Security Logic for a Medium-Small Railway Station—Layout

The security system of a station is generally composed of:

- CCTV system;
- Anti-intrusion and access control systems for sensitive rooms;
- SOS columns for user rescue;
- Supervision and control stations;
- Infrastructure interventions.

Table 2 CCTV Characteristics

Areas	Technologies	Advices
In front of station entrances	Dome cameras and fixed cameras	One or two dome cameras facing the external area, fixed cameras for main building entrances
External open areas	Dome cameras	Set the patrol function
Access gates to the station	Fixed or fixed dome cameras	According to your privacy law, you could use cameras for face detection
Entrance hall	Fixed and dome cameras	Fixed cameras on sensitive premises (ticket machines, ticket offices, etc.)
Waiting rooms	Fixed and dome cameras	–
Passageways, stairs, lifts	Fixed or fixed dome cameras	–
Underpasses	Fixed vandal resistant or fixed dome cameras	–
Platforms	Fixed cameras	Maximum coverage of 35–40 mt per camera

The areas within the stations to be video-monitored are:

1. Head house exterior;
2. sidewalks;
3. Underpass;
4. Second entrance to the station (e.g. goods yard).

Both Table 2 and Fig. 5 summarizes the main CCTV security measures to be implemented, in order to increase perceived security by customers.

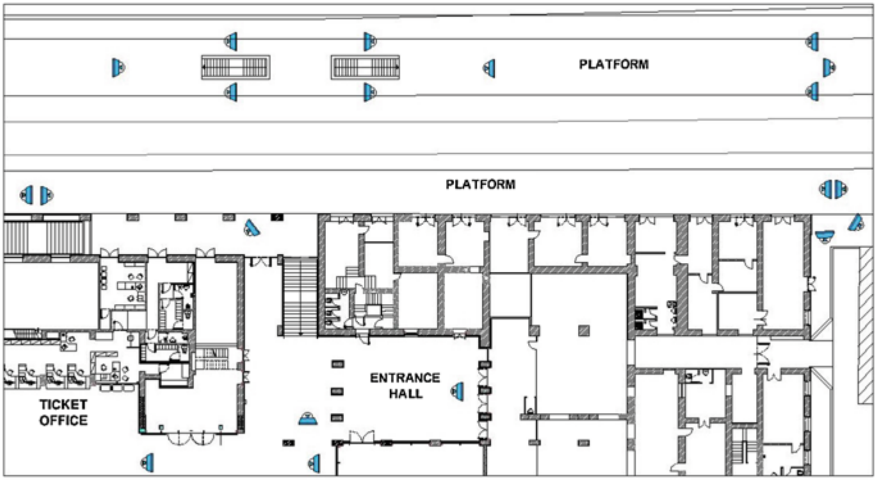


Fig. 5 Example of a station CCTV system draft

The CCTV real time and recorded images are transmitted, continuously or on demand:

- To the local station (if present):
- To the remote control stations.

The most suitable *Control Station* is periodically identified planning the project with local law enforcement in order to guarantee well-timed interventions.

The most recent CCTV systems are equipped with image analysis tools able to generate real time alarms for the security operators, so as to efficiently prevent events which could threaten security. The main functions of the image analysis, implemented in the new structures are:

- Motion detection: the system reveals the intrusion of unauthorized people into a protected area;
- Slow motion: the system reveals the prolonged presence of an object in the field of view. In that case, the system can generate an alarm if unattended objects are revealed;
- Anomalous behaviors detection: detection of situations where the same person roams or stays over a predetermined period of time on the scene.

An appropriate *level of lighting* in the most isolated areas of stations (e.g. underpass, second entrances) together with CCTV systems is effective deterrents against malicious acts (Fig. 6).

In stations it is also a good practice to use *anti-terrorism bins* for the garbage, which have a good deterrent power against potential sabotage or illicit activities (explosive, combustive material, etc.). The anti-explosion bins have the peculiarity to show the garbage bag, in order to allow the law enforcement and occasionally the customers to check the content.

Infrastructural interventions are often utilized to guarantee the security of public space. Gates and enclosures aimed at guaranteeing a limited number of entrances/exits into the station, monitored by CCTV systems or law enforcement are in this category. The existence of second entrances to the stations, far from the most frequented areas can cause security problems in specific socio-economic context, related to the entrance of malicious or homeless people.

The cooperation with the municipalities and the other public transportation companies (especially in large metropolitan areas) is of utmost importance for the railway assets protection, in order to safeguard the station clients through the integration of internal and external security systems:

- CCTV systems and SOS rescue columns outside the railway jurisdiction area;
- Appropriate lighting in the external service area, in the walk access and in parking;
- Enlightenment, decor, control of the underpass given for extended loan to the municipality;
- Station accessibility and interchange with other transportation systems (e.g. bus stops proximity);

Fig. 6 Underground stop

- Urban decor of area adjacent to the station (vegetation cutting, absence of dumps and huts);
- Law enforcement control of the territory surrounding the station.

14.4 Security Logic for the Main Head Stations and New High Speed Structures—Layout

The new high speed stations can be designed and built applying the “Security by design” concept, borrowed from the information security field, i.e. designing new infrastructures taking into account the security issues from the first feasibility studies.

In fact intervention often happens after the accomplishment of the works with “buffer” actions which mitigate the security gaps, but do not achieve the same efficiency and effectiveness of preliminary studies during the design phase. Further the “Security by design” approach significantly reduces costs and enhances the designers’ awareness on the topic. Conversely, the main head stations instead are already running adjustment interventions according to international best practices. In particular, it is possible to identify technical solutions in order to install *access* *control passages* in the quay area. The aim is to divide the commercial area from the quays through attended passages to monitor the access, in the most sensitive areas from the security point of view, of individuals not interested in taking the train and often responsible for illicit actions (thefts, harassment, etc.) against customers and railway personnel.

An effective barrier is the implementation of slide-closing modules along the track entrance, possibly integrated with the traditional turnstiles; these modules can be opened or closed depending on the need to manage the entering flow towards the tracks and the exit flow from the trains and towards the station. Because of the existence of many different travel documents, the access control of these passages cannot be totally automatic, thus a human presence will be needed. Furthermore, the passages will help manage the ashore anti-evasion controls and help filter activity in case of security criticalities (e.g. sports fans management, important events, etc.).

Another sensitive area within a railway station is the *luggage storage*, where various types of explosives could be allocated for terrorist purposes. Hence it is necessary to position this service at an appropriate distance from highly crowded zones and from bearing structures of the station building. For the same reasons, the luggage storage location should not have sensitive areas on top or underlying and it should be distant from glass surfaces or other materials which could produce splinters. Double walls with a cavity between the luggage storage and adjacent rooms are required. It is necessary for the safe-deposit box to be fabricated with a material such that the box would be expelled in a unique block in case of an explosion, without producing splinters. Finally, the safe-deposit boxes should be equipped with appropriate technological devices for the luggage control (e.g. X-ray systems) and for the access control, in order to allow only the access of authorized personnel. The minimum set of required equipment also includes a video-surveillance system inside and outside the luggage storage.

Particular attention must be paid to the appurtenant *parking* management in large stations, often located in underlying or top positions with respect to tracks, especially in the new high-speed stations.

The parking access should be appropriately managed, arranging:

- Plate reading-based checks;
- Detachment of the areas dedicated to commercial vehicles for station services/providers/maintenance from those reserved for private vehicles;
- Inhibition to vehicles with a height greater than 2.10 m in the client-reserved parking areas in order to prevent the access of potentially dangerous vehicles such as trucks or vans which could bring flammable or explosive wares/substances;
- Parking closure at night when there is no railway circulation, with suitable shutter/gates.

14.5 Control Room

For a railway corporation it is necessary to have all the security systems in strategic locations on the territory and monitored on demand from a centralized control room connected to the *Management*. The room should also be able to manage the priorities, the accounts, and the access authorizations to those systems for the entitled personnel, in addition to the security systems. Thus, the *Management* receives an essential support for the current phenomena assessment (operational anomalies, "important event" management, sports fans and protesters transportation, etc.) thanks to the criticality joint arrangement.

The main activities the Control Room should support in case of security criticality or important events management are listed below:

- Presentation of security information acquired via CCTV systems to the *Management* and to authority users;
- Report of data coming from the dedicated assessment system regarding the current or potential risk level;
- Management of the relationships with the Institutions and the Public Security Authorities;
- Report of unambiguous and updated information regarding the current situation to the management also through the activity of the personnel on the territory.

14.6 Security for Railway Undertakings

As mentioned in the introduction, the strategic assets of a railway undertaking are:

- Rolling stock
- Ticket office and self service
- Stocks/Structures.

Installations on the Train

The rolling stock security measures are aimed at protecting the company assets against sabotage and attacks, protecting the personnel onboard and at preventing malicious actions which could damage the train.

The Mechatronic Key

The mechatronic keys are utilized to safeguard the trains, for example opening/closing systems for the driver's compartment and wagons, instead of the previous utilized system (Fig. 7).

The considered system includes an electro-mechanic European cylinder lock. The opening key is equipped with a microchip with a LCD display and a battery, with the battery level indication available. In particular, these keys are characterized by unique electronic codes, internal memory, profile cylinder and anti-drilling and

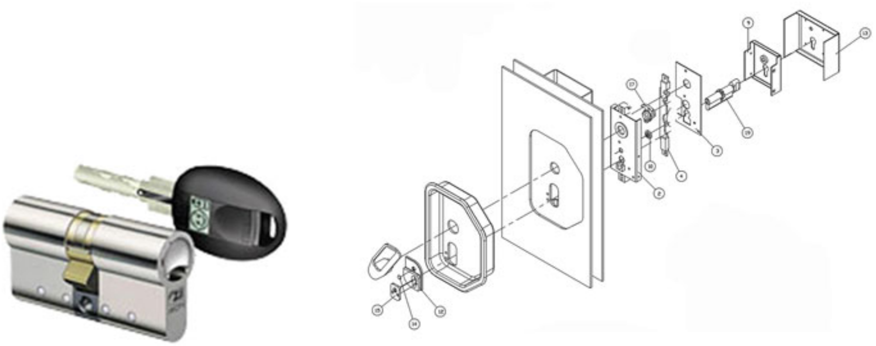


Fig. 7 Mechatronic key

anti-spurt protection. Managed by appropriate software, the internal memory is able to store at least several tens of events and the battery lasts for thousands of opening and closing events, depending on the type of the memory.

Advantages are expected in the following aspects:

- Once closed, the driver's compartment will be inaccessible if not in possession of the key
- Only the train operators are authorized to access the driver's compartment

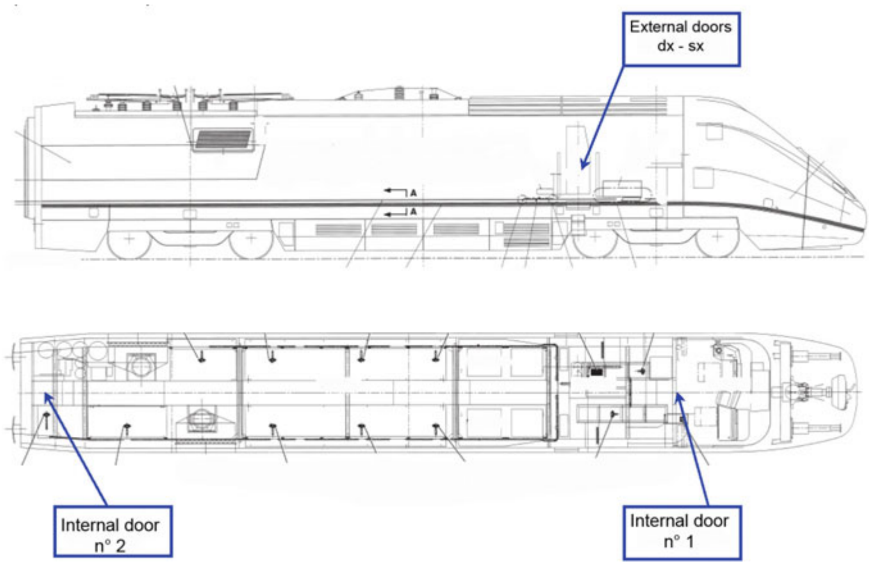


Fig. 8 Train Entrances

- Only authorized operators can access trains
- The keys and the locks will record the date and time of access
- After accessing the compartment, the same person will be responsible for closing (Fig. 8).

Video-Surveillance and Security

The onboard video-surveillance system provides a service aimed at guaranteeing the protection of the train and of passengers during the travel. The common carriage areas are under surveillance to prevent illegal behaviors and assure the complete security of passengers.

The architecture of the video-surveillance systems are constituted by the following components:

- CCTV system
- Management Server
- Data transmission devices.

Advantages:

- Number of onboard crimes reduced (thefts, assaults, vandalism, etc.) as a result of the deterrent effect of the cameras, with subsequent decrease of related costs, including false claims for damages;
- Reduced incident response time;
- Both law enforcement and security personnel can access the images (Figs. 9 and 10).

Ticket Office and Self-service Machines Security

The active measures adopted in *ticket offices* are:

- Sensors installed on glass walls, windows and doors
- Volumetric alarms
- Access control
- Cameras: placed in the hall, in office and back office, normally turned-off during the office hours but they can be activated at any time from the personnel through the anti-robbery pushbutton.
- Both law enforcement and security personnel can access the images.

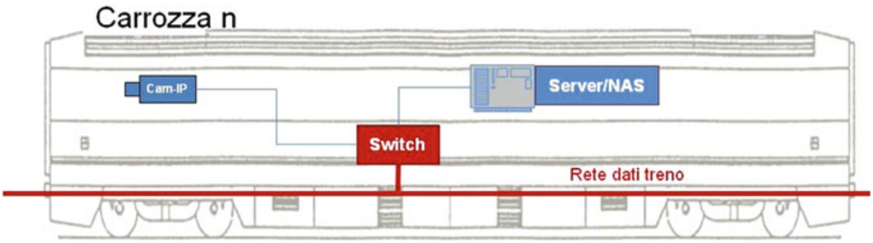


Fig. 9 Wagon CCTV Architecture

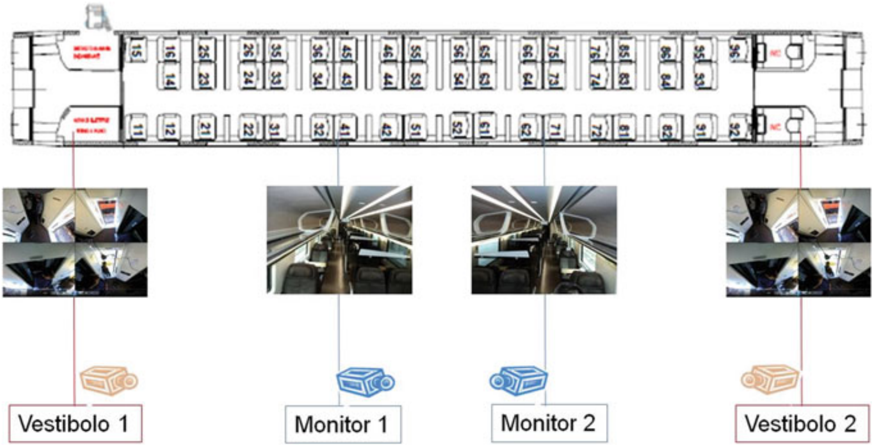


Fig. 10 CCTV on board

The passive measures are:

- Armored shutters
- Gates
- Concrete or full brick brickwork
- Strongboxes, continued counter.

In addition, the self-service machines are equipped with active (cameras and alarm sensors) and passive (armor, strongbox and anchoring) systems.

Train Stop Stocks Security

The indications are the same as under the "Components of a Security System" section.

15 Conclusions

The "open" context of the railway infrastructure, the related risks and vulnerabilities, and the need to adapt counteractions to the new types of criminal acts, require a constant and systemic approach and a strong synergy with institutional and international partners.

The economic needs of the Security corporate business are due to experience a progressive enlargement as transport operators and the community in general are increasingly demanding safer, more livable and decent railway environments, also taking into account the persistent critical conditions in the current socio-economic scenario.

The security activity should fully contribute to provide customers of the railway transport and stations with higher levels of service quality.

The security function within the Company's structure cannot but reflect the requirements expressed by the community, also by recruiting and constantly training the personnel and developing a sense of involvement.

Supporting such a belief, with constant efforts and awareness activities within the railway organizations, targeted at providing a modern, specialized, and differentiated security response, is strictly necessary to contribute to the current European changes with an active approach.

Appropriate financial plans for the technological and infrastructural systems, achieving the requests of human resources (education, experts recruitment, etc.), and finding the right balance in the relationships with governmental bodies in charge of public security are essential keys for the success of the adopted strategies.

Vulnerability Assessment in RIS Scenario Through a Synergic Use of the CPTED Methodology and the System Dynamics Approach

Francesca De Cillis, Maria Carla De Maggio and Roberto Setola

Abstract The 9/11 attacks dramatically stressed the fragility of our CI against terrorist and criminal actions. For their peculiarities and symbolic value, CI are largely exposed to attacks, as evident by the large number of targeted incidents that occurred. Within this context, the Railway Infrastructure System (RIS) holds a high-ranking position. Vulnerability analysis and quantitative simulation approach play a crucial role in identifying weak-points and outlying new and more appealing protection strategies. In this chapter, a vulnerability assessment mean fulfilled through a synergic use of System Dynamics method, CPTED (Crime Prevention Through Environmental Design) multidisciplinary approach and crime opportunity theories is depicted. The aim consists in analyzing how different factors may influence the railway asset attractiveness, fragility and vulnerability. Starting from the CPTED technique and situational crime prevention theories, we were able to outline which are the main physical, social and environmental aspects that provide opportunity for criminality in railway scenarios. Using the System Dynamics approach, we propose a pattern to model the railway asset scenario, integrating physical aspects and social factors. Results of simulations reproducing different operative conditions are presented and analyzed.

Keywords Railway infrastructure system security · CPTED · Situational crime prevention · System dynamics

F. De Cillis (✉) · M.C. De Maggio · R. Setola
Università Campus Bio-Medico di Roma, Rome, Italy
e-mail: f.decillis@unicampus.it

M.C. De Maggio
e-mail: m.demaggio@unicampus.it

R. Setola
e-mail: r.setola@unicampus.it

R. Setola et al. (eds.), *Railway Infrastructure Security*, Topics in Safety, Risk, Reliability and Quality 27, DOI 10.1007/978-3-319-04426-2_4

1 Introduction

In the last few years, the subject of security in infrastructure facilities gained interest among engineers, security professionals, public and private entities. Critical Infrastructures (CI) are the most important support for life in the built environment, bringing communities to civilized standards of life. They are the most feasible indicators of the economic capacity of the most advanced countries, but at the same time are susceptible to potential threats with devastating consequences for human life and economy.

The 9/11 attacks dramatically stressed the fragility of our CI against terrorist and criminal actions. For their peculiarities and symbolic value, CI are largely exposed to attacks, as evident by the large number of targeted incidents that occurred. Within this context, the Railway Infrastructure System (RIS) holds a high-ranking position. The sheer number of incidents worldwide demonstrates the attractiveness of RIS targets for criminals and terrorists. The high fatality rates, the open and accessible design, heavy crowds and basic reliance for survival within cities all serve as contributing factors in deducing why the RIS is considered a soft target for assailants [1].

Vulnerability analysis and quantitative simulation approach play a crucial role in identifying weak-points and outlying new and more appealing protection strategies. As mentioned in the Chap. 1, the European Commission (EC) co-funded project METRIP is devoted to the development of methodological tools aimed to increase the protection of a critical railway infrastructure system. The basic idea is that an effective protection strategy has to be based on the development of tools using quantitative measures of the criticality levels of a single asset and/or of the entire system [2].

As mentioned in [1], the vulnerability analysis relies on the evaluation of the assets' main features, the description of the attack scenarios, and the type of the protection devices, which the assets are equipped.

In this chapter, we are going to depict a vulnerability assessment mean fulfilled through a synergic use of System Dynamics method, CPTED (Crime Prevention Through Environmental Design) multidisciplinary approach and crime opportunity theories. The aim consists in analyzing how different factors may influence the railway asset attractiveness, fragility and vulnerability.

Starting from the CPTED technique and situational crime prevention theories, we were able to outline which are the main physical, social and environmental aspects that provide opportunity for criminality in railway scenarios. Using the System Dynamics approach, we propose a pattern to model the railway asset scenario, integrating physical aspects and social factors. Results of simulations reproducing different operative conditions are presented and analyzed.

The elaboration of a dynamic model could help one to analyze the potential effect of integration/addition of protection devices within a specific asset and the impact inferring from building environment improvements. Ultimately, the profile could aid professionals of which would be the overall effects of undertaken actions in the protection level of the asset, giving at the same time a realistic probability and effects of an attack to the asset itself.

To make realistic simulations, we used the results inferred from the RISTAD [2] (RIS Terrorist Attacks Database), set up inside the METRIP project. It includes a collection of about 500 criminal incidents and terrorist assaults involving RIS that occurred worldwide from 1970 to 2011.[1]

The Sect. 2, briefly overviews the CPTED approach and outlines which are the main factors that can influence railway asset's security.

In the Sect. 3, a short description about System Dynamics method and the implemented profile will be depicted. The Sect. 4 briefly describes the RISTAD and illustrates the results inferred from simulations. Conclusions and future works are illustrated in the Sect. 5.

2 The CPTED Methodology

Since the events of 9/11, the security and urban design fields face new challenging to design, redesign, retrofit and renovate, and operate assets to ensure the health, safety and welfare of occupants, visitors and the public. The urban designer must now integrate and combine security concepts, architectural elements and security technologies into a balanced holistic solution.

The process of designing security into architecture is known as Crime Prevention Through Environmental Design (CPTED). CPTED is a multi-disciplinary approach, drawing on criminology, planning and environmental psychology, and is specifically located within the field of environmental criminology, deriving theoretical support from *opportunity theories* such as rational choice theory, routine activities and situational crime prevention theories [3].

CPTED involves designing the built environment to reduce the opportunity for, and fear of, crime and disorder. This approach to security design recognizes the intended use of space in an asset and is different from traditional security practice, which focuses on denying access to a crime target with barrier techniques such as locks, alarms, fences, and gates. CPTED specialists believe that natural and normal uses of the environment can meet the same security goals as physical and technical protection methods.

The theory has begun taking shape from 60s, getting inspiration from the work of Elizabeth Wood, Jane Jacobs and Schlomo Angel. The term CPTED was coined about 10 years after by the criminologist and sociologist C. Ray Jeffery. A clear dissertation about the theory first appeared in his own book in 1971, "Crime Prevention Through Environmental Design" [4]. Concurrently, the architect Oscar Newman developed a more limited approach, termed *defensible space*. While Jeffrey's book was ignored, Newman's principals were widely adopted but with mixed success.

[1] Readers interested in RISTAD can refer to [2] or to the website http://metrip.unicampus.it.

Later models of CPTED were developed based on the Newman Model, with Crowe's work being the most popular.

Currently, CPTED is popularly understood to refer strictly to the Newman/Crowe type models, with the Jeffery Model treated more as multi-disciplinary approach to crime prevention, which incorporates biology and psychology.

A revision of CPTED, initiated in 1997 and termed second Generation CPTED, adapts CPTED to offender individuality, further indication that Jeffery's work is not popularly considered to be already a part of CPTED.

In the next sections, a short description about the historical evolution of the theory, its key aspects and their application into the railway field will be presented.

To trace a comprehensive overview about CPTED, we referred to [3, 4]. For a deep understanding about the theory, we suggest readers to consult the above-mentioned texts.

2.1 CPTED's Historical Evolution and Main Influences

As stated by Crowe [5], CPTED bases on the ground hypothesis that the proper design and effective use of the built environment can lead to a reduction in the fear and incidence of crime, and an improvement in the quality of life. Brantingham and Faust asserted that CPTED is concerned with identifying conditions of the physical and social environment that provide opportunities for criminality, and the modification of those conditions in order to reduce such opportunities. Wallis attested that CPTED's objective is to proactively prevent crime, as compared to the reactive (and often ineffective) strategies of most criminal justice systems (police, courts and correctional facilities) [3].

The earliest forms of crime prevention by design can be traced in the 1960s and 1970s. Starting from 60 with Elizabeth Wood, moving to CPTED largest supporter C. Ray Jeffrey as far as to latest refinement by Cozens and Crowe, in the last 50 years extensive effort has been done in the CPTED framework. In Table 1, a brief description of the main contributions to the CPTED means is presented.

Traditional criminological theories are concerned with *criminality*. They seek to explain how biological factors, developmental experiences and/or social forces create the criminal offender. The CPTED perspective takes a very different view, finding location within the field of *environmental criminology*. In this perspective, *crime* is the object of interest while the offender is just one element of a criminal event.

Rational choice, situational crime prevention, routine activity, opportunity model, *geography of crime*, and *hot spots of crime* are all examples of criminological theories that explain factors that provide criminal opportunities. Such theories, usually classified as *crime opportunity theories*, had great influence on CPTED.

Table 1 Main contributions to CPTED theory

60s	Elisabeth Wood	American sociologist. She developed guidelines for addressing security issues, placing emphasis on design features that would support natural surveillability
	Jane Jacobs	American urban planner. Founder of the "eye on the street" theory
	Schlomo Angel	Physical environment exert a direct influence on crime settings. Surveillance by the citizenry and the police can be facilitate by territories delineation, reducing or increasing accessibility by boundaries and circulation networks
70s, 80s	C. Ray Jeffery	Criminologist, Florida State University and CPTED founder. Environments design and implementation of social policies could systematically decreased the rewards for criminal behavior and increased the risks. Criminal behavior could not occur without *opportunity*
	Oscar Newman	*Defensible space* theory initiator. Territorial influence (real and symbolic markers such as fences and gates, signage), surveillance opportunities (windows, routing of pedestrian traffic, elimination of blind spots), placing residential structures close to safe areas, designing sites and buildings not perceived as vulnerable, decrease crime opportunity
80s, 90s and 2000	James Q. Wilson, George L. Kelling	Founders of the *broken windows* theory: small acts of deviance, such as littering, graffiti, and broken windows, could escalate into serious crime. Property maintenance assumed as also in CPTED strategy
	Patricia and Paul Brantingham	Founders of *environmental criminology* theory. *Perception of target availability* and *vulnerability* influence criminal choices (target that appear open, accessible and vulnerable, or offering more potential escape routes)
	Severin Sorensen and Ronald V. Clarke	They developed a new CPTED curriculum that used s*ituational crime prevention.* The consequent CPTED follow-up conducted at various sites showed statistical reductions in crimes from 17 to 76 % depending on the basket of CPTED measures
	Greg Saville and Gerry Cleveland	Founders of second generation CPTED. They exhorted practitioners to consider the original social ecology origins of CPTED, including social and psychological issues beyond the built environment (social cohesion, connectivity, community culture, threshold capacity)
	Timothy Crowe	American criminologist. He developed a comprehensive set of guidelines to reduce opportunities for crime in the built environment

The environmental perspective is based on two main premises: the *criminal behavior* and the *crime distribution*.

The *criminal behavior* is significantly influenced by the nature of the immediate environment in which it occurs. The environment is not just a passive backdrop for criminal behavior; rather, it plays a fundamental role in initiating the crime and shaping its course. Moreover, the *distribution of crime* in time and space is non-random. Because criminal behavior is dependent upon situational factors, crime is patterned according to the location of criminogenic environments. Crime will be concentrated around crime opportunities and other environmental features that facilitate criminal activity.

The design of buildings, the arrangement of streets, public facilities and other outdoor spaces may influence the opportunities for crime and affect the level of fear of crime. Cautious environmental design may help make places safer and less vulnerable to crime, as well as help people to feel more comfortable outdoors. Numerous studies (e.g., [3, 4, 6]) have proved that the built environment affects humans' behavior in terms of fostering or preventing criminal acts.

As well as environmental criminology, current models of CPTED evolved principally from Newman's model of *defensible space* (Fig. 1). According to Newman, defensible space promotes the use of design to enhance territoriality and promote a *sense of ownership* by delineating between private and public space, using real and symbolic barriers. Building and site design to increase *surveillance*

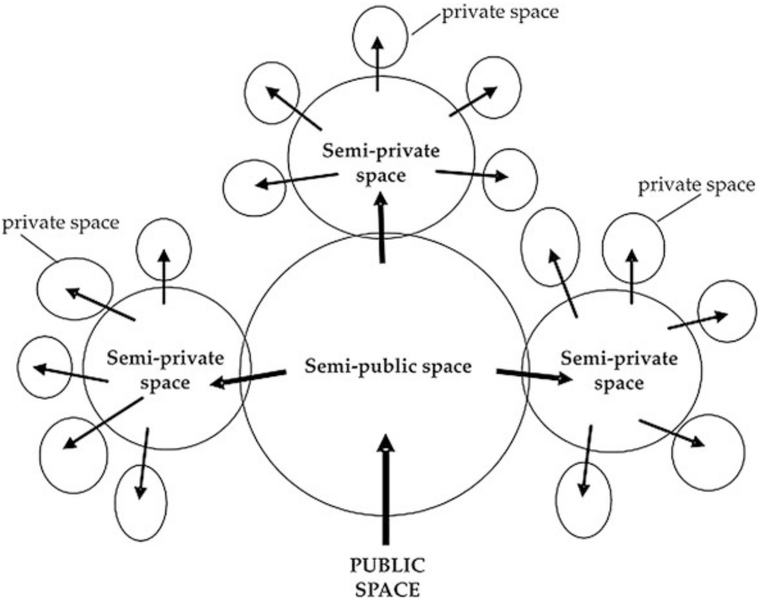


Fig. 1 Hierarchy of defensible space. *Note: Arrows* indicate entrance and exit points at different levels of the hierarchy. *Source:* Richard Wortley and Lorraine Mazerolle, Environmental Criminology and Crime Analysis. Adapted from Newman, 1973: levels of the hierarchy

(Jacobs' terminology referred to this as *eyes on the street*) and the *image of housing* are also central to defensible space. The wider environment or *geographical juxtaposition* and the *anonymity* are also important and affect crimes rate.

2.2 CPTED: Key Elements

As with defensible space and crime opportunity theories, CPTED draws heavily on behavioral psychology, and is concerned with the relationships between people and the environment.

The way people react to an environment is commonly influenced by environmental cues, which are variously perceived and decoded [3]. Elements that make normal or legitimate users of a space feel safe, may discourage abnormal or illegitimate users from pursuing undesirable behaviors.

CPTED requires natural strategies to be incorporated into human activities and space design. Crime prevention has traditionally relied almost exclusively on labor intensive (e.g. security guards and police patrols) and mechanical devices (e.g. security cameras, locks and fences) which increase existing operating costs for personnel, equipment and buildings.

As stated in [3], access control, surveillance, and territorial reinforcement represent the three most common CPTED strategies.

In general, each of these strategies can be implemented through:

- organized methods: manpower, (e.g., police, security guards, receptionists);
- mechanical methods (e.g., technology products, tools, alarms, CCTV, gadgets);
- natural methods (e.g., site planning and design, landscaping, signage).

CPTED theory stands on the last strategies, because CPTED specialists believe that natural and normal uses of the environment can meet the same security goals as physical and technical protection methods.

Territorial reinforcement is a design concept directed at promoting notions of proprietary concern and a sense of ownership in legitimate users of space, thereby reducing opportunities for offending by discouraging illegitimate users. Early CPTED ideas, now referred to as first-generation CPTED, considered territorial reinforcement as the primary concept of CPTED strategy.

The *Natural territorial strategies* include the use of symbolic (e.g. signage) and real barriers (e.g. fences or design that clearly defines and delineates between private, semi-private and public spaces), walls and landscaping. Other forms of territorial reinforcement include *organized territorial strategies* (e.g., neighborhood crime watches, guard stations) and *mechanical strategies* (e.g., perimeter-sensing systems).

Surveillance strategies are design concepts directed at keeping intruders under observation. It consists of increasing visibility within and around a facility by encouraging its legitimate occupants and casual observers to increase the observation, detection, and reporting of trespassers or misconduct [4]. In this framework, *natural strategies* include the proper placement of windows, low landscaping, raised entrances, removing obstructions to enhance sightlines, including softening "hard corners" to increase visibility and standoff distance.

Organized surveillance strategies include police, guard patrols; lighting, and CCTV are *mechanical strategies* for surveillance.

Access control is a design notion directed at reducing the opportunity and accessibility for crime. The focus of access control strategies is to deny access to a crime target and create in offenders a perception of risk and detection, delay, and response. *Natural methods* of access control make use of spatial definition (wall, floors, doors and windows) and circulation patterns. An example of natural design is the use of security zoning. By dividing space into zones of differing security levels (e.g. unrestricted, controlled, and restricted) sensitive areas can be more effectively protected. Alternative forms include *organized methods* (e.g., security guard forces, guards patrol) and *mechanical strategies* (e.g., the use of locks and card key systems).

Refinement of CPTED has added several other strategies including activity support, image/space management and target hardening.

Activity support involves the use of design and signage to encourage intended patterns of usage of public space. As stated by Wortley and Mazerolle [3], the placement of safe activities (kiosks, offices, libraries, etc.) in unsafe locations, serve as magnets for ordinary citizens who may then act to discourage the presence of criminals.

Image/space management and *routinely maintaining* the built environment ensures that the physical environment continues to function effectively and transmits positive signals to all users. The significance of the physical condition and image of the built environment, and the effect this may have on crime and the fear of crime, have long been acknowledged (e.g., the *broken windows theory*, by Wilson and Kelling [3]).

A lack of care indicates loss of control of a space or area and can be a sign of tolerance for disorder. Establishing care and maintenance standards and continuing the service preserves the intended use of the space/area.

Target hardening increases the efforts that offenders must expend in the commission of a crime and is the most established approach to crime prevention. However, there is much disagreement concerning whether or not target hardening should be considered as a component of CPTED. It is directed at denying or limiting access to a crime target using physical barriers (e.g., fences, gates, locks, electronic alarms and security patrols), appearing very similar to mechanical and organized strategies for access control.

It is argued in CPTED that by optimizing opportunities for surveillance, clearly defining boundaries (and defining preferred use within such spaces) and creating and maintaining a positive image, urban design and active management can discourage offending. This is explained by the fact that offenders are potentially more visible to law-abiding others, and therefore perceive themselves to be more at risk of observation and subsequent apprehension. Additionally, a well-maintained and appropriately used environment can signify that a sense of ownership and proprietary concern exists within the community and offenders may perceive that residents are more vigilant and more likely to intervene during the commission of a crime.

2.3 The Application of CPTED to Railway Infrastructure System

CPTED has been applied in a range of diverse environments, including residential, commercial/retail, schools, universities, hospitals, car parks, offices, convention centers, stadiums and public transport [7].

Several studies (e.g., [8–13]) have regarded the application of CPTED to RIS. For example, in [13] La Vigne discusses how, using CPTED principles, Metro Washington's subway station exhibited significantly lower levels of crime than other stations and the local environment in which it is located.

Results in [8] show that opportunities for crime are dependent on stations' environmental attributes, type of neighborhood in which they are located and city context (Fig. 2). Researchers observed that although crime rates are obviously affected by the long-term socio-economic context of these stations (i.e., population density, housing mobility, police patrol in the neighborhood), specific

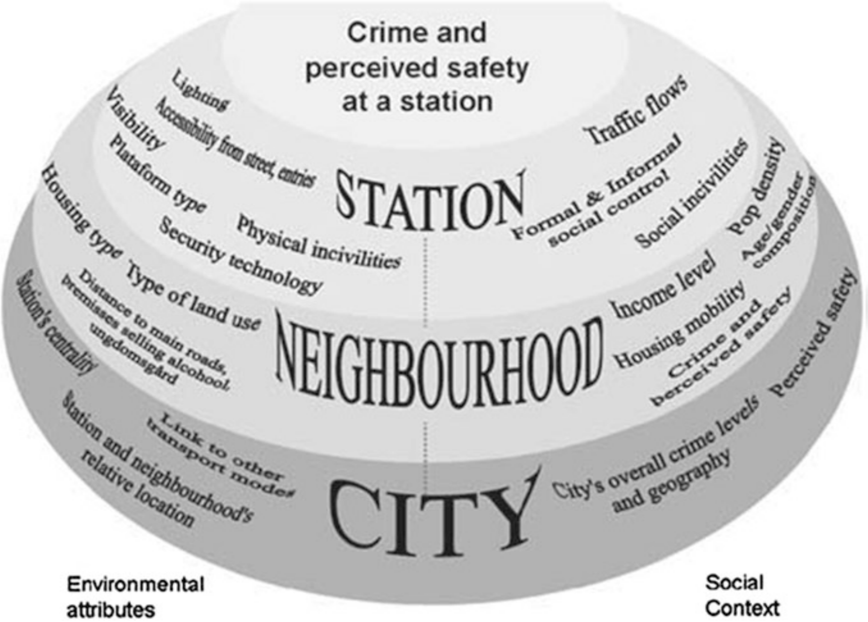

Crime and perceived safety at a station
Lighting
Accessibility from street, entries
Visibility
Plataform type
Physical incivilities
Security technology
STATION
Traffic flows
Formal & Informal social control
Social incivilities
Pop density
Age/gender composition
Housing type
Type of land use
Distance to main roads, premisses selling alcohool, ungdomsgård
NEIGHBOURHOOD
Income level
Housing mobility
Crime and perceived safety
Station's centrality
Link to other transport modes
Station and neighbourhood's relative location
CITY
City's overall crime levels and geography
Perceived safety
Environmental attributes
Social Context

Fig. 2 Security in underground stations: a tentative conceptual framework [8]

environmental aspects (design and land use of stations) may be reconsidered to better promote security at underground stations.

An interesting application of CPTED is provided in [10]. It is about a study of railway stations in the UK that used CPTED principles in the regeneration and redesign of a local rail network. In this approach, the surveillance of the station platform and waiting areas has been enhanced and the station after the modifications provides minimal opportunities for concealment. Researchers show how the installation of signage has clearly designated and defined the space as an operating railway station, while the design of transparent shelters allowed the station and passengers to interact with the local community, thus reducing the fear of crime. The use of additional way-finding information also enhanced passengers' sense of personal safety.

Significantly, the rail network has witnessed an increase in annual passenger flows and reduced levels of crime and fear of crime.

The use of CPTED strategy in RIS field has been also promoted with success by several security agencies, such as the Security Work Group by the American Public

Table 2 CPTED strategies and applications in RIS field promoted by APTA [14]

Natural surveillance	• Maximize visibility (designing doors and windows to look into public areas, parking lots, roadways or sidewalks)
	• Adequate illumination of public areas
	Organized strategies: police and guard patrols. Mechanical surveillance strategies: lighting and CCTV. *Natural strategies*: widows, low landscaping and raised entrances
Natural access control	• Use landscape structures and architectural designs to discourage access to private areas
	• Design streets, roadways, pathways, driveways and neighborhood gateways to mark public routes
	• Signage
Territoriality	• Clearly distinction between restricted and public areas
	• Implementation of landscape plantings, pavement surface treatments, fences, T-walls, etc., to reinforce the territory of restricted or public areas
	• Create physical designs that enhance or extend the sphere of influence for developing a sense of proprietorship
	Organized strategies: neighborhood crime watches, receptionists, and guard stations. *Mechanical strategies*: perimeter-sensing systems. *Natural strategies*: fences, walls and landscaping
Activity support	• Identify activities that create community involvement in the public space
	• Ensure that public space activities complement other activities in the same space
Maintenance	• Maintain the cleanliness and functionality of revenue and nonrevenue areas and spaces
	• Inspect assets, equipment and facilities to ensure satisfactory operation
	• Removing trash and debris; enforce a zero tolerance policy to graffiti and vandalism. Maintaining aesthetic appearance of assets, equipment and facilities

Transportation Association (APTA). The *APTA Recommended Practice* [14] provides guidance about the use of crime prevention through environmental design at revenue and non-revenue transit facilities. The APTA report provides guidelines in order to incorporate security considerations prior to designing, planning, building or remodeling transit facilities and areas; and to identify all pertinent stakeholders in the process application of CPTED concepts and strategies. Table 2 provides a brief description about the CPTED strategies in RIS promoted by APTA.

3 The Systems Dynamics Approach

The System Dynamics (SD) approach is a powerful methodology and computer simulation modeling technique for framing, understanding, and discussing the dynamic behavior and no-intuitive casual relationships among variables in complex systems.

Originally introduced by Jay W. Forrester in the 1960s and used to help corporate managers improve their understanding of industrial processes, SD is now currently used throughout the public and private sector for policy analysis and design.

System theory approaches rely almost exclusively upon the use of past data to predict the future. The use of historical data allows researchers to relate frequencies or specific occurrences to certain events, time frame characteristics and/or populations, as well as enabling them to make inferences based on observations. Although this sometimes is helpful, they frequently can lead to very wrong predictions, especially when the actual outcome is counter-intuitive. In contrast, the SD approach is based on identifying individual causalities and how they combine to create, often non-linear, feedback loops that are the causes of the counter-intuitive outcomes. It is important to point out that the expected outcomes are not necessarily quantitative point predictions for a particular variable, but rather a measure of the dynamic behavior pattern of the system, given the inputs and conditions in the model.

System Dynamics has been used for a wide range of purposes, such as to capture the dynamic relationship of energy and the economy, to model the world petroleum market over a period of thirty decades, to explore dynamics of economic growth, or to analyze the environmental implications of international trade.

Most recently, SD approach has been used to analyze complex physical and social phenomena, such as Terrorism, in order to design policies for management and change or to explore effects of counterterrorism policy [15–17].

Next section brief illustrates the main features of SD. To emphasize the crucial aspect of the methodology, an easy application of SD approach in the Terrorism-Counterterrorism scenario will be also presented, using the open source platform Vensim® by Ventana System Inc.

3.1 Systems Dynamics Main Features

The core of the SD strategy consisting in representing the system structure in terms of stocks, flows, and the causal mechanisms that govern their rates of change. Stocks are essentially pool or inventory where accumulation of elements takes place, while flows represent rates at which elements move through the system between stocks.

The stock-flow structure allows representing in a simple way complex dynamical process. According to the principle of accumulation, dynamic behaviour arises when element flows, collecting or accumulating in the stock. In SD modelling, both informational and non-informational entities can move through flows and accumulate in stocks.

From a SD point of view, a system can be classified as either open or closed. Open systems have outputs that respond to, but have no influence upon, their inputs. Closed systems, on the other hand, have outputs that both respond to, and influence, their inputs. Closed systems are thus aware of their own performance and influenced by their past behaviour. In this framework, feedback loops are the building blocks for articulating the causality represented in the models.

Of the two types of systems, the most prevalent and important, by far, are closed systems. In those systems, stocks and flows are usually part of feedback loops, and joining feedback loops by nonlinear couplings can often cause counterintuitive behaviour. The interaction among the various feedback loops in a model can represent and explain the dynamical behaviour of complex systems.

Closed systems are controlled by two types of feedback loops: positive and negative loops. Positive loops portray self-reinforcing processes wherein an action creates a result that generates more of the action, and hence more of the result. Positive feedback processes destabilize systems and cause them to move from their current position. Thus, they are responsible for the growth or decline of systems, although they can occasionally work to stabilize them. Negative feedback loops, describe goal-seeking processes that generate actions aimed at moving a system toward, or keeping a system at, a desired state. Negative feedback processes stabilize systems, although they can occasionally destabilize by causing them to oscillate.

In the field of SD, positive and negative feedback processes are often described via a simple technique known as causal loop diagramming. Causal loop diagrams are maps of cause and effect relationships between individual system variables that, when linked, form closed loops.

Figure 3, for example, presents a causal loop diagram aimed to capture the possible effects of the implementation of policies aimed at reducing terrorism acts. The arrows that link each variable indicate places where a cause and effect relationship exists while the plus or minus sign at the head of each arrow indicates the direction of causality between the variables, when all the other variables (conceptually) remain constant.

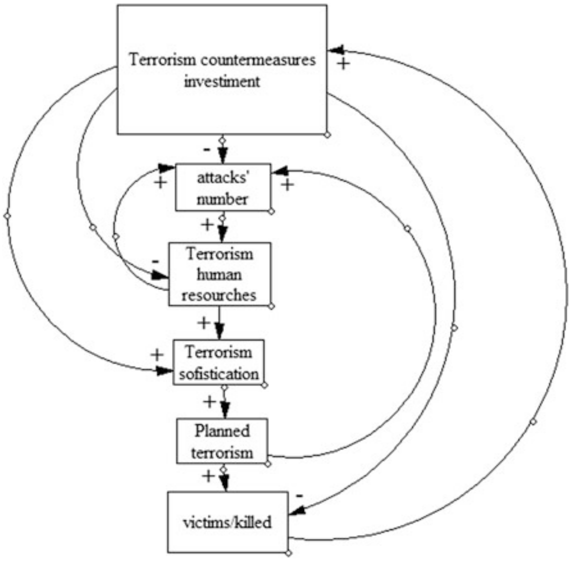


Fig. 3 Causal loop diagram of terrorism countermeasures investment by Governments (modified from [17])

The causal diagram shown in Fig. 3 can be interpreted in the following way. As the Government increases its investment in anti-terrorism countermeasures, the number of the perpetrated attacks and the number of Terrorist human resources decrease. On the other hand, the anti-government sentiment (as felt by extremist groups) increases. This sparks the hatred extremist groups that use religion, force and/or political causes to obtain resources and recruit more members. Therefore, Terrorist human resources (recruitment) increase. As Terrorist human resources increase, also terrorist sophistications (strength, lethality and/or capability) increase. As a consequences, the number of terrorist attacks (planned or not) increases as well. These give a boost to the number of victims and killed, causing the increment by the Government of the terrorism-defense resource allocation.

In the next section our models, the main assumption and the simulation results will be provided.

4 The Model

Our model has the objective to show how the adoption of CPTED actions in the railway asset environment could affect the means security. In our SD model, the means selected represent railway stations. Starting from a vulnerability assessment of the assets, we illustrate how the implementation/lacking of CPTED measures have repercussion on the assets' attractiveness, becoming actual the probability of real attacks.

Data input were inferred from RISTAD. It consists in a database including a collection of about 500 criminal incidents and terrorist assaults involving RIS that

Table 3 Techniques of situational crime prevention using CPTED

Increase efforts	Increase risks	Reduce rewards	Reduce provocations
Target harden	Extend guardianship	Conceal target	Reduce frustration and stress
Control access to facilities	Assist natural surveillance	Remove targets	Avoid disputes
Screen exit	Reduce anonymity	Identify property	Reduce emotional arousal
Deflect offenders	Utilize pace managers	Disrupt market	Neutralize peer pressure
Control tools	Strengthen formal surveillance	Deny benefits	Discourage imitation

Modified from Richard Wortley and Lorraine Mazerolle, Environmental Criminology and Crime Analysis [3]. Adapted from CPTED Matrix of Ron V. Clarke

occurred worldwide from 1970 to 2011. RISTAD includes RIS incident/attacks information and data surrounding the characteristics of the targets (i.e., number of tracks, number of daily passengers, station extensions, presence and type of security systems, etc.). This provides us the ability to isolate which environmental elements make a target more "appealing" [2].

CPTED theory and Situational Crime Prevention (SCP) technique represent the starting points from which we build-up the model. In Table 3, the CPTED matrix developed by Clark in 1992 is illustrated. It takes into account techniques for SCP using CPTED that can generally be applied to almost any situation. Our aim focused on the need to select and identify techniques and strategies devoted to enhance railway asset security.

We assume that assets attractiveness and the opportunity of crime to occur can be reduced acting with practical, cost effective, and permanent alterations to the physical environment of the asset. Situational crime prevention measures do not provide for the massive adoption of protection systems, but for a rational uses of the available resources through the implementation of the CPTED means.

Increasing the effort needed to commit crime, *increasing the risks* associated with crime, *reducing the rewards* of crime and *reducing provocations* represent the approaches that we selected from SCP-CPTED strategy to reduce asset appealing. Each methods depends upon one or more CPTED factors, as illustrated in the model (Fig. 4) and in Table 3. Figure 5 illustrates the symbol explanation chart of the model.

The model is composed by several variables and stocks connected by arrow links. The arrow links symbolize existing casual influences among the variables connected. In Fig. 4, the dotted arrow links represent negative feedbacks, while the continuous ones stand for positive causal influences.

Variables represent constants, stocks and flows. Each variable includes specific equations and/or data input. Equations' peculiarities (linear, integral) depend on the nature of the variable selected (constant, stock, flow), as illustrated in the following. By chancing the values of the inputs, the model produces different outcomes, which can be used for a deeper understanding of the dynamical process.

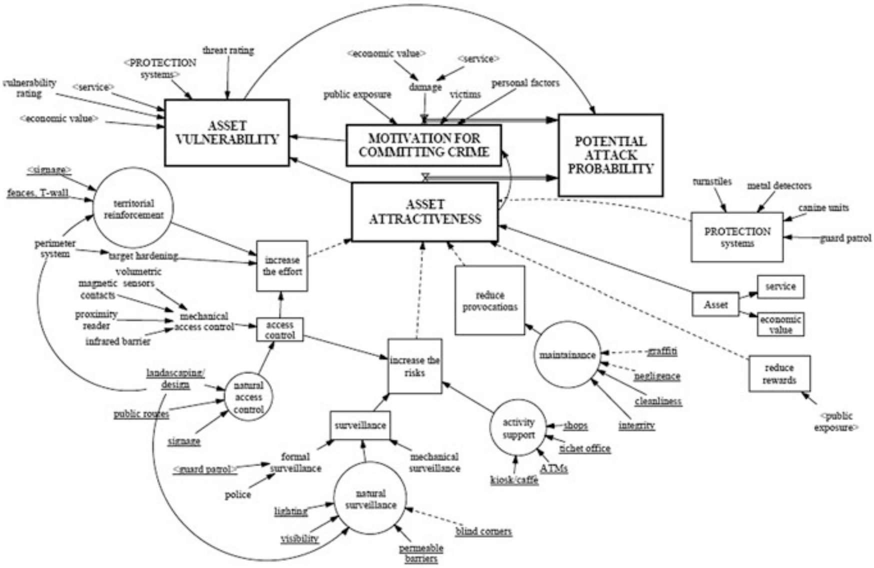


Fig. 4 SD model layout

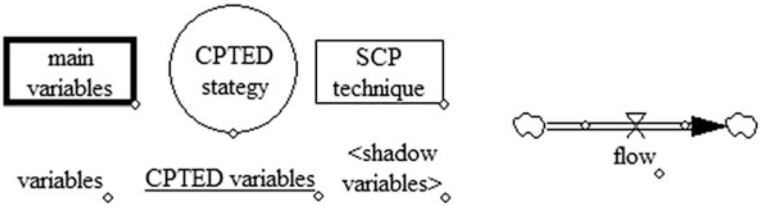


Fig. 5 Symbol explanation chart

The main variables (tick-line box in Fig. 4) are asset vulnerability (variable), potential attack probability (stock), motivation for committing crime and asset attractiveness (flow).

Asset vulnerability hails from a vulnerability assessment analysis of the asset investigated. We use FEMA 426 guidelines for threat and vulnerabilities ratings definition [18]. Data inferred from RISTAD database supply the definition of the asset features (protection systems, asset service and economic value). The flows motivation for committing crime and asset attractiveness contribute to the dynamical behavior of the variable.

The Potential attack probability stock represents the probability that hypothetical attacks can become real. Asset vulnerability, asset attractiveness and motivation for committing crime all contribute to influence its trend. More specifically, both asset attractiveness and asset vulnerability condition in a positive fashion the potential attack probability: the more is the asset attractiveness and/or vulnerability, the more is the risk of attacks. On the contrary, motivation for committing crime decreasing contribute to decrease the probability of attacks.

The motivation for committing crime flow takes into account all factors that contribute to the attack execution, from a terrorist point of view. Well-known triggers are: the public exposure of the target, the potential damage achievable (it depends by the target, i.e. its economic value and the service offered), the potential number of victims, the personal factors (ideological, political, economic aspects) and the asset attractiveness. All these factors contribute to increment the motivation for committing crime.

The asset attractiveness flow is the core of the model. It takes into account the asset features (asset service and economic value), the protection systems with which it is equipped (cameras, turnstiles, canine units, metal detectors, security guards), the implementation/lacking of SCP-CPTED measures in the asset environment. SCP-CPTED measures as well as protection systems, contribute to reduce asset attractiveness, while the asset feature (economic loss, loss of service) contribute to make the target more appealing.

Concerning the equation, as stated, their peculiarities (linear, integral) depend on the nature of the variable selected (constant, stock, flow). Equation (1), for example, depicts the computation of the natural surveillance CPTED strategy. In our model, it is a constant variable, represented by a linear equation as illustrated in Eq. (1).

$$\begin{aligned} natural\ surveillance = {} & w_{visibility} *' visibility' \\ & + w_{landscaping} *' landascaping\ design' \\ & + w_{lighting} *' lighting' \\ & + w_{barriers} *' permeable\ barriers' + w_{CCTV} *' CCTV' \\ & - w_{blindcorners} *' blind\ corners' \end{aligned} \tag{1}$$

Natural surveillance depends on CPTED constant factors as illustrated in Table 2 and Fig. 4 (such as lighting, permeable barriers, blind corners, etc.) through weighting factors. Data input (initial value of the weights, CPTED factors) are expressed in percent; they were inferred from RISTAD and changed throughout simulations accordingly to the implemented strategy.

According to Eq. (1), visibility stands for the perceived awareness of target's existence. More specifically, it means the visibility of the target to the general populace and to the terrorist in particular. In the specific case of railway stations, we assumed the maximum level of target awareness (100 %).

Landscaping design indicates the tendency to decrease target opportunities by a rational use of landscape and building environment (low landscaping, use of landscape structures and architectural designs to discourage access to private areas and to mark public routes; implementation of landscape plantings, pavement surface treatments, fences, etc.). Lighting, permeable barriers and blind corners indicate the presence of adequate illumination, the use of see-through fences (glass-walls, windows) and the possible presence of dead-zone within the asset, respectively. Finally, CCTV denotes the presence of cameras within the railway means. All these factors (landscaping design, lightening, permeable barriers and blind corners), depends on the specific asset selected and the data available on RISTAD.

The plus or minus sign in Eq. (1) indicates how each variables can affect the strategy: reduction in the number of blind corners or an increase in the level of illumination can contribute to enhance the natural surveillance. The weights go from zero to one depending on the preponderance of the factor in the implementation of the strategy in the asset: increasing the number of cameras can probably affect the strategy more than interventions in landscaping design.

$$\begin{aligned} \mathit{potential\ attack\ probability}(t) = {} & \mathit{potential\ attack\ probability}(t - dt) \\ & + (\mathit{motivation\ for\ committing\ crime} \\ & + \mathit{asset\ attractiveness} + \mathit{asset\ vulnerability}) * dt \end{aligned} \tag{2}$$

Equation (2) illustrates the computation of the *potential attack probability* stock. As mentioned before, it depends on motivation for committing crime, asset attractiveness and vulnerability and on the potential attack probability at the previous step itself. The initial amount used in the model has been inferred from RISTAD database, based on the initial value settled for motivation for committing crime (that depends on public exposure, damage, victims, personal factors and protection systems), asset attractiveness (that depends on SCP-CPTED factors, asset features and protection systems) and asset vulnerability (threat rating, protections systems, asset features and vulnerability rating).

A real evaluation of the actual level of the above-mentioned strategies based on the data inferred from RISTAD, turned out to be rather complicated. In simulations, we firstly assumed a lacking level of these strategies and cost-effective ones, after the implementation of the CPTED measures.

4.1 Simulation Results

Simulations concern with a medium size station. As stated, data input and asset's features have inferred from RISTAD database. The main asset features are illustrated in.

Objective of the simulations pertains to show how different level/lacking of CPTED measures implementation can affect asset attractiveness and the probability that potential attack evolves into a real one. We split the simulations in two stages: in the first simulation set, we assumed that no CPTED-SCP strategies have been implemented within the asset, while a gradual implementation of the security means has been assumed in the second part of the simulations.

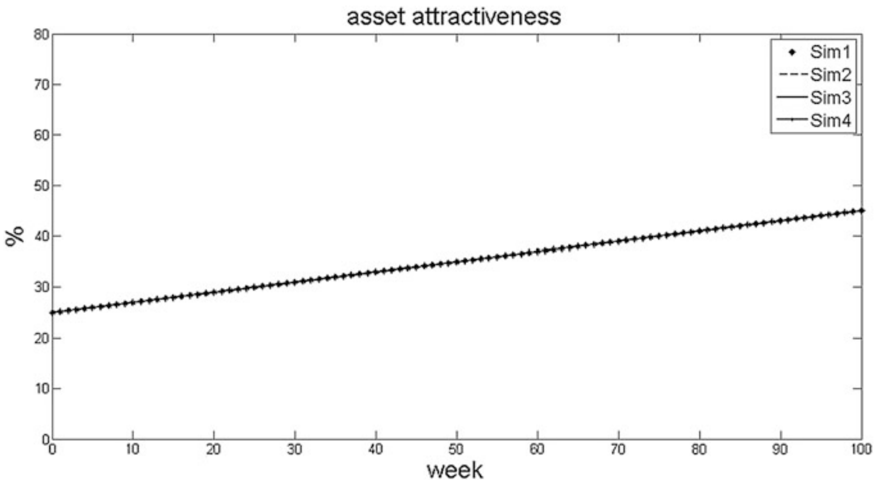


Fig. 6 Asset attractiveness—results for the first simulation set for a medium size station. We assumed that CPTED measures and updating of ordinary protection systems have not been implemented during the simulation time. As result, the asset attractiveness increases in time

Each trend variable is expressed in percent; the number of weeks has been selected as time unit for the simulations.

In the first set of simulations (Sim1, Sim2, Sim3 and Sim4), we analyzed the trend of the main variables assuming that:

- CPTED measures have not been implemented;
- Political, economic, ideological and personal factors actively shape terrorism's motivation.

The lacking of CPTED measures and the defective update of the ordinary protection systems contribute to make the asset more appealing. In the first set of simulations, we assumed that no action have been undertaken to improve the asset security in the simulation time. Consequently, the asset attractiveness increases in time (Fig. 6).

Although asset's appeal increases in time, the probability of potential attack depends also on the attacker's motivation. We supposed that attacker could show different behavior, as illustrated in Fig. 7.

Acting on attacker's triggers (asset public exposure, damage deriving from the attack, the potential number of victims and personal factors), we obtained different trends for the motivation for committing crime, as illustrated in Fig. 7.

In Sim1, attacker's triggers are constant (damage deriving from the attack = 0.4, personal factors = 0.3, asset public exposure = 0.3, victims = 0.6[2]) and the motivation for committing crime is fixed at 20 %.

[2] Data were inferred from RISTAD, taking into account: the size of the station, the number of passengers and trains per day, the number/type of security device which the station is equipped.

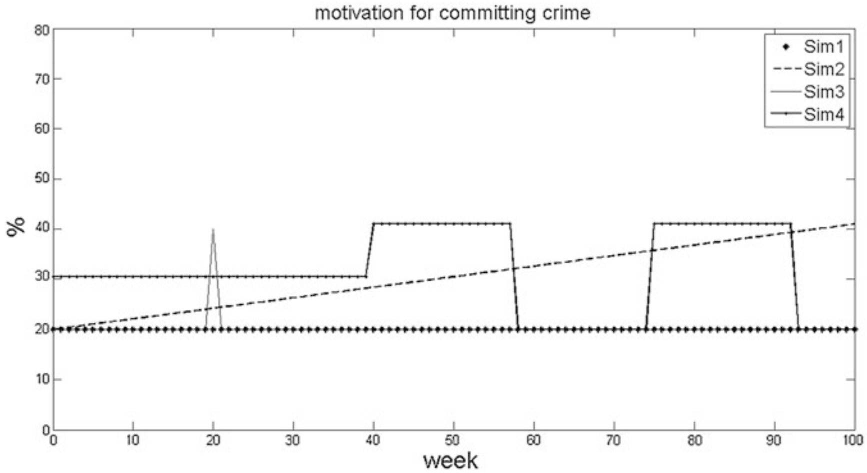


Fig. 7 Motivation for committing crime—results for the first simulation set for a medium size station. In Sim1 we assumed constant attacker's triggers and motivation is settled at 20 %. Changing the trigger factors, we simulated an increasing trend (Sim2) and very quick changes in the attackers' motivation (Sim3 and Sim4)

In the Sim2, Sim3 and Sim4 all the variables have been assumed constant except for the personal factors. In Sim2 it has been assumed an increasing trend (ramp from 20 to 40 %) during the simulation time, while Sim3 and Sim4 show a sudden change in the personal factors and, consequently, a rapid variation in the motivation for committing crime. This variation have been represented respectively by a pulse at time 20 for Sim3 and by a square wave starting from week 40 for Sim4.

The most interesting results come out by the comparison of Figs. 8 and 9. Asset vulnerability and potential attack probability show almost the same behavior in Sim1 and Sim2. Both variables increase in time, whether the motivation is constant or increases in time. Different results are shown in Sim3 and Sim4.

In Sim3, the sudden change in the motivation for committing crime (week 20) causes quick alterations both in asset vulnerability and in potential attack probability, with some differences. The asset vulnerability shows a saturation phenomenon: when the motivation for committing crime increases, the asset vulnerability increases accordingly setting its value at fixed level, even though the motivation for committing crime starts decreasing (week 21). It can be explained considering that an increasing risk of attacks suddenly cues an increasing attention level; the alert usually lasts longer, until each threat vanishes.

The potential attack probability (Fig. 9) changes accordingly to the asset vulnerability, asset attractiveness and the motivation for committing crime. After the fast change at week 20, it does not reach the starting value and is settled at about 66 % showing an increasing trend. Even though the motivation for committing crime at week 21 decreases, the asset vulnerability is constant at 40 % while the asset attractiveness increases, shaping the potential attack probability accordingly.

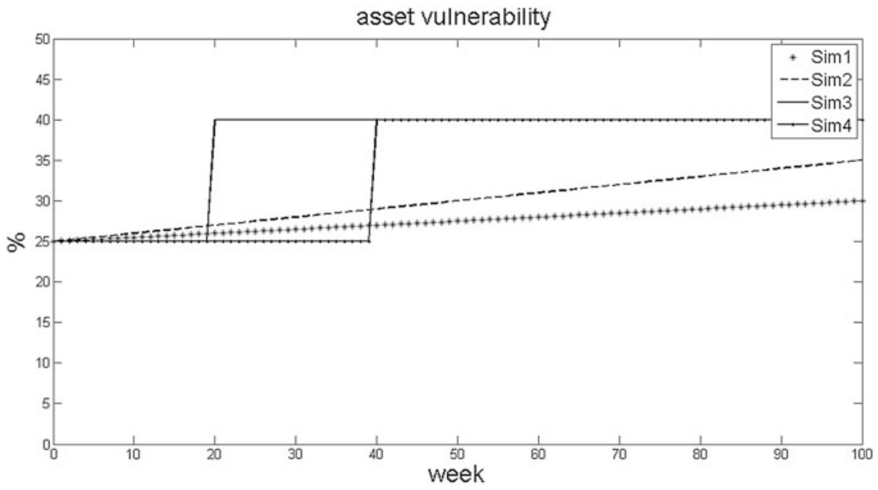


Fig. 8 Asset vulnerability—results for the first simulation set for a medium size station. It changes accordingly to the asset attractiveness and the motivation to committing crime, showing a saturation behavior

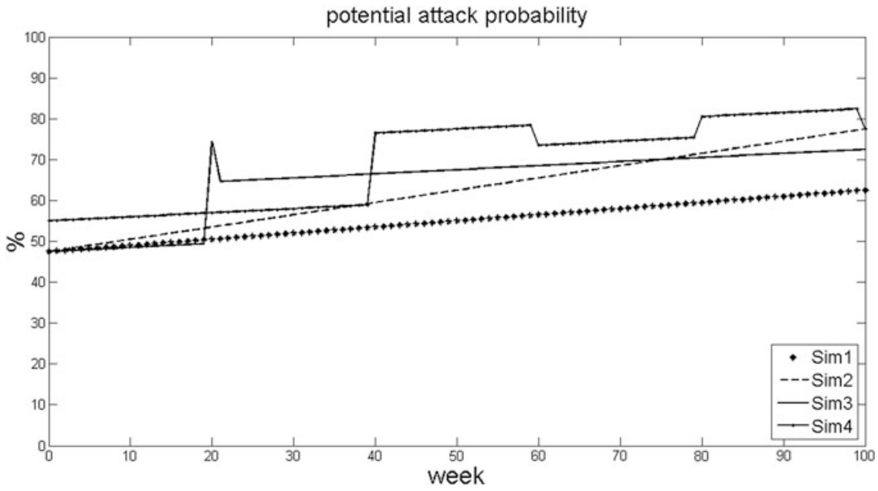


Fig. 9 Potential attack probability—results for the first simulation set for a medium size station. It changes accordingly to the asset vulnerability, asset attractiveness and the motivation for committing crime

The almost same results have been achieved in Sim4: the rapid change in the motivation trend is instantly perceived both by the asset vulnerability and by the potential attack probability. While the asset vulnerability presents a saturation behavior, the potential attack probability is affected by the course of asset vulnerability, asset attractiveness and motivation for committing crime.

Different results have been achieved in the second part of the simulations (Sim5, Sim6, Sim7, Sim8 and Sim9), illustrated in Figs. 10, 11, 12 and 13. Objective of the simulations is to show how the implementation of CPTED measures can affect asset security, also keeping unchanged the motivation for committing crime.

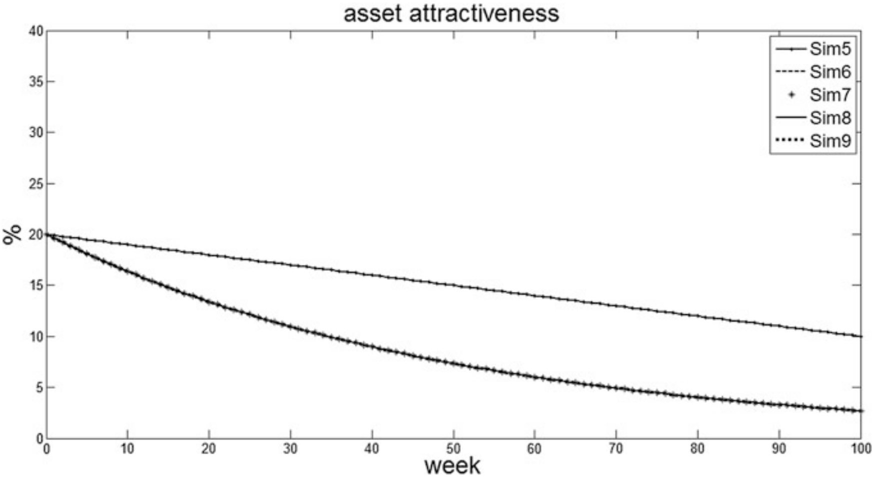


Fig. 10 Asset attractiveness—results for the second simulation set for a medium size station. We assumed that for the same asset, CPTED measures have been implemented during the simulation time. In Sim5 only conventional CPTED strategies were effected (natural surveillance, natural access control, territorial reinforcement). Form Sim6 to Sim9, we assumed that all the strategies have been implemented (including maintenance and activity support). As result, the asset attractiveness decreases in time with different trends, depending on the measures effected

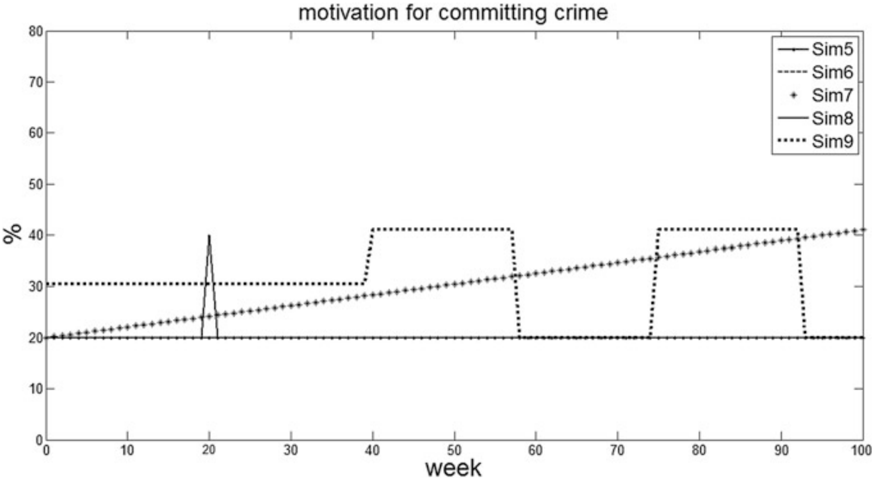


Fig. 11 Motivation for committing crime—results for the second simulation set for a medium size station. Motivation has been assumed as the same as for the first simulation set

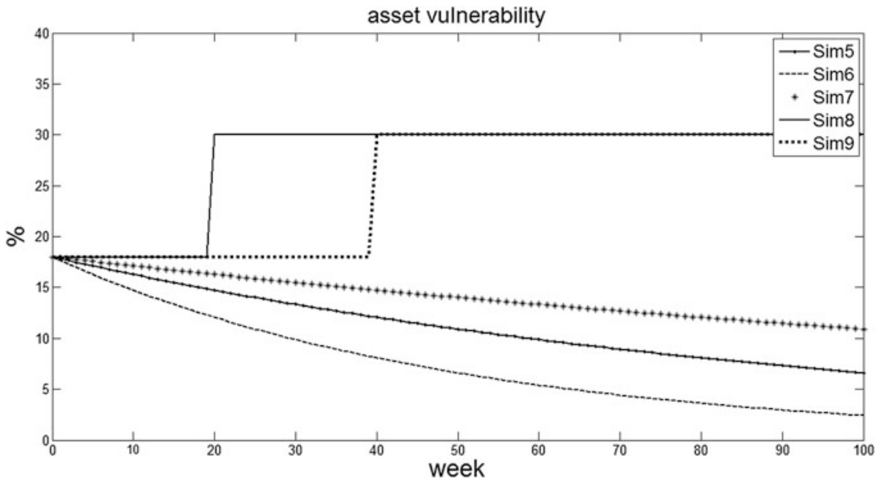


Fig. 12 Asset vulnerability—results for the second simulation set for a medium size station. As in the previous case, it changes accordingly to the asset attractiveness and the motivation to committing crime

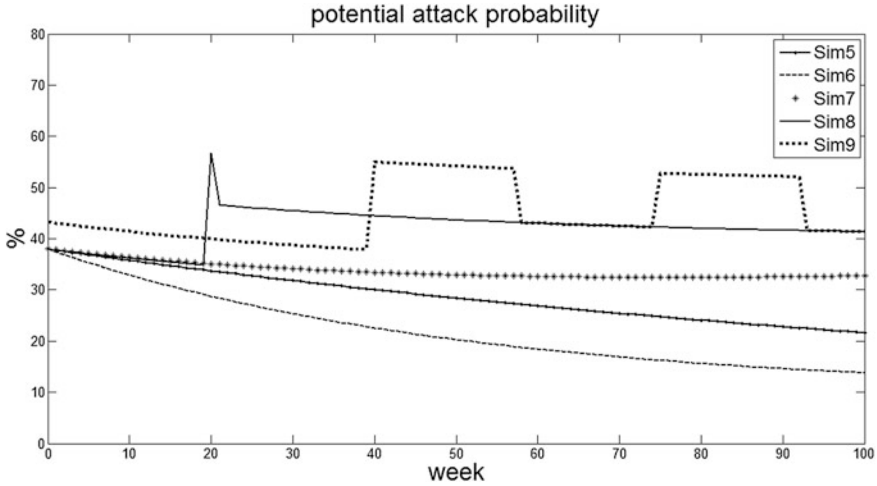


Fig. 13 Potential attack probability—results for the second simulation set for a medium size station

In the second simulation set, we assumed that some or all CPTED strategies have been implemented within the asset. It causes a decrease of the asset attractiveness in time (Fig. 9), with different trends depending on the number of effected measures.

In the first simulation (Sim5), we assumed that the asset has been equipped only with the classic CPTED strategies (natural surveillance, natural access control, territorial reinforcement). In this case, the asset attractiveness decreases in time with a first order trend, passing from 20 to 10 %.

The implementation of maintenance actions and the introduction of activities support (such as kiosks, ticket offices, shops, etc.) produce faster decrease of the asset attractiveness, which sets its value at about 3 % at the end of the simulation time.

For motivation for committing crime (Fig. 11) the same behavior has been assumed as for the previous simulation set. Nevertheless, the asset attractiveness decrease causes a reduction in the motivation with respect to the previous cases, as illustrated in Fig. 10.

The asset vulnerability (Fig. 12) shows a decreasing trend in Sim5, Sim6 and Sim7. A comparison between Figs. 6 and 10 clearly depict how the asset attractiveness decrease affects also the asset vulnerability. Figure 10 shows that the decrease is faster depending on the number of implemented CPTED strategies, accordingly to the asset attractiveness course. The behavior changes in Sim8 and Sim9. As in the previous simulation set, the sudden changes in the motivation for committing crime cause the saturation of the asset vulnerability that settles its value at 30 % in both simulations (week 20 for Sim8, week 40 for Sim9).

A comparison between Figs. 9 and 13 shows how the implementation of CPTED strategies could affect asset security. In the last simulation set, the potential attack probability presents a decreasing trend, nevertheless the quick increases of the motivation for committing crime. It means that the implementation of the CPTED measures reduces in time the risk of potential attack and the more is the number of strategies effected, the more is the potential reduction, nevertheless the motivation for committing crime increases in time. The comparison between Sim5 and Sim6 illustrates this result: the potential attack motivation in Sim6 decreases faster than in Sim5, although the motivation for committing crime increases in time. In Sim7, although the motivation for committing crime increases, the potential attack probability keeps on a decreasing trend. The same happens also in Sim8 and Sim9: the potential attack probability shows almost the same trend shaping of the motivation for committing crime but maintaining the decreasing tendency.

5 Conclusions

As dramatically stressed by Madrid and London attacks, CI in general, and RIS more specifically, represent the most feasible indicator of the economic capacity of countries, but at the same time are susceptible to potential threats with devastating consequences for human life and economy. Vulnerability analysis and quantitative simulations play a crucial role in identifying weak-points and outlying new and more appealing protection strategies. In this chapter, we presented a vulnerability assessment tool based on SD approach and CPTED-SCP strategies. Objectives of the simulation were to show how the adoption/lacking of CPTED actions in the railway asset environment could affect the means security.

In our SD model, the means selected represent railway stations. Starting from a vulnerability assessment of the assets, we illustrated how the implementation/lacking of CPTED measures have repercussion on the assets' attractiveness, becoming actual the probability of real attacks. Using CPTED-SCP means, we were able to define which are the main physical, social and environmental aspects that provide opportunity for criminality in railway asset scenarios.

Simulation concerned a medium-size station. Acting on specific triggers, we simulated different behaviors for the attackers. Changing the level/lacking of CPTED measures implementation, we modified also the asset vulnerability courses. Results show that the implementation of CPTED strategies could affect asset's security. The implementation of the CPTED-SCP measures causes a decreasing trend in the risk of potential attack, nevertheless the motivation of the attackers shows an increasing trend. It means that the implementation of the CPTED measures reduces in time the risk of potential attack and the more is the number of strategies effected, the more is the potential reduction, nevertheless the motivation for committing crime increases in time.

References

1. Marrone S, Nardone R, Tedesco A, D'Amore P, Vittorini V, Setola R, De Cillis F, Mazzocca N (2013) Vulnerability analysis and modeling for critical infrastructure protection. Critical infrastructure protection VI. Springer, Heidelberg
2. De Cillis F, De Maggio MC, Pragliola C, Setola R (2013) Analysis of criminal and related episodes in railway infrastructure scenarios. J Homel Security Emerg Manage 10(2):1547–7355
3. Wortley R, Mazerolle L (2008) Environmental criminology and crime analysis. Willan Publishing, Portland
4. Atlas R (2008) Designing for critical infrastructure protection and crime prevention. Auerbach Publications, Quincy
5. Crowe DT, Zahm DL (1994) Crime prevention through environmental design. Land Development magazine by National Association of Home Builders, Florida
6. Hedayati Marzabali M, Abdullah A, Nordin RA, Maghsoodi Tilaki MJ (2012) Validating crime prevention through environmental design construct through checklist using structural equation modelling. Int J Law Crime Justice 40:82–99
7. Crowe TD (2000) Crime prevention through environmental design, 2nd edn. University of Louisville, National Crime Prevention Institute (NCPI), Louisville
8. Ceccato V, Uittenbogaard A, Bamzar R (2011) Security in Stockholm's underground stations: the importance of environmental attributes and context. Secur J 26(1):33–59
9. Cozens P, Neale R, Hillier D, Whitaker J (2007) Tackling crime and fear of crime while waiting at britain's railway stations. J Publ Transp 7(3):23–41
10. Cozens P, Neale R, Whitaker J, Hillier D (2003) Managing crime and the fear of crime at railway stations. a case study in South Wales (UK). Int J Transp Manage 1(3):121–132
11. Diec J, Coxon S, De Bono A (2011) Deterring anti-social behaviour and crime in the public train environment by design. www.designoutcrime.org/ocs2/index.php/iDOC/2009/paper/view/14. Accessed 2013
12. Kennedy DM (2008) Personal security in public transport travel in New Zealand: problems, issues and solutions. Land Transport New Zealand, Wellington

13. La Vigne NG (1973) Safe transport: security by design on the Washington metro. U.S. National Institute of Justice, Washington DC
14. American Public Transportation Association Transit Infrastructure—Security Work Group (2010) Crime prevention through environmental design (cpted) for transit facilities. American Public Transportation Association, Washington DC
15. Benigno G, Alcantara R, Matsuura M, Molina Monzon C, Samothrakis I (2005) The use of system dynamics analysis and modeling techniques to explore policy levers in the fight against middle eastern terrorist groups. Naval Postgraduate School, Monterey
16. Leweling T, Sieber O (2007) Using systems dynamics to explore effects of counterterrorism policy. In: Proceedings of the 40th Hawaii international conference on system sciences
17. Madnick S, Siegel M (2008) A system dynamics (SD) approach to modeling and understanding terrorist networks. Massachusetts Institute of Technology, Cambridge
18. U.S. Department of Homeland Security (2011) Reference manual to mitigate potential terrorist attacks. Accessed October 2011

Cumana and Circumflegrea Railway Lines: A Circle Network in the Western Metropolitan Area of Naples

Arturo Borrelli, Francesco Murolo, Antonio Sforza and Claudio Sterle

Abstract Cumana and Circumflegrea railway lines constitutes a circle network in the western metropolitan area of Naples, named Area Flegrea (the ancient name of the places). These two lines are strongly inserted in the urban transportation system of the city of Naples and moreover serve other four districts, rich of places which generate and attract relevant people flows. The structure of the railway network is described and data about travel demand are provided. Characteristic of the used rolling stock and its development perspectives are presented. Current security problems are described and finally an optimization approach for the improvement of the network security is proposed.

Keywords Cumana · Circumflegrea · Urban transportation · Railway maintenance · Railway security · Network infrastructure protection

1 Introduction

The METRIP (MEthodological Tool for Railway Infrastructure Protection) Project foresees the application of the proposed methodologies to a test case related to urban transportation system [1]. To this aim, the SEPSA network composed of two

A. Borrelli
EAV, Ente Autonomo Volturno, Via Cisterna Dell'Olio, 44,
80134 Naples, Italy

F. Murolo
SEPSA Consultant, Naples, Italy

A. Sforza (✉) · C. Sterle
Department of Electrical Engineering and Information Technology,
University "Federico II" of Naples, Claudio, 80125 Naples, Italy
e-mail: sforza@unina.it

C. Sterle
e-mail: claudio.sterle@unina.it

R. Setola et al. (eds.), *Railway Infrastructure Security*, Topics in Safety, Risk, Reliability and Quality 27, DOI 10.1007/978-3-319-04426-2_5

lines, Cumana and Circumflegrea, has been chosen. These two lines serve four districts of the western metropolitan area of Naples (Flegrean Area) and they are strongly inserted in the urban transportation system of the city.

The SEPSA system is an old railway system, indeed it dates back to 1883 and it serves a significant and consolidated transportation demand in the area of Naples. The system is formed by segments with very different characteristics in terms of capacity and technological level and hence it offers great opportunities of improvement in terms of network integration and innovation. These considerations have pushed the interest of the project towards this urban railway system.

In the following we provide a description of the system in terms of transportation demand, structure and rolling stock (Sect. 2). This allows to better understand the system under investigation. Then we focus on some reliability, safety and security issues which are fundamental for SEPSA railway infrastructure. In particular we present the actual and future emergency and security countermeasures that are going to be put in act (Sect. 3). Finally we provide a graph representation of the SEPSA metro system, aimed at highlighting its particular structure and its most critical assets. On this base, the chapter concludes with the applications of two network and combinatorial optimization methods on the SEPSA network (Sect. 4).

2 SEPSA Urban Railway System: Cumana and Circumflegrea

SEPSA manages the Cumana and Circumflegrea lines. The company undergone several transformations from its foundation. In 1883 the “Società per le Ferrovie Napoletane” arose in Rome. This company had the aim of building and manage the railway system from Naples to Pozzuoli in the area of Cuma, i.e. the Cumana, which is on service from 1889 and was officially initiated on 1892.

In 1938, in order to improve and strengthen the system, SEPSA (Società per l’Esercizio di Pubblici Servizi Anonima) is constituted and replaced previous company in the management of the line. It restructured the Cumana and built the Circumflegrea after the II world war. With the aim of improving the standard of the offered service, SEPSA adapted its organizational structure to the international regulations established in ISO 9001:2008— ISO 14000:2004—SA 8000—2008.

SEPSA was organized as a business limited company, of which the Ente Autonomo Voltuno (EAV) was the owner. EAV was initiated in 1904 as a public company for the economic development of Naples. Its main target was the production of electrical energy from hydraulic power in order to deliver it to the Naples urban area. Moreover EAV was involved in the Public Transportation sector with reference to the management of the railway system of Naples.

Nowadays the company has the role of regional holding of railway public transportation system and it is owner of SEPSA, Cicumvesuviana, Metro Campania Nord-Est, EAVBUS. In the following, even if in practice SEPSA exists just as part of EAV, since our interest is just on Cumana and Circumflegrea lines, we will continue to refer to them as the SEPSA network.

SEPSA network, as said above, is composed of two lines, Cumana and Circumflegrea. To better understand the role of the two SEPSA lines, in Fig. 1 a sketch of the entire metro system of Naples is reported, where the urban segments of Cumana and Circumflegrea are referred to as line 5 and 7 respectively [2].

Cumana connects Montesanto, in Naples city center, with Torregaveta, in Bacoli district, passing through 14 intermediate railway stations. The line follows a costal path of about 20 km.

Circumflegrea connects Montesanto with Torregaveta passing through 14 intermediate railway stations located in the western districts of the Area Flegrea, i.e. Soccavo, Pianura, Quarto, Licola and Cuma. It follows an internal path of about 27 km.

Hence the two lines meet at Montesanto and at Torregaveta, so constituting a closed ring which connects Naples city center with Area Flegrea using two different paths, which are for the 40 % on the municipal area of Naples and for the 60 % in the suburban area.

The entire system constituted by the two lines, Cumana and Circumflegrea extends for 46,852 km, of which 14,258 km are double track lines and 14,419 km are

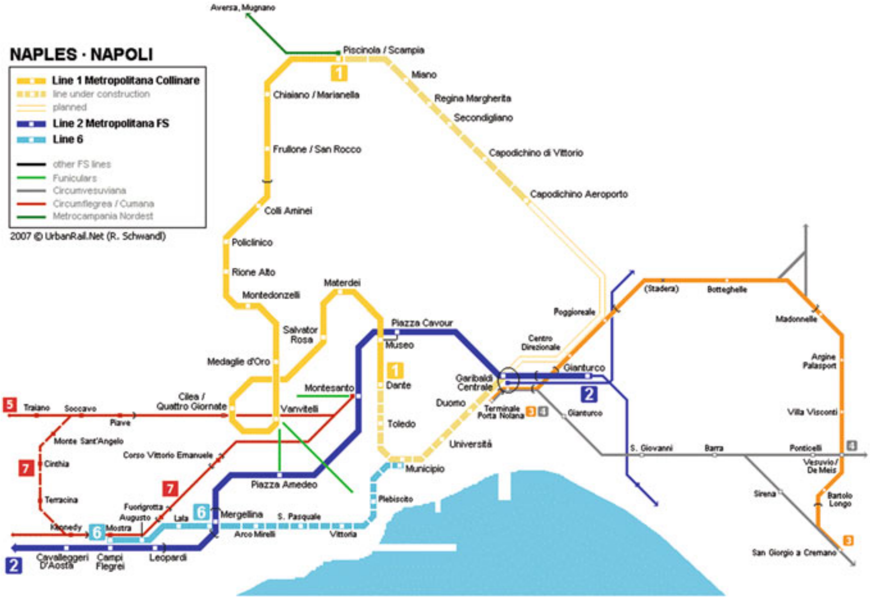


Fig. 1 Metro System of City of Naples

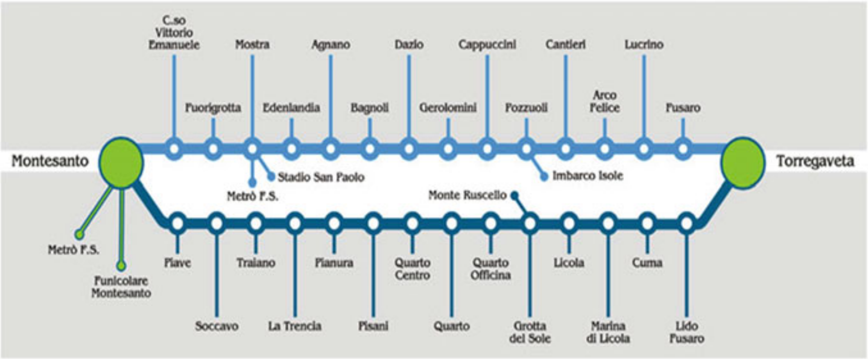


Fig. 2 SEPSA network: Cumana and Circumflegrea lines

galleries (single and double tracks). Given the increasing demand of transportation, during the years the need of doubling almost all the lines has been recognized, so important infrastructural interventions were and are actually carried out.

The circular structure of the SEPSA metro system, with the detailed list of the 30 railway stations composing it (as said above, 14 railway stations for each line plus the two terminal stations, Montesanto and Torregaveta), is reported in Fig. 2.

In the following we give some details of the railway stations of the two lines to better understand the relevance of the system under investigation, even if it is just a part of the metro system of Naples. In particular we will focus on the aspects related to the interconnections with other public transportation services and lines.

Concerning the Cumana line, Montesanto station is a terminal station and it represents an interconnection point with the funicular and with metro lines 1 and 2 managed by Trenitalia and Metronapoli respectively. It is composed of 4 platforms, where the first and the second track serve the Circumflegrea line, whereas the third and the forth track serve the Cumana line. The Corso Vittorio Emanuele (situated in the area of Mergellina) and Pozzuoli stations are located near two small ports of gulf of Naples and hence they are fundamental to serve the travel demand, composed of tourists and inhabitants of the near islands, reaching the city by ship. Mostra station plays a relevant role in the SEPSA metro system, since it serves several structures and places of the city for show exhibition and conference, education and research. Moreover it is an connection point with Campi Flegrei railway station (managed by Trenitalia) and a bus station managed by ANM (Neapolitan Agency for Mobility). Torregaveta station is the terminal station. As Montesanto, it presents 4 platfoms, where two are dedicated to the Cumana line and the other two to the Circumflegrea line.

Concerning Circumflegrea line, Soccavo station will be a connection point with the future station of the Line 7. Pianura station is an important interconnection point with the bus station managed by ANM. Finally, Cuma station is fundamental for its connection with touristic points of interests located in the Area Flegrea.

Table 1 Cumana and Circumflegrea daily average trips

Line	2009	2011
Cumana	29.067	29.674
Circumflegrea	28.816	26.225
Total	57.883	55.899

Fig. 3 SEPSA new power trains by Firema

SEPSA metro system serve 5 districts, Napoli, Pozzuoli, Quarto, Bacoli and Monte di Procida. The interested population is about 1.270.472 inhabitants. The total number of trips was 21.127.296 in 2009 and 20.403.136 in 2011.

The daily average trips for these years are reported in Table 1. It is important to underline that on the whole this value significantly increases until about 70.000 in the winter average working day. Hence the real daily demand that has to be satisfied is much higher than the average value [3].

SEPSA metro systems uses 40 power trains, whose average age is about 30 years. On 2008 the order of 12 new trains has been made. They will be put on service in the next years. These new trains will be realized by Firema, and will be equipped with most modern comfort and security features (Fig. 3) [4].

3 Security Challenges

As widely known, assuring the security and the reliability of a railway system is a very hard problem because of the particular characteristics of a railway system [5]. Indeed the "open" nature of rail systems, encompassing multiple access points and hubs serving multiple carriers on which passengers freely move about, makes them highly vulnerable to attack [6, 7]. Moreover the assets and the components of railway system are basically easily recognizable physical structures, varying in age and design, highly interdependent and widely distributed over large areas. This contributes to increase the vulnerability of the system and increases the difficulties in guaranteeing the reliability of the system in case of malfunctioning of one of its asset/component due to both natural or induced causes [8, 9].

In this context SEPSA has among its main strategic targets the security of the users and of the railway system itself. Hence its actions in the years were addressed to tackle the problem of improving the passenger security, the quality and the reliability of the offered services. In this context moreover SEPSA started a restyling process of the main railway stations in order to improve also the security perception of the users.

An important example of this initiative is represented by Montesanto railway station (Fig. 4) [10].

Among the other interventions, in particular, in the last 30 years, SEPSA adopted also several maintenance countermeasures and activities aimed at reducing the service time in case of system malfunctioning. More precisely these activities are aimed not only at solving the malfunctioning of the machines and facilities, but overall at the management of the effectiveness of the entire complex system. Hence we can say that these activities arose with the main target of maintaining the effectiveness of the infrastructure guaranteeing also the maximum quality, security, integrity and reliability standards.

In particular the main maintenance and security services performed by SEPSA can be reduced to five main sectors:

- Infrastructure facilities;
- Equipments and tracks;
- Energy supply;
- Signaling devices;
- Telecommunication devices.

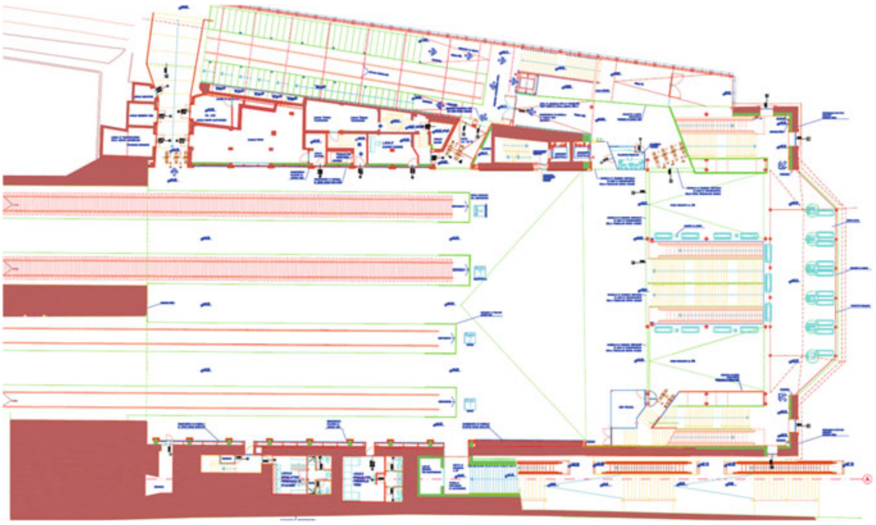


Fig. 4 Montesanto railway station layout after restyling

These services are provided by 3 different kind of centers placed within the SEPSA network at different railway stations:

1. *Train maintenance center*: maintenance and reparation activities on trains and locomotives are performed at the depot located at Quarto and Fuorigrotta;
2. *Electric facility maintenance center*: located at Quarto, Soccavo, Pozzuoli and Bagnoli
3. *Other facility maintenance center*: located at Quarto, Soccavo, Corso Vittorio Emanuele and Arcofelice.

Each center is composed of teams which intervene in case of system malfunctioning or disruption for technical reasons or because of sabotages, in order to restore the normal functionality conditions.

SEPSA put in act also several measures to tackle maintenance, security and reliability problems and developed several procedures to be used in case of emergency:

- Procedure PRQ-05MLI "Maintenance and Construction of lines and facilities": it reports the design, registration and realization criteria to be put in act in the preventive and corrective maintenance activities.
- Procedure ORQ-17eme "Management of the service emergences": it reports the rules and the responsibilities of each company function in case of occurrence of a dangerous situation for the people or for the system.
- Emergency Plan: it reports the coordinated actions to be used by the employees of the company in case of event which can be a real or a potential danger for the health and safety of people and of the infrastructures.

These procedures are yearly updated on the basis of the innovation/improvement of the infrastructure, available technologies and regulations requirements.

The main security problems observed in these years can be reduced to act of vandalism, small crimes and infractions. SEPSA regularly realizes a monitoring activity about the act of vandalism and the infractions which occur during an year. The inquiry on act of vandalism in the last 5 years, from 2007 to 2012, show a constant decrease of theft and robbery notifications on both the two lines, and the same result has been observed for what concerns aggression and persecution, for which no notifications have been registered in the last year. In this context SEPSA regularly performs also inquiry on the controlling activity performed during the year, evaluating the number of employees commitments, total infractions (paid on the spot and within 60 days), issued injunctions and terminated injunctions. Unfortunately the registered numbers are worse than the European average values.

These results derived by a deeper control activity of the law enforcement agency at the railway stations, but also by the increased number of installed surveillance cameras (from 116 to 202). The solutions adopted by SEPSA at its main railway station, i.e. Montesanto, in terms of number, location and performances of the security system could be used to perform a double evaluation of the results achieved in METRIP Project. Indeed on one side it could be used to evaluate the capability of the models and methods, proposed for the optimal placement of the security devices, in tackling a real test case and on the other side it could be used to evaluate the effectiveness of the already adopted solution.

4 Critical Infrastructures of Cumana and Circumflegrea Lines

The protection of a railway infrastructure system has to be performed on two levels: asset and network level. In the first case, the security of the single asset composing the RIS has to be guaranteed and increased adopting advanced technologies, new security devices and ad hoc methodologies. An example of this approach is represented by the methodologies implemented in METRIP project [1] (explained in the following chapters of the book).

Concerning instead the second case, in order to protect a railway infrastructure system it is important to consider its network structure, the connections among the assets and their positions. Then the system has to be studied by ad hoc network optimization methodologies aimed at improving the usage of the network and at identifying its most vital points. Network optimization theory has been widely used for different network problems and for critical infrastructure identification in different contexts, form transportation and communication networks to supply chain ones [11–14].

In the following sections the SEPSA network will be analyzed in this perspective. Indeed we propose a graph representation of the SEPSA network system and then we use it in solving two optimization problems. The first concerns the determination of the optimal placement of the maintenance and security teams at the SEPSA railway stations in order to minimize the service time. Hence the aim is to provide an evaluation of the security service level that can be guaranteed on the system. The second problem, starting from the results of the first, concerns the determination of the most vital maintenance facilities for the normal functioning of the system. Hence it provides an assessment of the facilities whose interdiction would affect most the reliability of the system.

The two problems will be solved using two integer linear programming models derived from network optimization literature. The models are solved by the optimization software FICO$^{\text{TM}}$ Xpress-MP 7.3 and run on an Intel$^{®}$ Core$^{\text{TM}}$ i7, 870, 2.93 GHz, 4 GB RAM, Windows Vista$^{\text{TM}}$64 bit.

4.1 SEPSA Network System

The critical infrastructures are generally modeled by a network with nodes which represent goods, facilities or activities and links which represent connections and relations among the nodes. The same can be done for the railway infrastructure, whose representation well fits with a network representation.

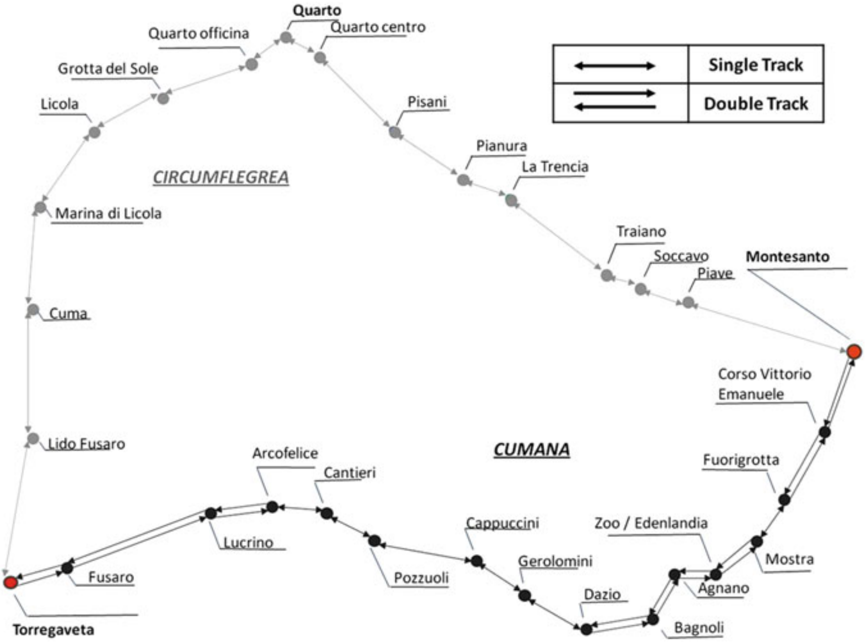


Fig. 5 Graph of the Cumana and Circumflegrea lines

The two SEPSA lines, Cumana and Circumflegrea, can be modeled by an oriented graph G (N, A) with 30 nodes and 40 links (Fig. 5).

Each node represents a railway station and each arc represents the physical connections between two consecutive stations, i.e. a track segment. In particular the double orientation arcs represent segment of the line where a single track to be used in both ways is present, whereas the usage of two single orientation arcs represent segment where two different tracks are used, one for each way.

The Cumana line is composed by 16 nodes and 25 arcs and has a single track segment between Dazio and Arco Felice and two double track segments, between Montesanto and Dazio and Arco-Felice and Torregaveta. The Circumflegrea lineis composed by 16 nodes and 15 arcs and it is all single track.

4.2 Critical Assets in the SEPSA Railway System

As widely known the most important and critical points of railway infrastructure systems are: Railway Stations, Electric substations, Bridges, Flyovers, Viaducts, Galleries, Depots, Level Crossings. All these assets represent critical points of a railway system since their malfunctioning or sabotage could significantly affect or interdict the functioning of the system. Along the two lines, Cumana and

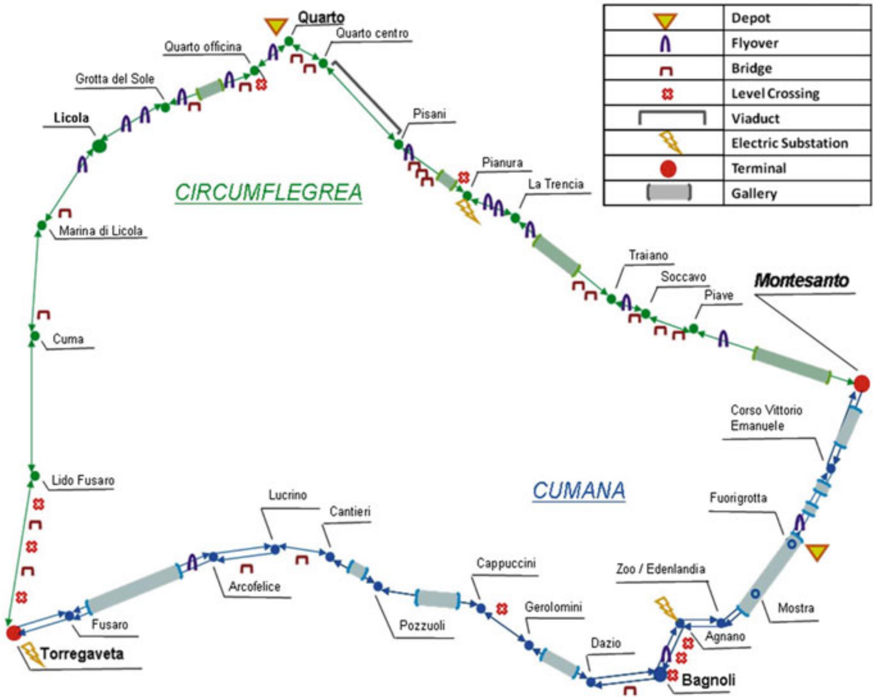


Fig. 6 Critical assets on Cumana and Circumflegrea lines

Circumflegrea, we individuates many critical points and they have been reported with a specific notation in Fig. 6.

In particular, concerning Cumana, we have:

- 1 depot;
- 4 level crossings;
- 2 electric substations;
- 3 flyovers;
- 3 bridges;
- 8 galleries.

Concerning instead Circumflegrea, we have:

- 1 depot;
- 5 level crossings;
- 1 electric substation;
- 1 viaduct;
- 10 flyovers;
- 14 bridges;
- 4 galleries.

4.3 Maintenance Center Location Problem

As said above, at present day, SEPSA has 7 different security and maintenance centers at Corso Vittorio Emanuele, Fuorigrotta, Bagnoli, Pozzuoli and Arcofelice railway stations of Cumana and at Quarto and Soccavo stations of Circumflegrea.

We evaluated for each kind of center and consequently for each team, the possibility of improving the whole service by redesigning it, i.e. re-locating the available teams on the network and introducing an additional one, on the base of a chosen performance criterion. In the following, for the sake of the brevity, with reference to the previous center classification (Sect. 3), we focus on the re-location of the security and maintenance centers in charge of the reactivation of all the other facilities located along the line. This location problem can be defined with two different approaches:

- On the entire SEPSA network
- On the single line of the SEPSA network.

In the first case we assume that all the team can intervene indifferently on the two lines, whereas, in the second case, we assume that each maintenance team is dedicated to the line which it belongs to. The optimal location of the centers along the entire SEPSA network or on the two separated lines is the one which minimizes the service time (also referred to as *first-response time*), i.e. the time required by the team to reach the point where the malfunctioning of the system occurred (*interdicted point*). The service time can be evaluated in two ways: (1) a team reaches the interdicted point by the SEPSA railway infrastructure; (2) a team reaches the interdicted point by the road network. The service times (in minutes) using the SEPSA network are reported in Fig. 7.

The teams under investigation are actually located at Quarto, Soccavo, Corso Vittorio Emanuele and Arcofelice. As said above, we suppose to have an additional team and we want to know how to reposition all of them on the network on the base of the pre-defined performance criterion, i.e. the service time computed using the SEPSA railway network. The complete re-design of this kind of service is possible since it does not require a significant effort in replacing the facility infrastructure, but mainly a decision of re-locating the team members. If we assume that each station has to be served by just one team, then this location problem corresponds to the known *p-median problem* and can be solved by the related integer linear programming model. Indeed the *p-median problem* consists in determining the optimal location of *p* facilities to serve a set of demand points, with the aim of minimizing the service cost or the shortest demand weighted distance between customers and facilities [15, 16].

Implementing the model and solving it by Xpress-MP solver we obtained the solution reported in Fig. 8, where the teams are located at Zoo/Edenlandia, Cantieri, Traiano, Quarto and Lido Fusaro and the total service cost is 109 min. The assignment of the 30 railway stations to the teams at chosen locations is highlighted using thick lines. A more focused application of this model on the network could be

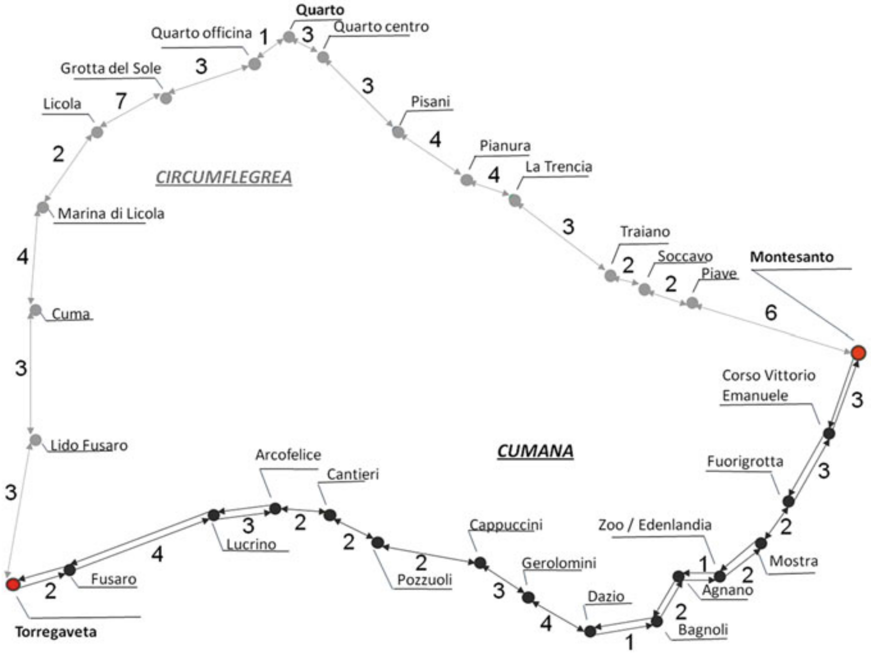


Fig. 7 Service time of Cumana and Cirumflegrea lines

done weighting differently the arc of the networks, keeping into account the kind and the number of critical assets distributed along the links of the network. This could also allow to better balance the work between the five teams.

4.4 Service Time in Case of System Failures

Once a set of facilities is located on a network, situations where one or more of them are unavailable can occur because of endogenous and external reasons.

Hence, starting from the solution of the *p-median* problem with p = 5, then we are interested in studying the effect on the reliability of the system when one or more teams are unavailable and cannot intervene on the network.

To solve this problem we can use the failure cost analysis and treat it as an *r-interdiction median problem*, to be solved by the related integer linear programming model. Indeed given an existing system of facilities and the assignment of the demand points to them, the *r-interdiction median problem* consists in identifying the set of facilities that, if lost, would affect the system performance the most, i.e. the ones which provide the highest *failure cost* [17, 18].

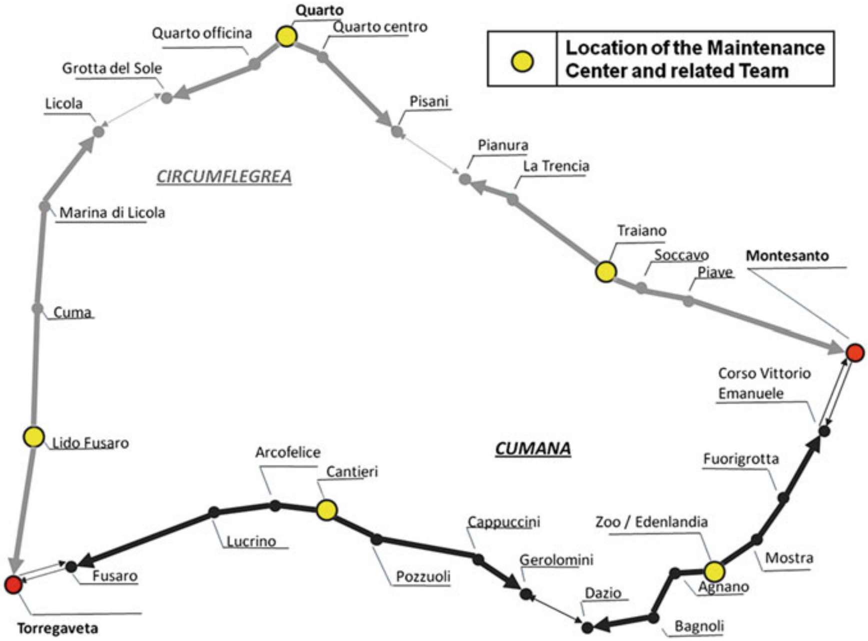


Fig. 8 Optimal location of the maintenance teams obtained by *p-median* model (*p* = 5)

In order to better understand the meaning of *failure cost*, let us suppose that among the 5 facilities located at Zoo/Edenlandia, Cantieri, Traiano, Quarto and Lido Fusaro, the one at Cantieri is unavailable. Hence all the railway stations that previously were served by its team, have to reassigned to the remaining facilities, taking into account the new service cost. This new cost, after the facility loss, can be computed by a failure analysis based on the service time matrix reported in Table 2. Indeed this matrix shows the service time of the 5 located teams with respect to all the railway stations of the SEPSA network, i.e. the 30 railway stations. When no loss occurs, each railway station is served by the nearest team (among the five available teams), i.e. by the one with the minimum service time value (minimum of a column). When instead a loss occurs, this corresponds to the cancellation of a row of the matrix and hence in the assignment of the railway stations previously solved by the lost team to the second nearest one. The increase of the service time due to this re-assignment is the *failure cost* of a facility.

If we apply previous failure analysis to the case of Cantieri loss, the railway stations of Gerolomini, Cappuccini and Pozzuoli will be reassigned to Zoo/Edenlandia, whereas Cantieri, Arco Felice, Lucrino and Fusaro to Lido Fusaro (Fig. 9).

Table 2 Service time matrix of the 5 located maintenance teams

	Montesanto	C.so Vitt. Emanuele	Fuorigrotta	Mostra	Zoo/Edenlandia	Agnano	Bagnoli	Dazio	Gerolomini	Cappuccini	Pozzuoli	Cantieri	Acro Felice	Lucrino	Fusaro
Zoo/Edenlandia	10	7	4	2	0	1	3	4	**8**	**11**	**13**	15	17	20	24
Cantieri	25	22	19	17	15	14	12	11	7	4	2	0	2	5	9
RioneTraiano	10	13	16	18	20	21	23	24	28	31	33	35	37	40	42
Quarto	27	30	33	35	37	38	40	41	41	38	36	34	32	29	25
Lido Fusaro	39	36	33	31	29	28	26	25	21	18	16	**14**	**12**	**9**	**5**
	Torregaveta	Piave	Soccavo	Rione Traiano	La TRencia	Pianura	Pisani	Quarto Centro	Quarto	Quarto Officina	Grotta del Soles	Licola	Marina di Licola	Cuma	Fusaro
Zoo/Edenlandia	26	16	18	20	23	27	31	34	37	38	41	38	36	32	29
Cantieri	11	31	33	35	38	42	40	37	34	33	30	23	21	17	14
RioneTraiano	40	4	2	0	3	7	11	14	17	18	21	28	30	34	37
Quarto	23	21	19	17	14	10	6	3	0	1	4	11	13	17	20
Lido Fusaro	3	41	39	37	34	30	26	23	20	19	16	9	7	3	0

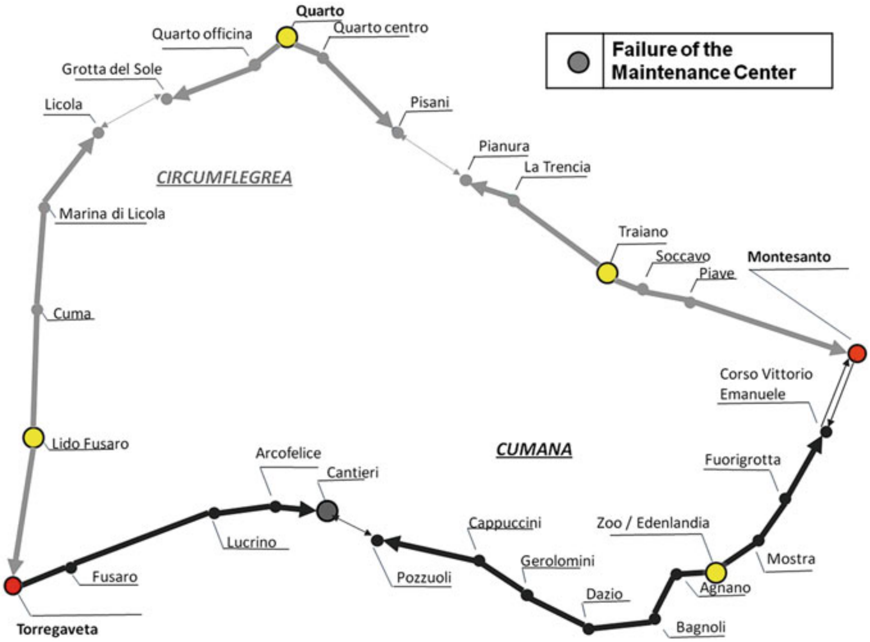


Fig. 9 Cumana and Circumflegrea railway station assignment in case of Cantieri loss

Table 3 Analysis of failure costs

Facility	Failure cost (min)
Zoo/Edenlandia	185
Cantieri	155
Rione Traiano	167
Quarto	170
Lido Fusaro	156

This provides an increase of the service time from 109 + 46 = 155 min, which represents the total failure cost for Cantieri. The same discussion can be repeated for all the other facilities already located on the network, so obtaining the failure costs reported in Table 3. Hence we can note that the most critical railway station is: Zoo Edenlandia.

The same result could be obtained by the implementation of the *r*-interdiction model with $r = 1$ by Xpress-MP solver. In this case the railway stations which were previously served by Zoo/Edenlandia will be now reassigned in this way (Fig. 10):

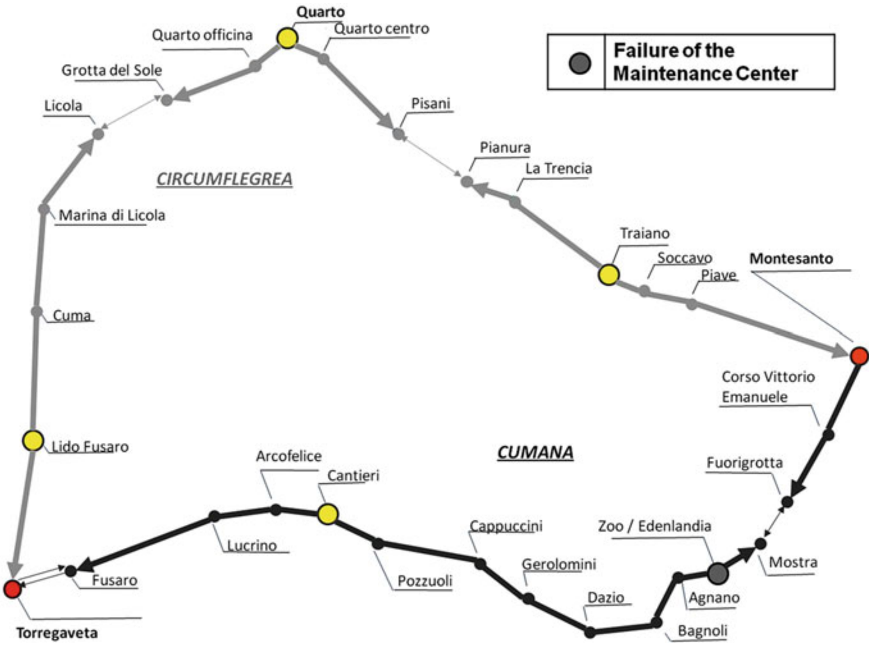


Fig. 10 Cumana and Circumflegrea railway station assignment in case of Zoo/Edenlandia loss

- Corso Vittorio Emanuele and Fuorigrotta will be assigned to Traiano;
- Mostra, Zoo/Edenlandia, Agnano, Bagnoli, and Dazio will be assigned to Cantieri

Implementing the *r-interdiction* median model with $r = 2$, we see that the most critical couple of facilities on the SEPSA network, is Zoo/Edenlandia—Cantieri. All the stations previously served by Zoo/Edenlandia, will then be served by Traiano, whereas all the ones served by Cantieri, will be served by Lido Fusaro, with a total failure cost of 292 min (Fig. 11).

It is important to note that the model returns a solution where the two most critical facilities are located on the same line, i.e. the Cumana. This could seem anomalous, but it is easy to understand that the interdiction of the only two facilities present on the Cumana line provides a great increase of the service time for all its stations, whereas the three facilities located on the Circumflegrea allows to have a much reliable solution in case of disruption or unavailability of a maintenance team.

This two examples allow to highlight which are the most critical maintenance and security facility of the SEPSA metro system, which if lost or interdicted for natural or human caused disasters would affect most the recover capability of the

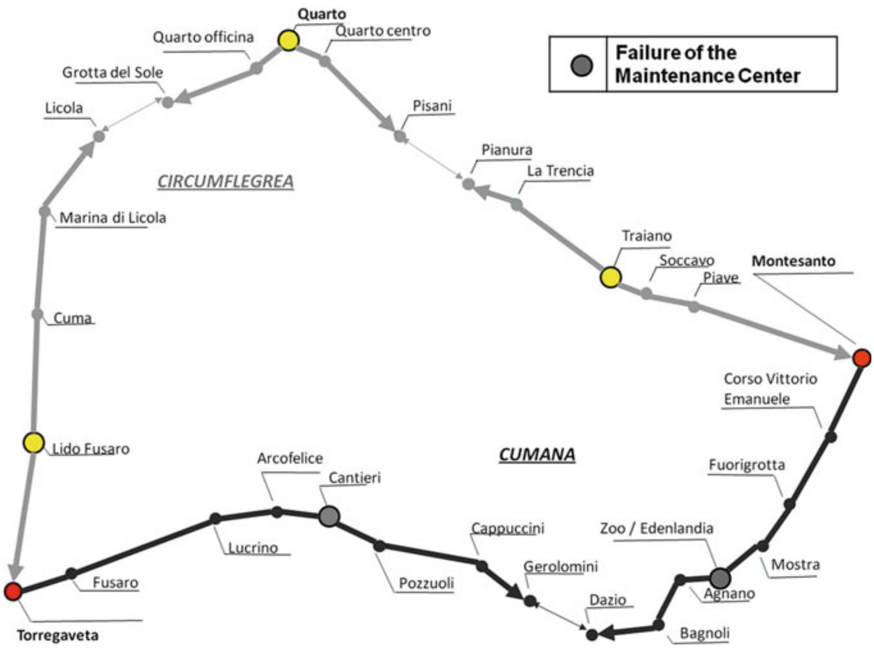


Fig. 11 Cumana and Circumflegrea railway station assignment in case of Cantieri and Zoo/Edenlandia loss

system and hence its reliability. A more deeper analysis, with reference to all the used centers and related teams should keep into account also the current placement of the working station on the SEPSA railway network.

5 Conclusions

In this chapter, we focused on the SEPSA metro railway system operating in the urban area of Naples. We first provided a description of the main characteristics of the SEPSA metro system and then we focused our attention on security problems that have to be faced in managing this system. Moreover, a graph representation of the SEPSA network and of the related critical assets has been realized. Finally, we showed two simple applications of optimization models to solve two test problems on this network.

Acknowledgments This work is partially supported by the European Commission, Directorate-General Home Affairs, within the Specific Programme on Prevention, Preparedness and Consequence Management of Terrorism and other Security-related risks, under Grant HOME/2010/CIPS/AG/035 METRIP—MEthodological Tools for Railway Infrastructure Protection.

References

1. Sforza A, Sterle C, D'Amore P, Tedesco A, De Cillis F, Setola R (2013) Optimization models in a smart tool for the railway infrastructure protection. Lect notes comput sci 8328:191–196. doi:10.1007/978-3-319-03964-0_17
2. Carriola B, Murolo F (1995) La rete ferroviaria della SEPSA. Le ferrovie Cumana e Circumflegrea. La tecnica Professionale
3. Data from Consorzio Unico Campania 2009–2011
4. D'Avanzo S, Murolo F (2010) L'applicazione delle tecnologie innovative sulla rete ferroviaria della SEPSA: apparato centrale computerizzato e nuovo materiale rotabile. In: proceedings of cifi conference, Naples
5. Fiumara F (2008) Come si gestisce la sicurezza: il caso delle Ferrovie dello Stato. Safe Secur 7:24–26
6. Wilson JM, Jackson BA, Eisman M, Steinberg P, Riley KJ (2007) Securing america's passenger-rail systems. Rand corporation, Santa Monica
7. Flammini F, Mazzocca N, Pragliola C (2008) Protezione delle infrastrutture di trasporto su ferro. Safe Secur 8:12–16
8. Jenkins BM, Butterworth BR (2010) Explosives and incendiaries used in terrorist attacks on public surface transportation: a preliminary empirical analysis. Mineta Transportation Institute, San Jose
9. Butterworth BR (2011) Empirical data to guide risk mitigation: examples from MTI database. Mineta transportation institute national, Transp Secur Cent
10. Murolo F (2008) Gli impianti tecnologici nella nuova stazione di Montesanto della SEPSA. In: Proceedings of f.s.-cifi conference, Naples
11. Snyder LV, Scaparra MP, Daskin MS, Church RL (2006) Planning for disruptions in supply chain networks. In: Johnson MP, Norman B, Secomandi N, (eds) Tutorials in operations research, Chap. 9, Informs
12. Boccia M, Sforza A, Sterle C (2009) Flow intercepting facility location: problems, models and heurisics. J Math Model Algorithms 8(1):35–79
13. De Cillis F, Sforza A, Sterle C (2013) Optimal location of flow intercepting facilities to improve security in urban areas. Int J Syst Syst Eng 4(3–4):222–242
14. Cappanera P, Scaparra MP (2011) Optimal allocation of protective resources in shortest-path networks. Transp Sci 45(1):64–80
15. Hakimi SL (1964) Optimum locations of switching centers and the absolute centers and medians of a graph. Oper Res 12:450–459
16. Hakimi SL (1965) Optimum distribution of switching centers in a communication network and some related graph theoretic problems. Oper Res 13:462–475
17. Church RL, Scaparra MP, Middleton RS (2004) Identifying critical infrastructure: the median and covering facility interdiction problems. Ann Assoc Am Geogr 94(3):491–502
18. Snyder LV, Daskin MS (2005) Reliability models for facility location: the expected failure cost case. Transp Sci 39(3):400–416

Coping with Suicide Bombing Israel Railways Security Challenges 2000–2005

Chanan Graf and Yuval Alon

Abstract This chapter presents an analysis of suicide bombing attacks carried out during a period of 5 years against the Israel Railways. Its draw upon data collected from interviews with Israel railways officials, the Israel Security Agency database and open sources. The chapter is divided into three main parts: (1) a brief overview of the Israel railways; (2) a description and analysis of suicide bombing attacks during the relevant period; (3) description of the response measures taken by the Israel Railways with regard to the threat.

1 Forward

Societies across the world relay on reliable, safe and convenient public transportation. Unfortunately, alongside with the rapid development and growing importance of public transportation systems, there is also an increase in the level of terror threats to industry. The rising number of terror attacks on public transportation systems in the last decade—including the lethal attacks on the Madrid (2004), London (2005), Mumbai (2006) and Russia (2009) systems—as well as the numerous terror plots that were averted, are indication to the attractiveness of public transportation systems as preferred terror targets.

Though terrorists use a variety of tactics to attack transportation targets, one of the main threats—arguably, the biggest one—to public transportation security is suicide bombing attacks. Suicide bombing attacks directed against public transportation systems are such big threat due to the fact that from one hand they are particularly difficult to prevent, and from the other hand create large impact both in terms of casualties and psychological effect on the society.

C. Graf (✉) · Y. Alon
G.Team Security Ltd, 96, Ahuza Street, 43450 Raanana, Israel
e-mail: chanan@gteamsecurity.com

Y. Alon
e-mail: yuval@gteamsecurity.com

R. Setola et al. (eds.), *Railway Infrastructure Security*, Topics in Safety, Risk, Reliability and Quality 27, DOI 10.1007/978-3-319-04426-2_6

Throughout 2000–2005 the Israel Railways was coping with a sustained threat of suicide bombings that was part of the terrorist suicide bombing campaign of the second “intifada”. Facing with that challenge, the company responded by developing a security strategy that was designed to allow a continuity of rail services while providing enhanced level of security for the passengers.

This chapter aims at providing insights for policy makers, security professionals, public transportation operators and other stakeholder’s, through the analysis of Israel Railways response to the threat of suicide bombing terrorism. While context and conditions may differ greatly between Israel Railways and European or American operators, the authors of this section believe that some useful insights can be realized through the analysis of this case study.

2 Israel Railways

Israel Railways Company Ltd.—established at 1948—is the state-owned principal railway company responsible for all inter-city, commuter, and freight rail transport in Israel.

By the mid-fifties the company was operating steam engines and outdated carriages succeeded from the British mandate train service. Throughout the fifties this obsolete equipment was gradually replaced with diesel engines and modern carriages and the last steam engine was retired at 1959.

During the sixties and the seventies the main effort of the Israel Railways was concentrated on the expansion of the existing network. Despite the development of the network the growth of rail services was halted by lack of public interest in rail transportation. Only the restructuring and modernization of the Israel Railways in the 1990s brought a fundamental change in the level of ridership and public perception of rail transportation.

Nowadays, the Israel Railway is one of the modern rail operators in the world (average age of rolling stocks—20 years) with many on-going development projects. The company operates 47 passenger’s stations and 30 operational stations serviced by a tracks network of 1,100 km. The company runs approx. 450 passenger’s trains daily.

The network is centered in Israel’s densely populated coastal plain, from which lines radiate out in many directions (Fig. 1).

3 The Suicide Bombing Campaign, 2000–2005

The Israeli—Palestinian conflict have taken many forms throughout the decades and claimed numerous victims from both sides. The “second intifada” (2000–2005), marked a new stage in the conflict; a stage which was characterized by the large number of suicide bombing attacks.

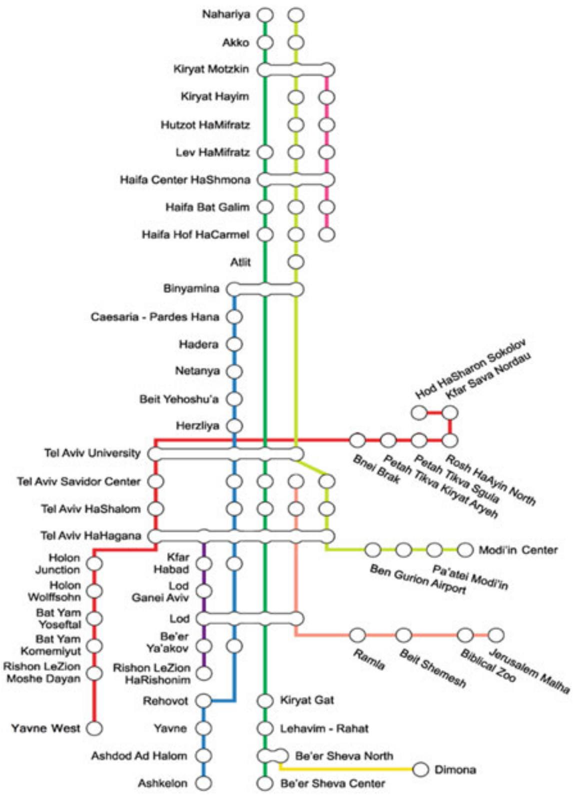


Fig. 1 The Israel railway network

During the second intifada, Palestinian organization (and particularly "al-Aqsa Martyrs' Brigades, Hamas and Islamic Jihad") waged numerous deadly suicide bombing attacks against Israeli targets inflicting high death toll. The effect of the suicide bombings campaign proved to be devastating to the Israeli society and lead to a significant escalation of the conflict.

Towards 2006 and onward there was a gradual reduction in the intensity of suicide bombing attacks. There were many reasons for that decline (which are not mentioned here, because they are beyond the scope of this section paper). The aim of following paragraphs is to describe the threat environment that affected the security of Israel Railway in that period, and to provide the context for the shift in its security strategy made as response for these threats.

From the beginning of the second intifada (September 2000) until the end of 2005 (which is considered as the cessation of that round of confrontation) compressively about 25,770 attacks have carried out against Israeli targets. These attacks claimed the lives of 1,178 people with additional 8,022 people injured in various degrees of severity. The Figures below provide the division of fatalities and injuries per year (Figs. 2 and 3):

A variety of tactics were used to carry out such attacks, but a distinct characteristic of this period was the wide use of suicide bombing attacks. A staggering

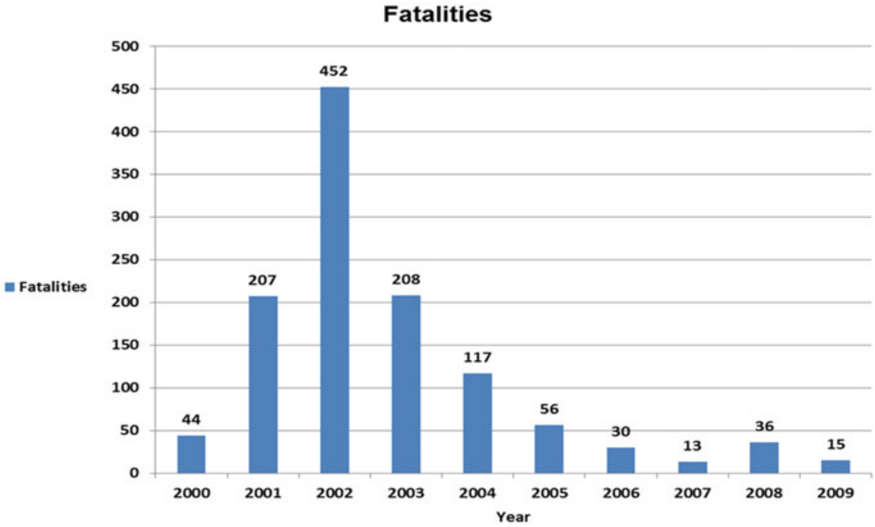


Fig. 2 Number of fatalities

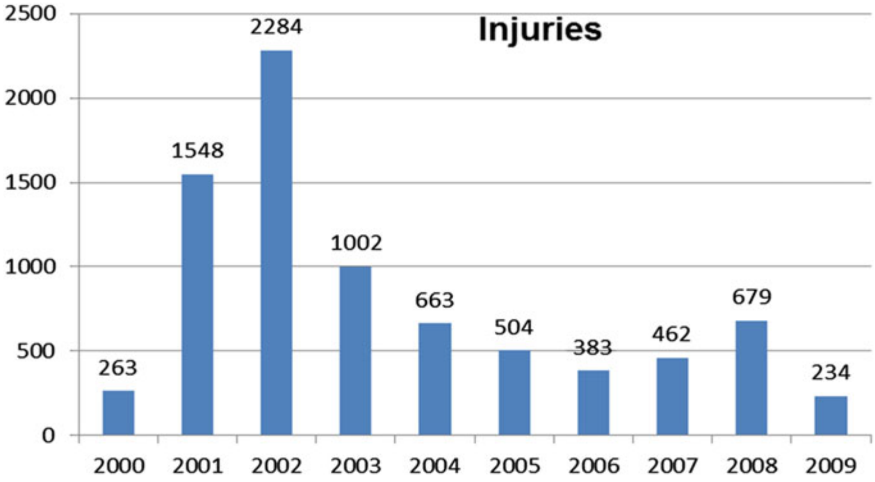


Fig. 3 Number of injuries

number of 146 suicide bombing attacks have been carried out during the second intifada and more than 389 suicide attacks have been foiled by the Israeli security forces. The Fig. 4 describes the number of suicide bombing attacks per year.

Analysis of fatality's numbers revels that although the majority of terror attacks were carried out by other tactics—such as Vehicle Born Improvised Explosive Devices (VBIED), Improvised Explosive Devices (IED), shooting—suicide bombing attacks are responsible for the majority of the fatalities. Of the total

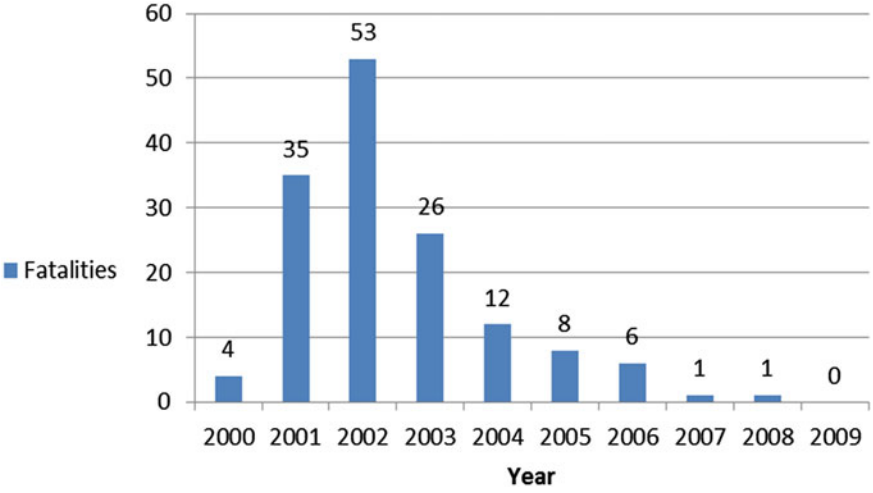


Fig. 4 Number of suicide bombing attacks per year

number of 1,178 fatalities almost 50 % were attributed to suicide bombing (516 fatalities). This statistic is clearly shown in the Fig. 5.

Not only that suicide bombing attacks proved to be the most deadliest and difficult to prevent, but they also caused a profound psychological effect on the Israeli society by creating a deep sense of insecurity. The majority of suicides bombing attacks were directed against public places such as shopping malls, entertainment hubs, markets and public transportation where mass killing is assured and security is difficult to provide. In particular, public transportation system seemed to be prone for such attacks.

Analysis of the available data shows that public transportation was prime target for suicide bombing attacks during that period. Much like other public

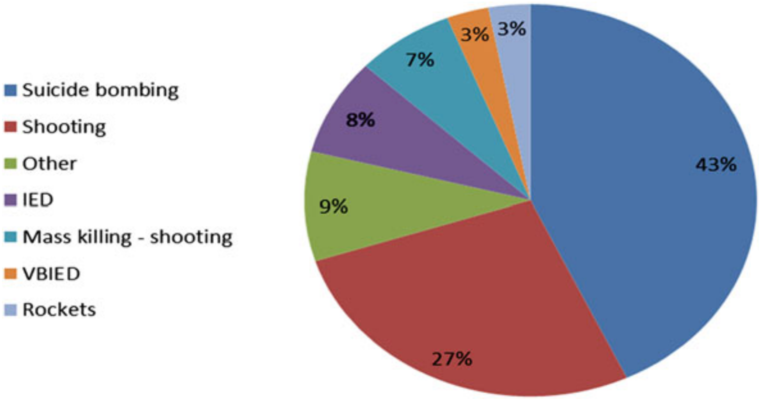


Fig. 5 Percentage of fatalities by most lethal attack tactics

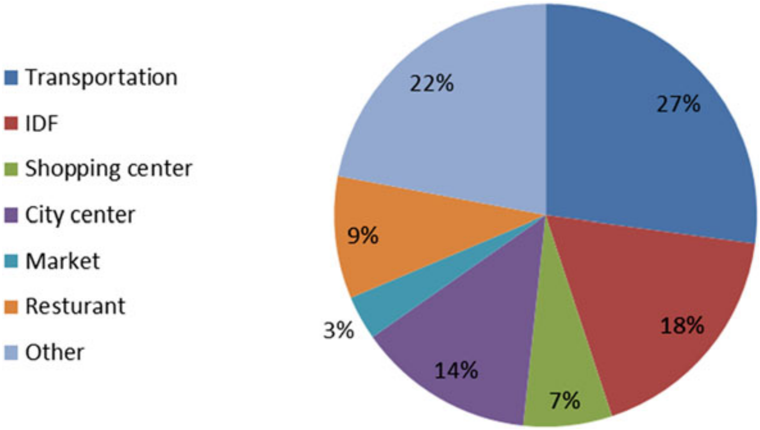


Fig. 6 Percentage of suicide attacks by target

transportation systems around the world, the public transportation sector in Israel is particularly vulnerable to terror attacks due to its inherent characteristics and a successful attack is likely to result in mass killing.

Indeed, as evident from Fig. 6, the majority of suicides bombing attacks (27 %) during the second intifada were directed against public transportation targets. These targets included mainly buses, bus stops, bus terminals, and train stations.

Not only the number of suicide bombing attacks against transportation targets was higher than the number of attacks against any other type of targets, they proved to be the most lethal. Figure 7 shows the percentage of fatalities according to target type.

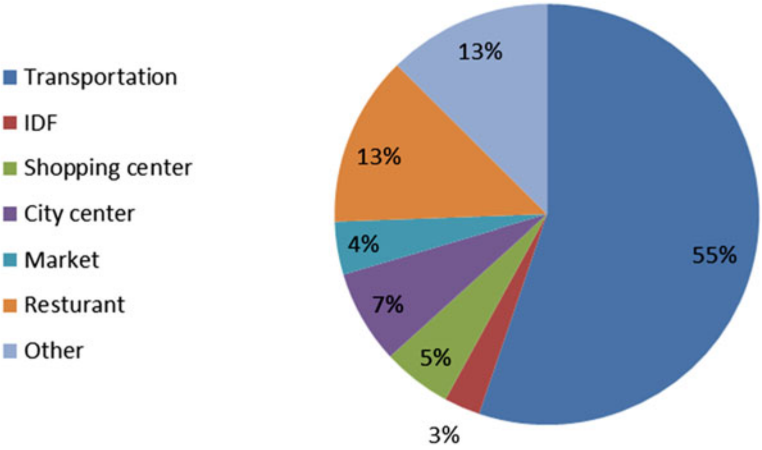


Fig. 7 Percentage of fatalities by target

Beyond the high number of casualties caused, the suicide bombing attacks also created a profound sense of fear that lead to sharp decline in the use of public transportation by the Israeli public. Only people which didn't had other alternatives continued to use busses and trains. In order to cope with the suicide bombing attacks against the public transportation sector, Israeli security authorities (mainly the police and ministry of transportation) and Israel Railways have taken a series of measures designed to prevent attacks and minimize their impact if materialized.

4 Israel Railways Response to Suicide Bombing

Since its establishment, the Israel Railways had to cope with terror threats generated from the Israeli—Palestinian conflict. The nature of the threats against railways was ever changing and forced the company to revise its security policy repeatedly to meet different tactics and modus operandi used by the terrorists in the various stages of the conflict.

- Sabotage and stand-off shooting
- High profile attacks (e.g. attacks which involve hostage taking)
- Suicide bombers attacks

In particular from the fifties until the mid-seventies the majority of terror attacks involved incidents of sabotage and stand-off shooting that mostly occurred in track areas located close to the Israeli borders. These attacks were usually carried out by perpetrators who crossed the borders with the intent to carry out surprised attacks and to escape back. Since the mid-seventies the nature of threat changed as the terrorist organization began to concentrate efforts in drawing the attention of the international media through execution of high profile attacks, and in particular, attacks which involve hostage taking. Another change in the terrorist's modus operandi occurred in the middle of the 1990s (the first "Intifada") when the first wave of predominantly religiously motivated suicide bombers carried out a number of devastating attacks.

The outbreak of the second intifada marked another shift in the modus operandi of the terror organizations; the wide use of suicide bombing attacks against public areas in Israel and in particular against public transportation. Although most of the suicides bombing attacks were directed against the Israeli bus system it was apparent that an attack on Israel Railways targets is only a matter of time.

These concerns were soon materialized when on the middle of 2001 two suicide bombing attacks were carried out against railway stations, followed by additional attack on the first half of 2003 (Table 1).

Analysis of the attacks reveals that while the operational characteristic of the attacks differ one from another, none of the terrorists succeed to enter the stations and to explode on the platforms or inside a train. Although these attacks resulted with a considerable number of casualties it is clear that the security measures implemented by the Israel Railways prevented a much higher death toll.

Table 1 Suicide bombing attacks against railways' stations

Date	Target	Delivery mode	Casualties	Description
16.07.2001	Benyamina station	Suicide belt	2 fatalities, 6 injuries	The terrorist, a man in his early twenties, arrived to the station around 19:35 carrying a suicide belt containing approx. 20 kg explosives and shrapnel. The terrorist intended to enter the station but when he noticed the increased presence of security guards, he crossed the road, and blew him-self at a bus stop opposite to the station
09.09.2001	Nahariya station	Carton box	3 fatalities, 94 injuries	The terrorist, a 58 years old man concealed the IED inside a carton box. Around 10:30 AM the terrorist blew him-self up just outside of the entrance to the station
24.04.2003	Kefar—sava station	Suicide belt	1 fatality, 16 injuries	The terrorist, an 18 years old boy, arrived to the station carrying a suicide belt around 07:20 AM. He was stopped by security guards at the entrance to the station and blew him-self up. The security guard was killed

5 Israel Railways Security Response

In response to the increased threat of suicide bombing the security division of the Israel Railways has adopted a security strategy that relays on several fundamental concepts:

- Emphasis on prevention;
- Continuous risk management process;
- Reliance on intelligence, use of profiling;
- Strengthening public awareness;
- Use of balanced combination of human resources with advanced technologies.

Prevention of terror attacks in rail systems is considered by many as an impossible task due to their inherent characteristics which are designed to be open, accessible and convenient. In light of that, at the time, most railways operators concentrated their efforts on response and recovery activities. The decision made by the Israel Railways to focus on prevention and pro-active strategy based on the perception that in order to minimize mass killing most efforts should be concentrated on stopping the terrorists as far as possible from their target, i.e. before they enter into the stations.

Risk management process is known to be a vital tool for coping with security threats. In response to the suicide bombing threat the Israel Railways initiated a process of methodology refinement to ensure adequate response is provided. Numerous security audits were carried out, both internally and by external body's (such as the Israeli police). Identified gaps found mainly with relation to protection of infrastructure and the perimeter of several stations.

Debriefing of past attacks discovered that in some cases civilians and members of the security forces had identified suicide bombers prior to the actual attacks. Some of them described "a gut filling" when seeing suicide bombers without being able to explain what was the cause for that feeling. Understanding the importance of the public as "human sensors" the Israel Railways security division launched an extensive awareness campaign directed at both the passengers and the railways staff. The awareness campaign included mainly placement of posters in the stations and use of pre-recorded messages. Employees were trained with specialized course and repeatedly instructed to report immediately about suspicious persons.

Considerable efforts were made by the Israel Railways security division to improve the flow of information between the organization and intelligence agencies and the police. Throughout this period the company managed its resources—raising and lowering the alert levels in its facilities—based on Intelligence information. This measure was proved its importance in the attack on the Benyamina station (16.07.2001). Acting upon targeted intelligence, the station's security was reinforced significantly with additional security guards, deterring the terrorist from entering into the station (when noticing the heavy presence of security personnel he detonated the explosives opposite to the station).

In the unique conditions of the second intifada it was clear that passengers will be willing to accept some degree of inconvenience assuring higher level of security. Consequently, the security of the stations was strengthened with special emphasis on the external layer. Passengers arriving to the stations were screened (using the profiling process which is described in following paragraphs) by security personnel and then were subjected to search by walkthrough metal detector and X-Ray scanners. Additional measures included—for example—installation of barriers to distance vehicles (to minimize effects of VBIED's), use of dogs for explosives detection and deterrence, and extensive deterrence activities carried out by security personnel at the station's perimeter.

One of the biggest challenges of the Israel Railways security division when coping with the suicide bombing during the second intifada was in relation with the issue of profiling. The Israeli security concept traditionally emphasis the critical role of the human factor as key success element in the prevention of terror attacks. The main notion is that security cannot rely on technology alone and well-trained, highly competent security personnel are essential for coping with security threats. The profiling method is one of the most important tools used by Israeli security personnel and it proved its efficiency repeatedly in the fight against terror in Israel.

This method has several dimensions but in the context of rail transportation it is mainly involve the identification of potential terrorists through external indicators (typically referred as "suspicious signs"). In particular, these are indicators found in

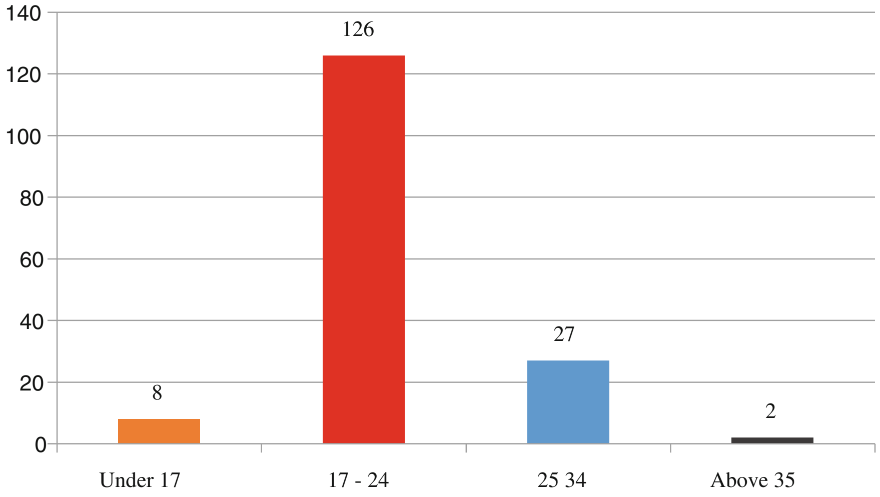


Fig. 8 Age distribution of suicide bombers

the appearance and behavior of an individual which may link him to potential terrorist activity.

Experience accumulated prior to the second intifada (and in particular in the first intifada) led Israeli security professionals to construct a series of signs that can provide indication of a suicide bomber. Such signs included among others:

Irritated face skin due to a freshly shaved beard (because most suicide bombers were fanatic religious who grow beards for many years and shaved them before action in order to blend with environment);

"Tunnel vision", a person that is fixed on the target and doesn't pay attention to the surrounding;

A person that express nervousness and physical symptoms of stress;

A person that wear big size clothing's (to conceal the explosive belt) or carrying heavy bag;

However in the early stages of the second intifada it became apparent that this profile is no longer valid due to a significant change in the characteristics of suicide bombers. Unlike the past where the majority of suicide bombers were identified with religious groups, the suicide bombers of the second intifada came from all walks of the Palestinian society, including a significant number of females. Only as the number of suicide bombing attacks grow, it became possible to draw a typical profile of the typical suicide bombers. Analysis of attacks reveled that most of the suicide bombers were young (under 24), single and well-educated. The Fig. 8 provides some statistical data about the profile of the suicide bombers in the second intifada (Figs. 9 and 10).

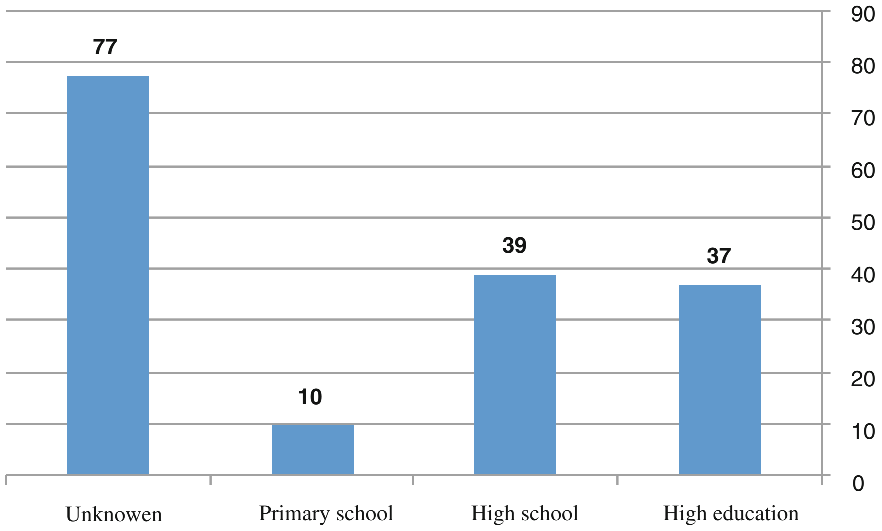


Fig. 9 Level of education of suicide bombers

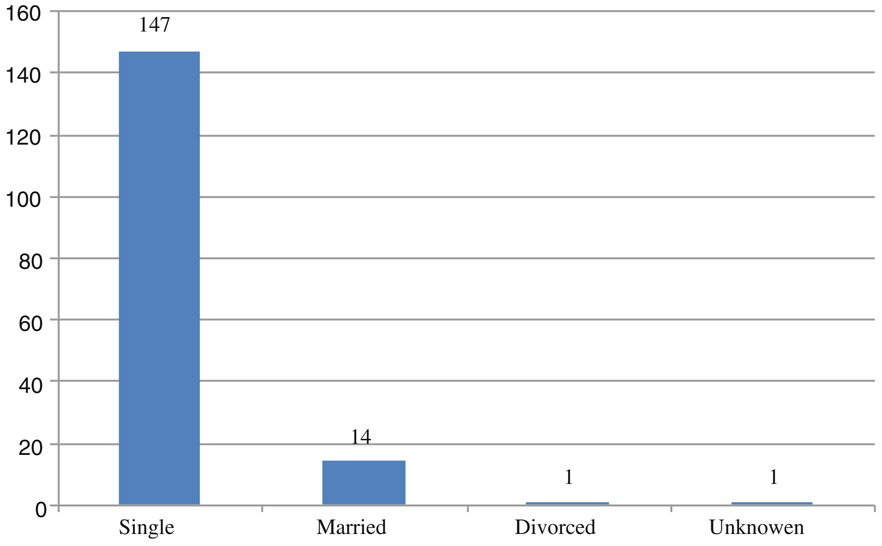


Fig. 10 Marital status of suicide bombers

Regarding the motivation of the suicide bombers, research showed that they can be classified into four distinct prototypes:

- Religious;
- Political;
- Revenge;
- Social.

Based on that analysis the security agents of the Israel Railways were be able to concentrate their efforts on passengers with similar profile. The security division of the Israel Railways developed a specialized training program for its security guards which emphasize the various aspects of profiling.

The implementation of new security technologies played an important role in the effort to reduce terror threats. The Israel Railways invested much effort and resources in installation of advanced security systems to protect stations. Various sensors and physical means were installed in the stations in order to create sterile areas and to limit access to authorized access points. This initiative proved to be more complex than anticipated due to limited availability of effective security systems capable of operating successfully in the unique conditions of rail environment. For example, when trying to install vibration sensors near track areas at the entrances of the stations, it became apparent that none of the available systems is suitable due to the huge number of false alarm produced by the train itself.

In parallel, the organization began a challenging and complicated process to protect its critical infrastructure. This step became necessary because of the rise in the number of incidents directed against the trains—mainly derailment attempts—through tracks sabotage and concealing of IED's charges under the tracks. Various sensors were installed at bridges and tunnels mostly integrated with specially developed software integration.

6 Conclusions

Experience shows that coping with the phenomenon of suicide bombing attacks is a very difficult task. Preventing a detriment suicide bomber from succeeding in his/her attack is almost impossible unless exceptional measures are implemented. Facing a sustained threat of suicide bombing attacks during the second intifada the Israel Railways responded by implementation of a series of countermeasures in a scope and scale unlike anywhere in the world.

Although three suicide bombing attacks were successfully carried-out against Israeli railways, there are many evidences that numerous other attacks were prevented due to the security measures implemented by the Israeli security professionals. Moreover, the consequences of these two attacks were relatively limited due to the inability of the perpetrators to enter inside the stations.

It is clear that most of these measures cannot be implemented in European countries (due to the different conditions, culture and railway dimensions), however some lessons can be learned. In particular, some aspects of the Israel Railways concept with regard to information sharing, public awareness and risk management that can be adopted also by European rail operators.

Still, the threat of suicide bombing remains a serious challenge and it appears that suitable response will be achieved only after additional technological developments (such as stand-off detection of explosives).

Further Readings

1. Israel Railways web site: http://www.rail.co.il
2. “Fifty years to the Israel Railways”, an Israel Railways publication
3. “Analysis of terror attacks in the last decade”, Israel Security Agency
4. “Suicide terrorism throughout the Israeli—Palestinian conflict (September 2000–December 2005)”, information center for intelligence and terror
5. “The rise and fall of suicide bombing in the second intifada”, Yoram Schweitzer
6. “Summary of suicide attacks on Israel railways targets”, Israel Railways
7. “Palestinian violence and terrorism since September 2000”, Ministry of Foreign Affairs

Technologies for the Implementation of a Security System on Rail Transportation Infrastructures

Pasquale D'Amore and Annarita Tedesco

Abstract Rail-based transportation systems nowadays constitute highly attractive targets for terrorist organizations as evidenced by repeated attacks in recent years. This is due to the fact that rail-based transportation systems are open systems that move high volumes of passengers daily, this two aspects make the system very vulnerable and extremely difficult to protect. It is well known that transportation is the backbone of the economy. The network of railways, keeps people and goods moving across the country and around the world and the urban metros today are the most efficient solution for the town mobility in the environmental respect. Therefore an attack to a metro or to a railway is an act of great relevance for media and for people and can cause big damages to the community. Railway transportation has some characteristics that make it vulnerable to an attack: trains make scheduled stops along fixed routes; their operations depend on people having quick and easy access to stations and trains and this results in large numbers of access points. In this context it becomes necessary to define the concept of "Security" in railway and metro transportation systems in order to enhance their level of security, while keeping their attributes of openness, extensiveness, accessibility, and affordability. The main challenges of a railway security system are:

- Ensure the security of passengers at stations and on board trains;
- Ensure the security of personnel;
- Protect critical assets;
- Protect the signalling and traffic control systems (IT and Telecoms);

All these targets must be accomplished while safeguarding the continuous operability of the rail-based transportation system. In addition, a reliable and efficient security system has a very effective preventive and reassuring function, because an asset (e.g. a station) will become less attractive for a possible attack.

P. D'Amore (✉) · A. Tedesco
Ansaldo STS, Naples, Italy
e-mail: pasquale.damore@ansaldo-sts.com

A. Tedesco
e-mail: annarita.tedesco@ansaldo-sts.com

R. Setola et al. (eds.), *Railway Infrastructure Security*, Topics in Safety, Risk, Reliability and Quality 27, DOI 10.1007/978-3-319-04426-2_7

Keywords Railway infrastructure system security · CCTV · Video analytics system · Access control and anti-intrusion system · Abnormal sound detection · CBRNe

1 Introduction

A railway or a metro system are infrastructures potentially vulnerable to attacks, that can range from simple vandalism to sabotage and terrorist attack.

Furthermore railway systems are more vulnerable than metros, because the distance between two next stops is very far (difficult to protect the tracks, many access point to the tracks) and the route normally runs along the towns (on bridges, levels crossing, etc.).

The most critical challenge for railways and metros throughout the world is enhancing their level of security, while keeping their attributes of openness, extensiveness, accessibility, and affordability.

The concept of Security for Railways and Metros may be defined as monitoring and protecting the infrastructure (stations, tunnels, rolling stock, bridges, viaducts, depots, yards, etc.), and the users (both passengers and working personnel) against:

1. Aggressions and anti-social behaviours;
2. Thefts and vandalism;
3. Sabotage and terrorism;
4. Unauthorized access to restricted areas.

This goal must be achieved safeguarding the continuous operability of the whole system.

While security can never be absolute, a security system also has a very effective preventive and reassuring function: a metro or a railway will be less exposed to possible attacks if it appears more secure and accordingly it will be considered much more as a valid mass transport way by people.

The typical approach to the design of a security system in rail-based transportation is made up by four main building blocks:

1. Risk Analysis;
2. Risk assessment;
3. Design of sensing and monitoring subsystems;
4. Design and development of a security integrated management system.

This article deals with the risk analysis problem, and with the main security technologies and their application for the protection of a rail-based transport system.

Furthermore in this article the topic of a security integrated management system is discussed, giving more explanations about the characteristics and the functionality it should have.

2 Railway/Metro Security System: Application Context

The issue of protection of passengers, material and immaterial assets, and of human resources is a fundamental matter for modern railways and metros all over the world.

In this context it is necessary to define the concept of security in rail-based transportation systems, which, in the last years, have been target of tragic terrorist attacks in Europe.

It is quite difficult to properly protect a railway or a metro system, due to their peculiar characteristics:

1. High volume of passengers;
2. Openness and accessibility;
3. Underground environments;
4. Valuable assets distributed in remote sites;
5. Multiple stakeholders.

The application context of a security system, for a rail-based transport system is constituted by those areas that could represent a possible objective of a malicious attack.

These areas are the followings:

1. Stations (that can be divided in areas open to public and restricted areas, closed to public). An attack to this area can cause deaths and injuries;
2. Tunnel and bridges. An attack to these assets can make the train derail;
3. Depot. It’s necessary to protect the depot to prevent events like the copper cables theft and graffitism;
4. Electrical substations. It is necessary to prevent a sabotage attack;
5. Tracks. An attack to these asset can make the train derail

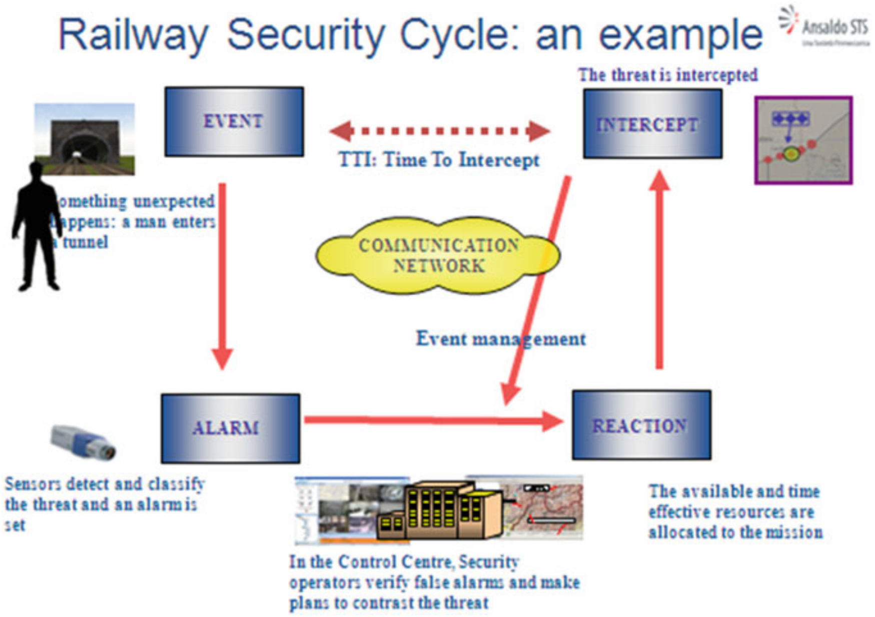
The security solution adopted must be flexible and modular, adaptable for each specific situation and open to be improved and increased during the system lifetime.

The achievement of a reliable and effective level of security is made up not only by the deployment and by tuning of the protection devices but also by the following further steps:

1. Capacity of prevention/reaction to a threat, to avoid/minimize damages;
2. Actions after the accidents occurrence;
3. History of events, interventions and consequences;
4. Procedures to respond to every kind of threat;
5. Continuous improvement of the system and procedures.

So it’s possible to summarize the three key factors of a reliable and consistent security system:

1. Technologies: targeted for the specific infrastructure and asset to be protected and at the state of the art;
2. Procedures: continuously updated according to the needs of the system;
3. Training: to allow the operators to be able to respond to the threats with the adequate preparedness



Railway Security Cycle: an example

The threat is intercepted

EVENT

TTI: Time To Intercept

INTERCEPT

omething unexpected appens: a man enters tunnel

COMMUNICATION NETWORK

Event management

ALARM

REACTION

Sensors detect and classify the threat and an alarm is set

In the Control Centre, Security operators verify false alarms and make plans to contrast the threat

The available and time effective resources are allocated to the mission

Fig. 1 Life cycle for the railway security

The Fig. 1 shows an example of a security cycle for a railway/metro infrastructure.

Starting from an alarm event, a man enters in a tunnel, the sensors installed to protect the asset identify the potential threat and an alarm is set to the operational centre. After the operator verifies that the alarm is true, the resources are allocated to respond to the alarm and the threat is intercepted.

3 Risk Analysis and Risk Scenarios

The possible risk scenarios in a railway or a metro can be classified into four macro categories of threats:

1. Damaging;
2. Goods theft;
3. Sabotage act;
4. Terroristic attack.

To the first category belongs the attacks performed by vandals, with the only aim to damage the facilities of the asset.

The good theft is made to steal valuable goods or devices, for example inside a stations, in technical rooms or to steal the copper cables, which is very common.

The first two categories are more frequent, but otherwise are less severe and don't cause big damages to the assets. Normally these two scenarios involve damages purely economic.

The third and the fourth scenarios are instead much less frequent, but when they happen can cause great damages to the infrastructures and can decrease the operability of the system or as an extreme situation they can lead the system out of service. Moreover these kinds of attacks, above all the terroristic attacks, cause very often deaths and injuries.

So it's important to do an in-depth activity of risk analysis of the infrastructure to be protected (from a station to a complete railway or metro line including depots or yards) in the design phase of a security system of a railway or a metro. This is necessary in order to evaluate the possible threats and to plan the most suitable measures and actions to reduce the risks. The concept of risk is represented by the combination of three main factors:

1. threats and their expected frequency;
2. system vulnerability with respect to the threats,
3. expected consequences of the threats.

To identify the significant attack scenarios and their related risk indexes it's necessary to make a risk assessment, performed after a field inspection through site surveys.

The second step is the risk management, aimed at evaluating the impact, in terms of risk reduction, of the different protection solutions.

The third step is the risk mitigation, performed after risk assessment with the aim to individuate different technologies and procedures to mitigate threats which can damage railway infrastructures.

4 Critical Assets of a Railway System

A rail-based transportation system is divided into many valuable assets. The assets are commonly named Main Areas of Interest (AOI) and are different by typology and function.

Below are listed the main assets:

1. Public areas:

   - main station entrance and corridors;
   - waiting rooms and concourses;
   - underpasses and stairs;
   - platforms.

2. Technical and operative rooms:
   - Command and command centre;
   - interlocking room;
   - technical rooms.
3. Restricted areas:
   - Tracks;
   - tunnels and shaft;
   - Depot;
   - Substations.
4. Open areas (particularly for railway system):
   - Bridges;
   - Viaducts;
   - Level crossing.

Each asset has a different role throughout the system and its correct functionality can affect the functionality and the continuous operability of other assets throughout the system.

For example the continuous operativity of an electrical substation is basilar for the operativity of the whole line. So the electrical substation has to be considered a possible target of a malicious attack and must be protected in the proper way.

5 Security Technologies

A very important phase of the security system design is the choice of the technologies to utilize to adopt adequate countermeasures in order to minimize the infrastructure vulnerabilities.

These technologies must be at the state of the art, cost effective, reliable and long lasting.

The most utilized technological subsystems by the designers to protect the assets of a rail transport system are the following:

1. CCTV and video analytics;
2. Access control and anti-intrusion;
3. Abnormal sound detection;
4. CBRNe.

The combined use of these subsystems allows to fulfill the aim of effectively protect the most critical areas inside the infrastructure and helps the operators to monitor and manage the whole system in real time.

6 CCTV and Video Analytics System

The CCTV subsystem keeps continuously under surveillance the railway assets by means of cameras installed at critical points [1, 2], and it is able to store the video streams over a useful time.

The video surveillance subsystem for the individual site shall be designed with the aim of monitoring critical areas in terms of security criteria, using adequate camera installation parameters (e.g. location point, sight angle, etc.).

Intelligent video analysis increase the video surveillance subsystem and is provided by a sophisticated image processing subsystem, which is able to produce a real-time elaboration of the pictures captured by the CCTV equipments and to identify and automatically tabulate (by comparison with the background) objects and individuals detected in the scene [3].

Spot events detection (unattended luggage, track crossing, abnormal behaviours, overcrowding, etc.) will be automatic: the system will send an alert to the operator, giving information about the kind of event observed and automatically displaying the associated video stream.

The need for the adoption of the automatic video content analysis (VCA) of the camera streams arises from the following considerations:

1. High number of cameras located in a metropolitan or in a railways system, while the number of the operators assigned for their monitoring is low;
2. Difficulty to maintain high the threshold of attention for an operator while monitoring a lot of video streams for a long time.

For these reasons the use of the VCA improves the level of protection of the assets of a railway system with respect to aggressions, thefts, vandalism, up even to sabotage and terroristic attacks.

In order to allow Video Analytics to produce reliable results the video stream needs to be of a certain quality that is related to several technical constraints which need to be fulfilled. These technical constraints must be regarded as a set of impacting factors that need to be adapted carefully for each specific application.

The most important technical constraint for video analysis are the following:

1. Adequate illumination: to get this aim, in stations, vehicles and transport facilities, normally artificial light sources are used to complement the natural light or as the only kind of illumination. Alternatively, it is possible to use the thermal cameras, that work in the infrared range and don't need light sources. These cameras have also the advantage of working well even in poor weather conditions;
2. Frame rate and object or scene kinematics: depending on the application the frame rate can range from some milliseconds up to some seconds. For example, guide way intrusion detection at railway tracks may require real-time performance to detect people or object within 200 or 300 ms to immediately inform the train driver or OCC personnel. The frame rate must be set also depending on the expected speed of the object to be detected, in order to allow its detection through video analysis;

Table 1 Video analytics functions

Function	Description	Action	Example
React	Detection of objects/person entering a predefined area	Motion detection	Protection of areas from unauthorised access
Prevent	Detection of objects being parked within pre-defined area	Suspect package	Detection of improvised explosive device (IED)
Prevent	Counting of person/vehicles or lengths of queues	Counting	Passenger counting system
			Visitor counting system
Prevent	Detection of loitering people	Loitering	Identification of drug dealer, pickpockets, etc.
React	Detection of tampering/vandalism on cameras	Camera tampering	Detection of sabotage of cameras
React	Detection of person moving opposite of common travel direction	Wrong direction	Access supervision of air planes
React	Triggering alarm if virtual fence is passed in any direction	Tripwire	Unauthorised access protection
React/ restore	Detection and tracking of person (if necessary by multiple cameras)	Tracking	Detection of stream of visitor
			Tracking of suspicious person

3. Maximum distance between camera and object to be detected: normally the maximum distance of the object from the camera not exceeds the 40 m, also depending from the object size;
4. Image resolution: of course to have HD cameras improves the quality of video analysis.

Among all the possible available cameras, fixed, PTZ and so on, the thermal cameras are particularly suitable to detect objects and people by video analysis, because they can detect a target much more far than other cameras. Moreover they can work in any illumination condition, also by night and in presence of fog or clouds.

The Table 1 presents the main video analytic functions available to detect issues on rail-based transport systems.

7 Alarm Outputs for a Video Analytic System

The video analytic system should have a good level of reliability in order to be used as a valid detection mean of threats toward an asset or an infrastructure.

The Table 2 shows the possible alarm conditions for a video analytic system and their meanings.

While the system behaviour in case (a) and in case (d) is correct, the other two cases (b) and (c) are problematic from an availability or a security point of view, respectively. The False Positive Alarms are most often called False Alarm. This

Table 2 Events of correct and incorrect detection

		Alarm condition appeared	
		Yes	No
Alarm output by system	Yes	(a) True positive alarms (system outputs an alarm in case of an alarm situation) correct behaviour	(b) False positive alarms (system outputs an alarm although no alarm situation) incorrect behaviour
			Availability-relevant
	No	(c) False negative alarms (system fails to output an alarm in case of an alarm situation) incorrect behaviour	(d) True negative status (system outputs no alarm in case of no alarm situation) correct behaviour
		Security-relevant	

means that an alarm output of the system is not justified from an end user or operator point of view. However, the precise and unambiguous definition of the Alarm Condition is sometimes very difficult and thus also the classification of an alarm as False (Positive) Alarms is often quite challenging. Due to the ambiguity of such an alarm condition from a human perspective this often leads to debates whether an alarm was correct or not.

Anyway, an alarm which was raised in this category and found irrelevant by the operator only causes availability problems, because of the wrong system output. Manual intervention is required in this case to confirm the alarm as False, i.e., irrelevant. Should this event happen too often, serious manual effort is required. As a result, a certain maximum False Alarm rate, e.g., per day, shall be required.

The last category of False Negative Alarms is more critical from a security point of view.

Certain events or situations are not correctly recognized by the system and it therefore fails to output an alarm. Thus, threateningly security situations may be identified too late.

Therefore, the False Negative Alarm rate shall be kept to a minimum.

8 Access Control and Anti-intrusion Systems

Anti-intrusion and access control subsystems are used to detect violation of restricted areas which should be accessible only to authorized personnel (e.g. control rooms). This is achieved by means of personal identification devices and sensors based on different technologies. All these signals are acquired by peripheral subsystems and managed a central monitoring system.

Of course if required, passing an authorized card at the proximity reader installed at the entrance door of a protected area, it is possible to disarm the intrusion detection subsystem in that area. Alternatively, or in addition to, the intrusion detection subsystem may be disarmed by a dedicated keypad or from the Central monitoring system.

The Access Control and Intrusion Detection (ACID) subsystems consist of the following elements:

1. ACID control panel;
2. proximity card readers including keypads;
3. magnetic contacts;
4. horns;
5. Volumetric Detectors;
6. Infrared barriers;
7. Window Glass break detectors;
8. Fence.

The infrared barriers are e.g. installed at the entrance of tunnels and are able to discriminate between a person entering the tunnel and the passage of a train. The magnetic contact instead are installed on the doors and the windows. If someone try to force the entrance to a door without passing an authorized card at the proximity reader, the access control and anti-intrusion system sends an alarm signal to the control centre. The Fig. 2 shows the occurrence explained above.

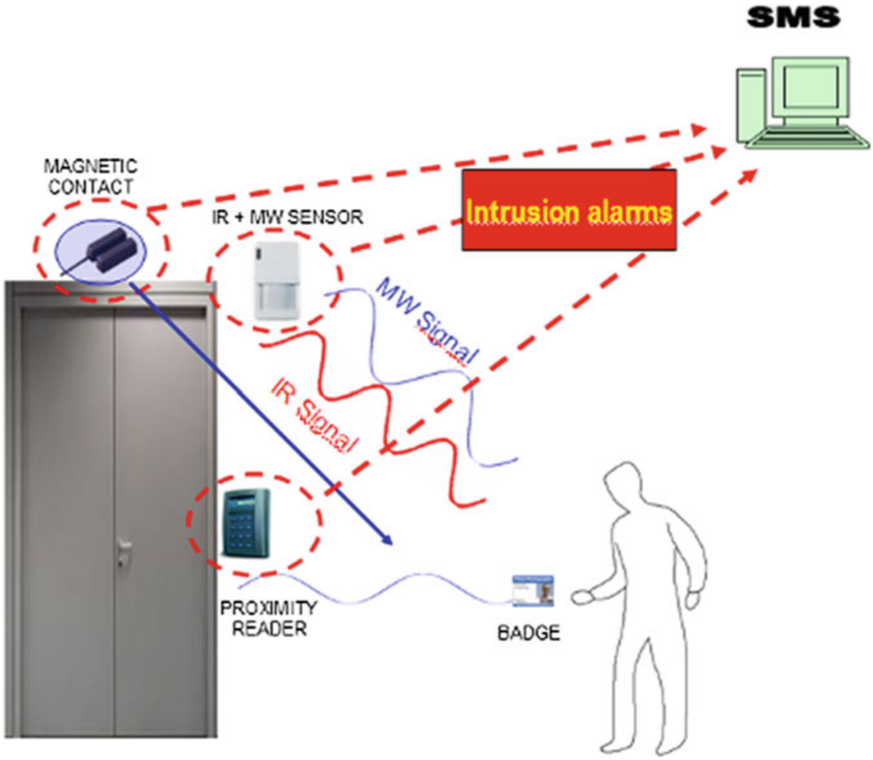


Fig. 2 Example of operation of an access control system

The ACS and IDS subsystems are integrated with the video surveillance subsystem to provide a complete visibility of both, authorized and unauthorized movements within all restricted areas.

9 Abnormal Sound Detection System

The Abnormal Sound Detection (ASD) subsystem provides intelligent acoustic monitoring in critical assets as train stations, platforms, etc.

The system is based on the calculus and analysis of acoustic features acquired by highly sensible microphones which allow to detect the localization of abnormal acoustic events like:

1. Gunshots;
2. Screams;
3. Explosions;
4. Broken glasses;
5. Graffiti.

As listed above, ASD allows to detect events which, due to their peculiarity, sometimes CCTV subsystem is not able to detect.

The phases for the identification process of acoustic events are the following:

1. Acquiring: audio streams are captured by the sensors and transferred to the analysis unit;
2. Pre-processing: audio streams are filtered to eliminate frequency components of less interest;
3. Features extraction: salient features from the audio streams are extracted, these allow to define comparison metrics for the classification and the recognition of different applications;
4. Classification: salient features are compared with audio stream features.

To configure ASD subsystem is necessary a preliminary phase where sensors acquire background noise of the asset to be protected. That allows subsystem to make an accurate tuning and optimize its performance minimizing the False Alarm Rate (FAR) and increasing Probability Of Detection (POD).

The microphones are installed in the open areas of the stations, attended by the public as e.g. concourses, stairs and platforms.

The ASD subsystem is integrated with the central monitoring system, moreover the integration of ASD with CCTV can increase significantly the security level in the asset protected.

The Fig. 3 gives an idea of what events can detect an ASD.

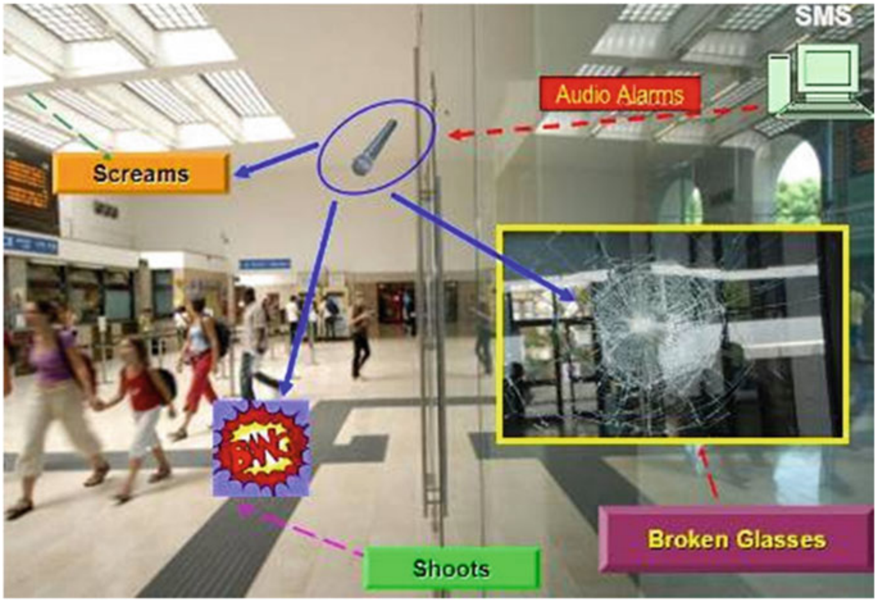


Fig. 3 Events detected by an ASD system

10 CBRNe System

The CBRNe (Chemical, Biological, Radiological, Nuclear and Explosive) Detection subsystem can prevent an attack done by explosive agent (E) or radiological-nuclear (RN), since it can detect the attack before it is acted on, while it can detect a chemical attack (C) and biological (B), only after that the agent has been released, so in this second case we can only try to limit the effects of the attack.

The CBRNe subsystem is provided of a function for each agent to be detected. The Chemical Detection function will be able to detect the agent and to classify it, to allow a quickly and precise situational awareness, the activation of right procedures and the alert of right authorities. The Biological Detection function will be able to detect the presence of biological weapons, and to monitor a possible contamination. The Radiological and Nuclear Detection function will able to detect the presence of radioactive sources brought by the terrorist. The Explosive Detection function will be able to detect trace of explosive or hidden object, depending on the kind of device we want to integrate.

The main aims of CBRNe Detection subsystem are:

1. Detect CBRNe threat as soon as possible to protect the passenger;
2. Identify the type of threat in order to maximize the assistance and mitigate the effects of the attack (detect-to-treat analysis).

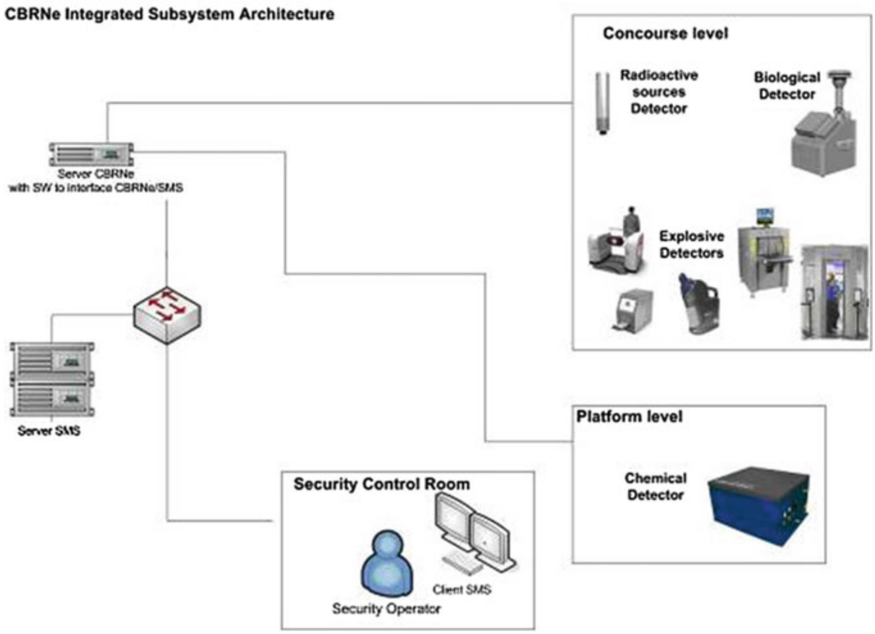


Fig. 4 CBRNE general architecture

(CBRNe) Detection subsystems are located at the entrances to the railway stations and at the main public areas to screen passengers and to detect the presence of the above dangerous agents. The Fig. 4 shows the CBRNe general architecture.

To detect a person who carries radiological-nuclear or explosive or a biological weapon, it could be possible to check all the passengers who queue in front of the turnstiles, waiting for entering the station. But this procedure, similar to those in the airports, is not possible to perform in a railway or a metro system, because the time to execute this check would be very long and would significantly affect the normal operativity of the station.

So in the stations are carried out random inspections on persons identified by station personnel or by security devices (e.g. by cameras through facial recognition algorithms), to focalize the checks only on suspect persons according to predetermined security criteria.

11 Application of the Protection Systems on the Assets of a Railway System

In the following sections the problems concerning the protection of the main asset of rail-based transportation systems are explained.

12 Stations

In the station the most critical areas, that need to be properly protected are:

1. main station entrances;
2. concourses;
3. platforms and tracks;
4. underpasses and stairs;
5. ticket offices;
6. waiting rooms;
7. railway Police offices;
8. technical rooms.

The technological subsystems are used as follows:

1. CCTV and video analytic subsystem—used throughout all the station's areas. It allows to view in real time what happens in the station and, thanks to the video analytics algorithms, in case of dangerous events can generate an automatic alarm and send it to the control centre. In addition the images are stored for a predetermined period, in order to execute forensic analysis in case an accident should occur in the station. This function helps the law enforcement in the investigation on the accident;
2. Anti-intrusion + access control subsystem—used at the entrance of technical rooms (card reader with a magnetic contact on the door). It is also possible to put a magnetic contact inside the rooms as further protection; in public areas of the stations open to public, like concourse, are located volumetric detectors that are activated when the station is closed; at the tunnel entrance are normally installed Infrared barriers who can discriminate between a person entering the tunnel and the passage of a train;
3. Abnormal sound detection subsystem ASD—installed in public areas and in hidden areas of stations, like platforms rear corridors, open to public, in order to detect gunshots, screams, explosions and broken glasses; a more recent kind of use of this technology is inside the train recovery facilities, in the depot, to detect people who enter into the facilities with the aim to draw graffiti over the train coaches.

The Anti-intrusion subsystem, the access control and the abnormal sound detection subsystems, are always used combined with the CCTV subsystem to better protect the station's areas and to helps the operators to monitor the whole station è [4].

13 Tracks

The main problem concerning the tracks, is about their extended length, that can reaches up to hundreds of km for the railway systems.

For this reason the technologies used to protect them are mainly:

1. Active Video Surveillance (Analytics);
2. Distributed Modular System.

The use of distributed modular systems every 200–500 m and of mixed VMD/NMD (motion detection and non motion detection) technics, represents a solution to tracks coverage problem.

Particularly recommended, along the track, is the use of long-range thermal cameras. These kind of camera can indeed covers several hundred of meters of track and also allows to monitor the track during the night and in bad meteorological conditions (clouds, fog and so on).

14 Depot

The main areas of a depot are:

1. external and internal perimeters;
2. area and building entrances;
3. rooms and premises with restricted access.

The main security technologies and equipments installed to protect these areas are the following:

1. CCTV with intelligent video analysis, for the yard;
2. Anti-Intrusion system (sensitive perimetral fence for the external perimeter of the depot;
3. typical security equipment and functions for the depot buildings (access control, anti-intrusion, CCTV);
4. Abnormal sound detection an CCTV for the train recovery facilities.

The abnormal sound detection, the anti-intrusion and control access subsystem are usually used and combined with the CCTV subsystem.

15 Tunnel and Bridges

Concerning tunnels, the critical areas that can create problems if they are not protected are:

1. tunnel entrances—protected by Infrared barriers, fixed and PTZ cameras with motion tracker algorithms;

2. emergency exits—protected by CCTV, Video Analytics, and anti-intrusion devices;
3. ventilation shafts—protected by CCTV, Video Analytics, and anti-intrusion devices.

The critical areas for the bridges are the following:

1 The entry points—protected by fixed and PTZ cameras with motion tracker algorithms;
2 The bridge pillars—protected by seismic sensors.

16 Electrical Substations

In the electrical substations the critical areas are:

1 external perimeter;
2 internal perimeters around the transformers;
3 entrances to the building;
4 technical rooms and premises (inside the building) with restricted access.

All the areas are analysed and monitored by CCTV with video analytic activated, combined with anti-intrusion and control access in order to minimize the false alarm number.

17 Integrated Management of the Protection Devices

To manage all the devices and the peripheral equipments installed on the assets of the railway infrastructure, there is the need of an intelligent software application allowing for the monitoring, analysis, control, command and follow up of all the security installations in one single, user-friendly interface.

This is the core application of any Railway or Metro security system and it is hosted in a central operative room, or in some case in a dedicated room, called security room, surely connected with the central operative room.

It is designed as a fully integrated control/command centre where relevant events detected by the local/peripheral subsystems are received and managed by the operators.

The management system supplies to operators only the informations relevant to activated "real" threats, minimizing the risk of false alarms and therefore optimizing security resources and response time of countermeasures. It also supplies the related emergency procedures, as agreed with the railway operator, and allows for the visualization of both the video streams associated with the alarms (automatically selected) and the ones selected by the operator.

At a glance, the main advantages/features of a Security Management System are listed below:

1 Shared, hierarchical and multi-level architecture;
2 Security management performed at local level;
3 “Rules engines” used at local level for the integration of security subsystems;
4 Integration with security subsystems already in place and train control solutions;
5 Animated graphical maps for alarmed sensors/cameras;
6 Intelligent and easy to use operators tools;
7 Event (alarms and user actions) reports;
8 Emergency management with step-by-step operations monitoring;
9 Tailored specifically for railways and mass transit;
10 User friendly interface.

The security management tool must have an user-friendly interface where the user can find all the information clearly, quickly and can use the last generation web technologies. The map of the sites can be bi-dimensional or in some management tools are also three-dimensional.

Operators can have an animated graphical maps with smart tools for managing alarmed sensors and cameras and by emergency management with step-by-step operations monitoring, as showed in Fig. 5.

In synthesis the principal characteristics of the Operator Interface are:

1 Plenty Ergonomics;
2 Easy and intuitive presentation;
3 Easy navigation through the use of graphic pages (Geographic maps, lay outs, etc.);
4 Use of latest generation WEB technologies.

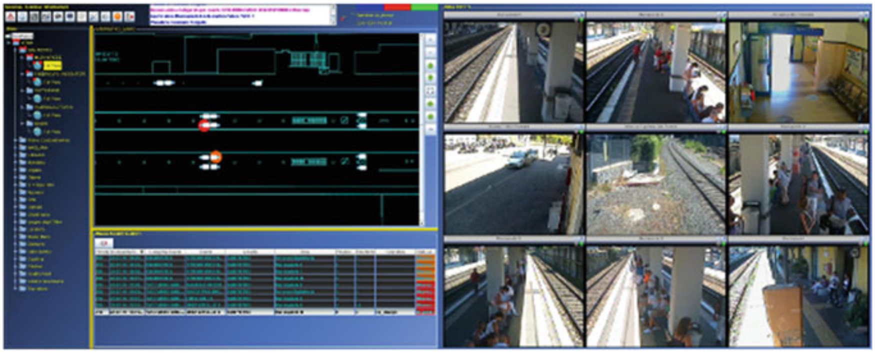


Fig. 5 Operator interface

18 Alarm Management

It must be possible to grade the alarms for their relevance and criticality. The classification of the alarms must be completely configurable and it can be modified in wherever time by the respective operators who have an opposite password for entering the system. The severity of the alarm event has to be highlighted with different colours and can be showed in a geographical map too.

The alarms are also associated to video surveillance areas, so it is possible to activate automatically the video stream associated to an alarm event.

For each alarm event detected, the system can show the operator a personalized operating procedure which is constituted by a set of issue. Each item can be managed by the operator (close, suspend, add comments, etc.) and also it is possible define for each item an automatic action the system can perform (i.e. send e-mail, announce messages via public address, etc.).

19 Conclusions

A security system is a valid support to metro/railway operators to prevent possible attacks and threats brought against the rail transportation infrastructure, that can range from simple vandalism to a terrorist attack.

The effectiveness and the reliability of a security system is strongly dependent on an in-depth activity of risk analysis of the infrastructure to be protected, in order to evaluate the possible threats and to plan the most suitable measures and actions to reduce the risks and on a good risk assessment, performed after field inspections on the sites to be protected.

In addition to these steps, when the security system is installed and fully operating, an educational training of employees working on the system must be provided, in order to allow the best managing of the system. The operators that are in touch with the everyday reality of the rail transportation infrastructure, are capable of identifying before anyone else the possible signs of a risk situation.

The integration of all these features, along with the adoption on the field of devices and equipments at the state of the art, allows to realize a performing and efficient security system that has a preventive and reassuring function on the whole metro/railway system.

References

1. Greenberger M (2006) The need for closed circuit television in mass transit systems. University of Maryland School of Law, Baltimore
2. Cupillard F, Avanzi A, Bremond F, Thonnat M (2004) Video understanding for metro surveillance. Netw Sens Control 1206:95–102

3. Ko T, Raytheon C, Arlington VA (2008) A survey on behavior analysis in video surveillance for homeland security applications. Applied imagery pattern recognition workshop, AIPR ’08. 37th IEEE, pp 1–8, 15–17 Oct 2008
4. Khoudour L, El-Koursi EM, Velastin SA, Buch N, Lim-Thiebot S, Fontaine F (2011) An approach for protecting transport infrastructure. J Rail Rapid Transit 225(4):383–393

A Model-Driven Process for Physical Protection System Design and Vulnerability Evaluation

Valeria Vittorini, Stefano Marrone, Nicola Mazzocca, Roberto Nardone and Annarita Drago

Abstract Vulnerability of railway physical assets against adversary's attacks is affected by a number of factors, hence the effectiveness of the physical security system in charge of protecting the potential targets is a crucial aspect in homeland security applications. This chapter addresses vulnerability modeling and analysis with a special focus on designing physical protection system for railways security. The Model-Driven process developed within the METRIP project is presented, which supports the automatic generation of vulnerability analysis models and the instantiation of optimization model templates for the localization of the protection devices. The steps and the aspects covered by the proposed process are described: the UML profile which has been developed to extend UML with protection and physical vulnerability concepts, the model transformations implementing the interface towards the optimization models and the automated generation of vulnerability models, as well as the mechanism to return the results to the designer. Finally, the overall process has been applied to a railway station from the METRIP case study.

Keywords Physical vulnerability · Model transformation · Railway infrastructure system · UML profile · Model-driven security

V. Vittorini (✉) · N. Mazzocca · R. Nardone · A. Drago
Department of Electrical Engineering and Information Technology (DIETI),
University of Naples Federico II, Via Claudio 21, 80125 Naples, Italy
e-mail: valeria.vittorini@unina.it

N. Mazzocca
e-mail: nicola.mazzocca@unina.it

R. Nardone
e-mail: roberto.nardone@unina.it

A. Drago
e-mail: annarita.drago@unina.it

S. Marrone
Department of Mathematics and Physics, Second University of Naples,
viale Lincoln 5, 81100 Caserta, Italy
e-mail: stefano.marrone@unina2.it

R. Setola et al. (eds.), *Railway Infrastructure Security*, Topics in Safety,
Risk, Reliability and Quality 27, DOI 10.1007/978-3-319-04426-2_8

1 METRIP Model-Driven Process

The ultimate goal of the METRIP model-driven process is to provide a practical support to the design of Physical Protection Systems (PPSs) and to reduce the effort needed to perform a vulnerability evaluation of the target railway system. Its main objective is to enable the automation of the activities to be performed for the localization of protection devices and for vulnerability analysis. At this aim, the METRIP model-driven process encompasses three main directions: models, metrics, and automation.

Models are used at different points of the design and evaluation approach, and they play different roles in the assessment process according to the phase in which they are used:

- UML models are used to represent railway systems, protection devices and attack scenarios. These models contain the information needed to specify the target system, the components of the PPS and the steps of the adversary's attack. They are the inputs for the localization and the vulnerability analysis phases.
- Optimization and localization models are used to provide a solution to the PPS design, according to some optimization objectives (e.g., the complete coverage of an area to be monitored by means of proper closed-circuit cameras). In particular, the solution of a localization model should provide the number and the position of the protection devices, according to the optimization objective. Predefined optimization models are used that must be instantiated by using the parameters values for the railway system and the protection devices which are included in the UML specification.
- Quantitative (probabilistic) models are used to evaluate the vulnerability of a railway system equipped with protection facilities against a specified attack. This modeling phase is automated on the basis of the structure and the information contained in the UML specification (including a representation of the attack scenario).

Modeling is addressed in Sect. 2, with a special focus on the *CIP_VAM* UML profile, a domain specific modeling language developed within the METRIP project.

Proper metrics have been used from the literature or ad hoc metrics have been defined which allow for measuring the vulnerability level of the system, comparing different configurations of the protection system or identifying system vulnerabilities. They provide quantitative indicators, but a detailed discussion about vulnerability attributes and metrics is out of the scope of this work which mainly copes with the definition and realization of the model-driven process.

As for automation, it is achieved at two different levels within the METRIP process. The first level realizes the interface toward the optimization models, allowing the automatic update of the UML specification with the localization data (obtained by solving an optimization model).

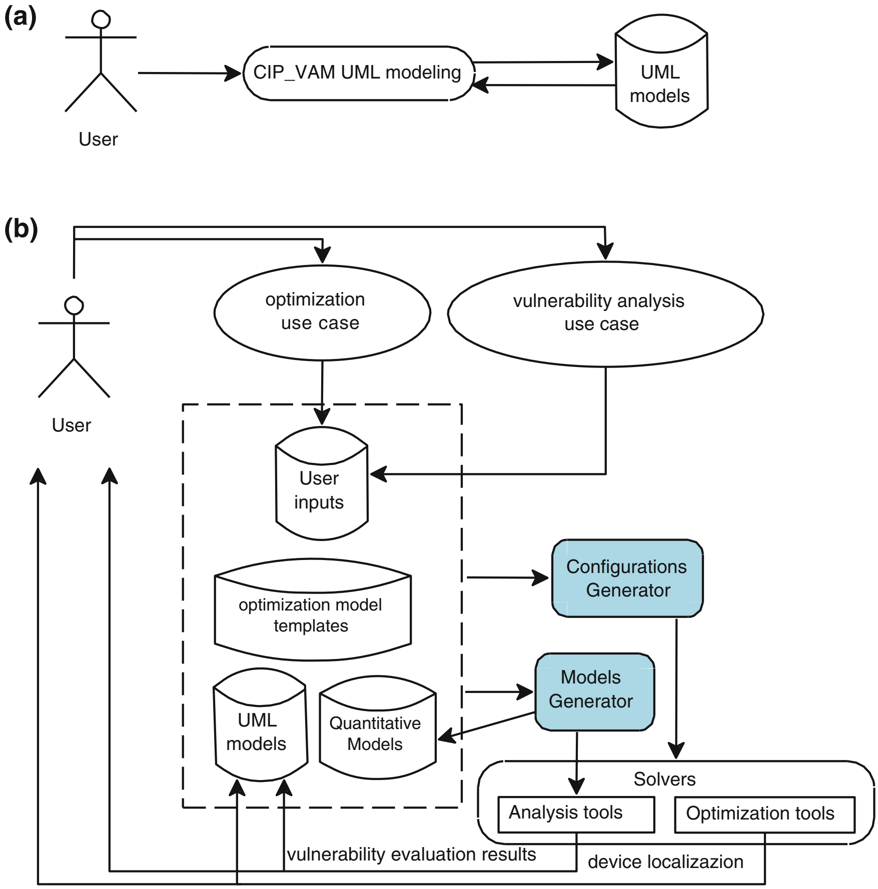


Fig. 1 Approach adopted by the METRIP model-driven process

The second level addresses the automated generation of the quantitative models for the vulnerability analysis.

Both these levels are built from the UML specification, according to a model driven approach based on the definition of proper model transformations. We deal with automation issues in Sect. 3.

A schema of the overall approach adopted by the METRIP model-driven process is shown in Fig. 1. Users, such as PPS designers or security analysts, build the UML models that are the inputs of the overall process (they may also use models previously built and stored). This specification is annotated with stereotypes and tags of the *CIP_VAM* UML profile (Fig. 1a). The user also provides (or retrieves from a proper database) the information needed to complete the specification (e.g., the concrete values of the parameters required to fully describe a specific railway station, or a specific camera, or a given attack scenario). Then, the user choices the kind of study (the use case) he/she wants to perform (optimization/localization or vulnerability evaluation) and provides the inputs needed to configure the study (Fig. 1b). In this step the user also selects the optimization model or the set of measures and indexes to evaluate. All these inputs are used to setup the Configuration Generator, the Model Generator and the Solvers. According to the use case scenario, the Configuration Generator automatically produces the configuration file(s) used to perform the study and invokes the Solvers. If a quantitative vulnerability analysis has to be performed, the Model Generator automatically builds the quantitative model from the UML specification and the user inputs. If the target is the localization of protection devices, the Model Generator automatically builds from the UML specification the inputs for the optimization module. Finally, the required metrics are evaluated by running the Solvers and the results are used to update the UML model and/or delivered to the user, so allowing to re-target the design choices, if this is necessary. The Solvers maybe existing optimization and analysis tools, as exemplified in Sect. 4, where the METRIP model-driven process is applied to model and evaluate of a PPS for a railway station.

2 The *CIP_VAM* UML Profile

The *CIP_VAM* UML profile provides an answer to the need for a Domain Specific Modeling Language (DSML) which enables the modeling of RIS infrastructures, attack scenarios and protection systems.

UML profiling is actually a lightweight meta-modeling technique to extend UML [1]. It is a powerful mean to define DSMLs [2] which exploits two main advantages within a Model-Driven Engineering context with respect to the development of ad hoc DSMLs: (i) a UML profile is effective from the modeler's point of view, as it captures and easily replicates the modeler's architectural knowledge of a specific domain at different levels; (ii) a UML profile allows for the adoption of available and standard techniques and tools which maybe easily integrated into existing production systems. In addition, the usage of a modeling language based on few and well specified domain-related concepts support the definition of model transformations (Sect. 3) so allowing the development of a complete model-driven design methodology.

Hence, the *CIP_VAM* profile extends UML by adding domain specific concepts for the modeling and the analysis of Critical Infrastructure Protection systems and their Vulnerability. Since it is a profile, *CIP_VAM* extends UML through the use of stereotypes, tagged-values and constraints. A systematic approach has been adopted in the profile development, as introduced in [3]. First, a domain model has been defined to cover the necessary concepts according to the practical experience in PPS designing of Ansaldo STS and the current literature [4, 5]. The *CIP_VAM* domain model (described in detail in [6]) is organized into three packages, as shown in Fig. 2:

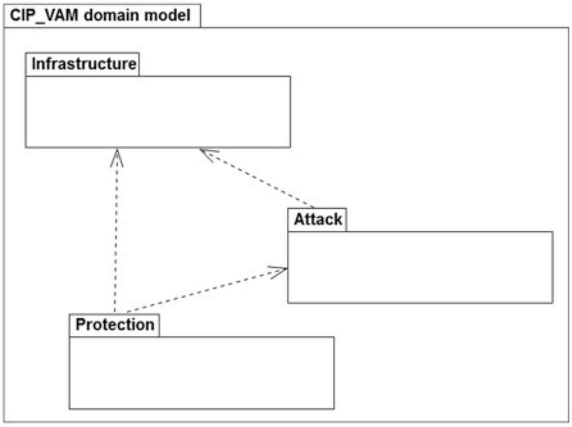


Fig. 2 *CIP_VAM* domain model

- The *Infrastructure* package includes all the concepts which are necessary to a full description of the physical system under analysis. It contains both asset and environmental related concepts.
- The *Attack* package individuates concepts related to threats and attack events conducted against the assets within the infrastructure.
- The *Protection* package introduces protection related concepts and provides a description of techniques and countermeasures which may be applied to defend the assets.

Dependencies between packages stand for relationships between concepts: the target of an attack is always an asset (i.e., a dependency exists between the *Attack* package and the *Infrastructure* package); a protection is applied to a specific asset against one or more attacks classes (i.e., dependencies start from the *Protection* package and arrive to both the *Infrastructure* and *Attack* packages).

Then, the domain concepts have been mapped to the elements of a UML profile. The new stereotypes extend UML meta-classes, specific types introduced by the *CIP_VAM* library are used in the definition of the attributes of the stereotypes.

The profile structure is depicted in Fig. 3, where the high-level view of the *CIP_VAM* Library is also shown. The *CIP_VAM* profile imports an already existing library (i.e., the MARTE library [7]) in order to reuse and extend data types already defined in it, in particular NFP (Non-Functional Properties) types.

The relevant stereotypes, tags and data types, are introduced and described here below. We do not include all the details of the profile, but the information needed to understand the case study presented in Sect. 4.

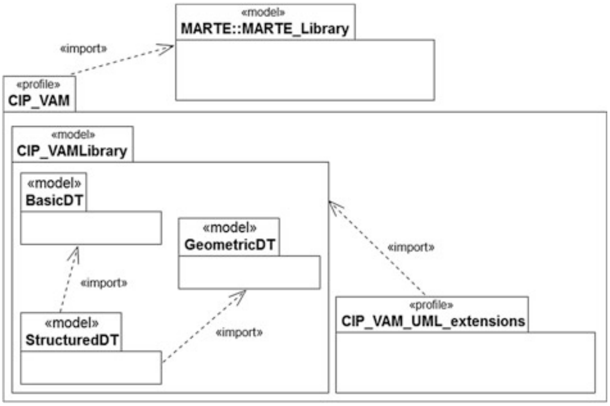


Fig. 3 *CIP_VAM* profile

2.1 CIP_VAM UML Extensions

The stereotypes introduced to model the *Infrastructure* of a RIS have been reported in Fig. 4. The three main stereotypes are: *Site*, *Object* and *Interface*.

Site shall be applied on all modeling elements which represent physical (or logical) areas in which the system under analysis can be decomposed (e.g., control rooms, waiting rooms, platforms, etc.). *Interface*s join more sites, examples are doors, windows, balconies as they join two sites (specified by the *exposures* tag). *Objects* can be located in a site, or they may be considered on their own if no sites are specified (in this case the tag location will not be assigned a value).

Site, *Object* and *Interface* are different specifications of *Item* through the *Physical* stereotype. Both *Item* and *Physical* are abstract stereotypes (i.e., they are not directly applicable on modeling elements): they specify some tags that model features shared by *Sites*, *Objects* and *Interfaces*. In particular, they all may be assets. This is modeled by specifying a value for the tag *asset* (see *Item*) which represents the weight of the asset according to several indexes. Among them, the economic loss in case of destruction, damage or theft of the asset. Hence, by definition, an asset has an economic price.

As for the *Physical* stereotype, its meaning is that, at the state, the entities we deal with are not "virtual" but concrete things. They may have a *shape* and be 3D object (*volume*). With respect to the initial version of the profile [6], the *opacity* tag has been added to specify if a physical entity is not transparent (i.e., it cannot be seen through, for example by an optical protection system).

The hierarchy described above extends UML as the root stereotype *Item* extends the UML meta-class *Classifier*. This implies that its specialized stereotypes can be applied on all the UML *Classifiers* (Classes, Associations, Components, etc.) making it possible the usage of all the UML *Classifier* modeling elements. For example, nested sites can be modeled through a Component Diagram in which

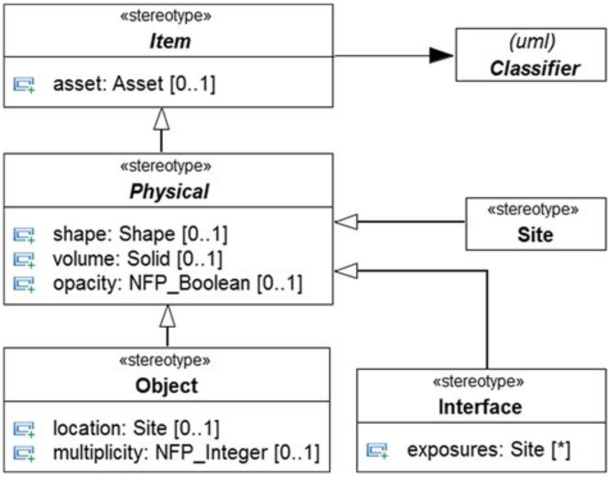


Fig. 4 Infrastructure-related stereotypes (excerpt)

Components can be nested or, similarly, the *Interface* stereotype could be applied on Association because both Component and Association are UML *Classifiers*. This deep specialization chain between stereotypes also enables future extensions of the profile.

The stereotypes introduced to model *Attacks* have been reported in Fig. 5. The main stereotypes in the Figure are: *Attacker*, *Attack* and *Action*. The *Attacker*

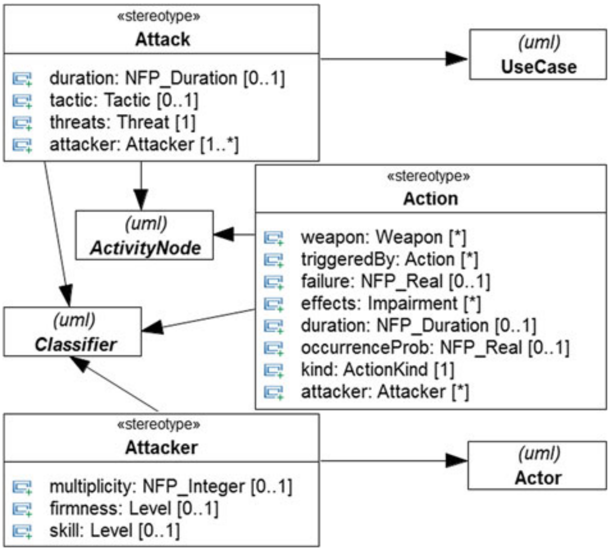


Fig. 5 Attack-related stereotypes (excerpt)

models person or people which conduct an *Attack* against an asset. It is possible to represent the attacker's capabilities through the *firmness* and *skill* tags, while some features of the attack may be modeled using the tags *duration*, *tactic* and *threats*. The *Action* stereotype is introduced to model the steps of an attack. Details about each action may be expressed through its tags: for example, *weapon* may be used to specify the kind of weapons used during a specific attacker's action; *occurrenceProb* tag is the probability that the action is performed.

Attacker, *Attack* and *Action* extend the UML meta-class *Classifier*, too. Nevertheless, further extensions could allow to model an attack by using also different UML modeling elements: *Attack* extends the UML meta-class *UseCase* and *Attacker* extends the UML meta-class *Actor* allowing to reuse the UML Use Case Diagram in modeling the structure of an attack. Finally, *Action* and *Attack* extend the UML meta-class *ActivityNode* so enabling the insertion of attack related concepts into the UML Activity Diagram.

The stereotypes used to model *Protection* facilities have been reported in Fig. 6. In particular the *ProtectionDevice* stereotype may be applied on modeling elements which represents classes of devices. They may be characterized by their *nature* and *failure rate*. *ProtectionDevice* is specialized by the *Sensor* stereotype (e.g., cameras, microphones, bomb sniffer, etc.) which adds information about the *range* of the sensor, its false positive and false negative rates (*fpr* and *fnr* tags) and the sensing *latency*. *ProtectionDevice* is in turn a specialization of the abstract stereotype *Protection* which represents a general protection system (it is not necessarily a device).

Similarly to *Item* and *Physical*, the *Protection* stereotype enables further extensions of the CIP_VAM profile. Hence, its tags are general enough: *cost*, *successProb*ability, *application*, and others. Among them, *application* provides the information about the installation point of a device (e.g., coordinates, height from the ground, etc.). With respect to the version showed in [6], the tag *multiplicity* has been added to the *Protection* stereotype in order to specify the maximum number of protection systems (if necessary).

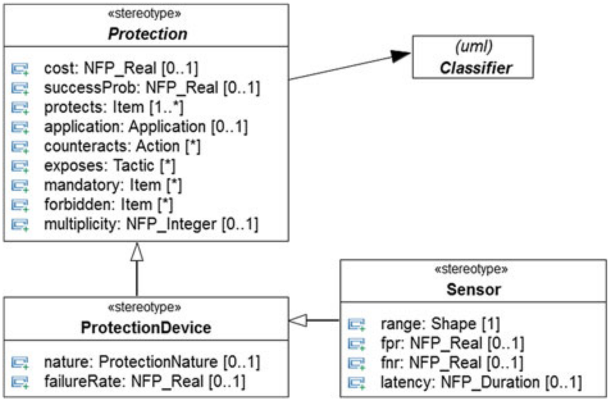


Fig. 6 Protection-related stereotypes (excerpt)

2.2 CIP_VAM Library

The CIP_VAM library contains basic, geometric and structured data types; they are necessary to define the type of some tags. Specifically, the BasicDT package defines a set of simple enumerative types, the GeometricDT package contains the data types necessary to model geometrical features, and the StructuredDT package defines vulnerability related data types. Both GeometricDT and StructuredDT import the MARTE Library (see for example the type prefixed by NFP in Figs. 4, 5 and 6).

The BasicDT package (Fig. 7) includes a set of enumerations, such as *RiskLevel* and *Level* which are needed to the qualitative estimation of a risk or of some generic class of levels; other enumeration types (i.e., *ActionKind*, *WeaponNature*, *Tactic* and *ProtectionNature*) are used to classify the attacks, the actions, the weapons and the protection devices, respectively.

The GeometricDT package (Fig. 8) defines a set of data types needed to model geometrical features of physical systems: in fact the types *Point*, *Shape* and *Solid* are defined. The enumeration (i.e., *PolygonType*) has been defined to simplify the modeling of regular geometric shapes.

The StructuredDT (Fig. 9) package defines a set of complex data types (aggregates of BasicDT types). For example, *Asset* is a structured type which models the weight of a physical asset through several indicators, the *Application*

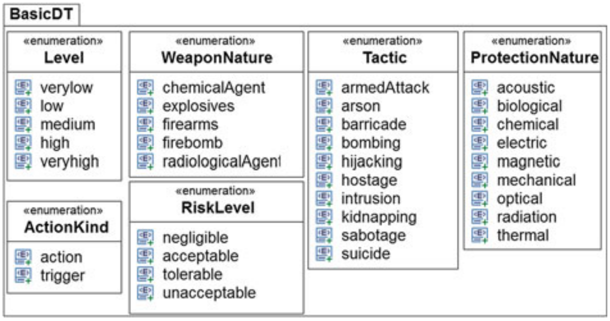


Fig. 7 *BasicDT* package

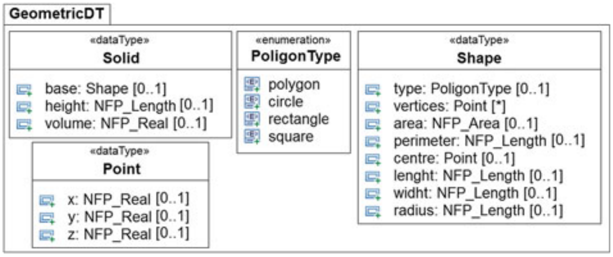


Fig. 8 *GeometricDT* package

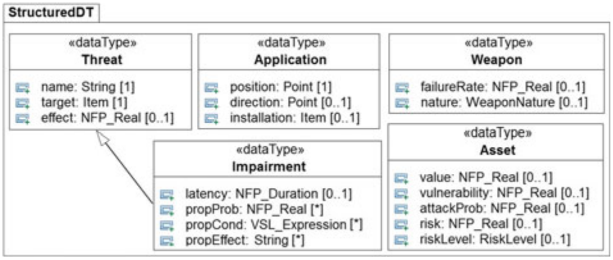


Fig. 9 *StructuredDT* package

data type provides information needed to specify the installation point of a protection device, and *Weapon* is a data type which integrates information about the nature and the failure rate of a weapon.

3 Model Transformations

The automation of the workflow underlying the PPS design and vulnerability evaluation described in Sect. 1 is based on the development and the usage of proper model transformations [8] which are a key technique in Model Driven Engineering (MDE) [9]. The realization of the METRIP process requires the definition of both Model-to-Model (M2M) and Model-to-Text (M2T) transformations, which need also to be combined into transformation chains where: (1) M2M transformations produce target models from UML models (stereotyped with the *CIP_VAM* profile), and (2) M2T transformations are used to perform queries on input models and provide the results on text files according to a specific format. At last, it is also necessary to provide the final user with the results obtained by solving the optimization and the vulnerability models: this requires that the results shall be further elaborated and used to update the UML models in order to be perceived at the presentation layer.

Here on, we call *forward transformation* a chain which requires, as input, a model expressed by means of the *CIP_VAM* profile and generates input files in the concrete syntax of the solver or of the optimization tool; we call *backward transformation* the chain of transformations and/or elaborations defined to update the UML model with the output of the analysis.

3.1 Forward Transformation Chains

In Fig. 10 the two main *forward transformation* chains defined within the METRIP approach are depicted, they are part of the Configuration Generator and the Model Generator components (Sect. 1).

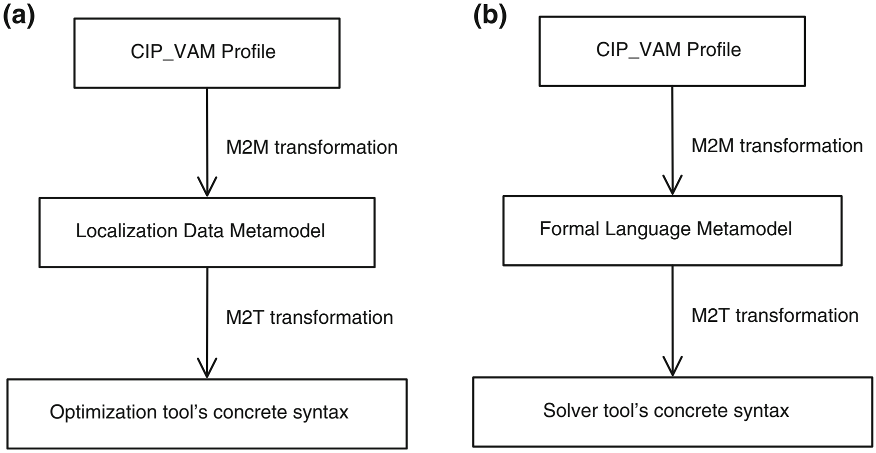

(a)
CIP_VAM Profile
M2M transformation
Localization Data Metamodel
M2T transformation
Optimization tool's concrete syntax
(b)
CIP_VAM Profile
M2M transformation
Formal Language Metamodel
M2T transformation
Solver tool's concrete syntax

Fig. 10 *Forward transformation* chains. **a** ODM transformation chain, **b** VA transformation chain

The *Optimization Data Model* (*ODM*) *transformation chain* (Fig. 10a) combines one M2M and one M2T transformation. Here it is customized to a subclass of optimization models, specifically the *localization models*, which provide the localization (and the number) of devices which fulfill the optimization objectives. The M2M transformation is defined from the *CIP_VAM* profile to an intermediate metamodel for data representation. It works by extracting the relevant data for the localization phase from the UML models and producing a model of them according to the target language. The M2T transformation is in charge of producing the input text file for the optimization tool from the intermediate data model.

The *Vulnerability Analysis* (*VA*) *transformation chain* (Fig. 10b) also combines one M2M and one M2T transformation. The M2M transformation is defined from the *CIP_VAM* profile to a metamodel describing the elements of a formalism for quantitative analysis modeling (such as Timed Petri Nets, Bayesian Networks, Fault Trees, etc.). It produces models expressed by the target formalism from UML models. The M2T transformation is in charge of producing the input textual file for the analysis tool to be used to solve the target model.

Implementation Hints We have used the Atlas Transformation Language (ATL)[1] to implement the M2M transformations. ATL is a model transformation language and toolkit developed on top of the Eclipse platform, which in turn is one of the most popular and free-for-use platform for building integrated development environments and tools. The M2T transformations are implemented in ATL, too. Hence, the metalanguage used to define the localization metamodel is Ecore. These implementation choices are in the direction of interoperability with the Eclipse Modeling Framework based tools and application[2] which are widely used within MDE.

[1] http://www.eclipse.org/atl/.

[2] http://projects.eclipse.org/projects/modeling.emf.

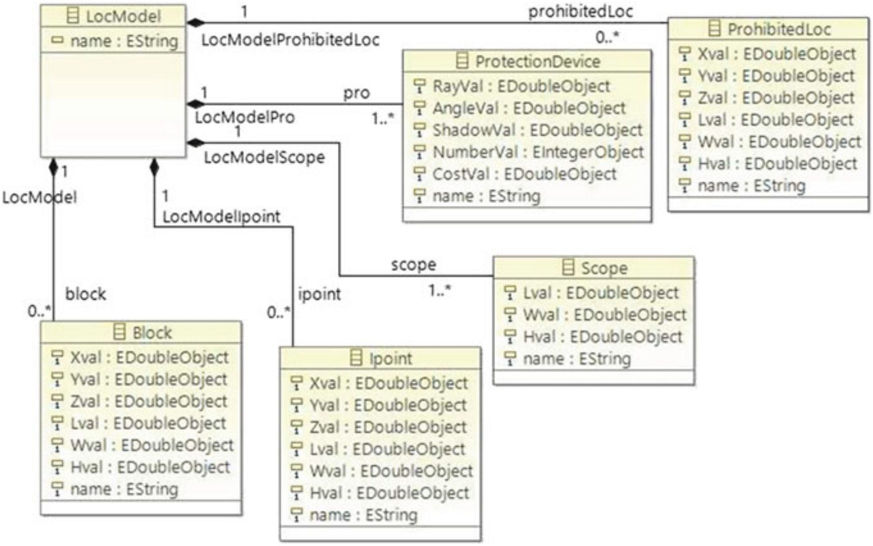


Fig. 11 ODM chain: localization data ecore metamodel

ODM transformation chain. Figure 11 shows the localization data metamodel which has been defined to provide the target language for data description. The localization metamodel has to contain all and only the information needed to instantiate the localization models for the optimization tool. Indeed, the M2M transformation of the ODM chain in Fig. 10a automatically generates the localization data model from the UML model. This M2M transformation is named *VAM2LD*.

Starting from Fig. 11, we highlight some relevant issues to be taken into account in defining *VAM2LD*:

- The class *Scope* represents the area that must be covered by means of protection devices. Hence, it may precisely correspond to one (or more) Site, Object or Interface which is also an asset, or it may be wider (if you want to protect an access by using intrusion sensors like magnetic contacts, you place them on the access point; but if you want to do video surveillance, and look at a door by a smart camera, you should not place it on the jamb of the door!). Its attributes include the scope dimensions (length, width and height).
- The class *Block* represents objects which are obstacles for the localization models. For example, pillars placed into a room area to be covered by means of cameras. Its attributes provide information about the spatial coordinates of blocks as well as their dimensions.
- The class *ProhibitedLoc* represents areas or points that **must be not** considered by the localization models, due to specific restrictions imposed by national and international laws, or by technological and other constraints. For example, this is

the case of privacy laws which limit the usage of cameras in presence of men at work. Its attributes are the same as the class *Block*.

- Opposite to the class *ProhibitedLoc*, the class *Ipoint* represents **mandatory points** for the localization models, i.e. points that must be protected, due to internal or external rules, or national and international laws; for example the interfaces that represent entrances to a Scope site (windows, doors, etc.) could be Points of Interest and consequently be covered by the localization models. Its attributes are the same as the classes *Block* and *ProhibitedLoc*.
- The class *Pro* represents a (kind of) protection device that has to be used by the localization models. Its attributes include the technical features and capabilities of the device, its cost, the maximum number of devices to be utilized, etc.

VA transformation chain. In Sect. 4 a vulnerability analysis is performed at the aim of evaluating the probability that a successful attack takes place against a railway station. We use a Bayesian Network model [10] and the JavaBayes tool[3] to compute this probability, hence in this case the M2M transformation in Fig. 10b has to generate the BN from the UML model. This M2M transformation is named *VAM2BN*. Of course a metamodel for the BN formalism is needed to represent the target language of the transformation, as in [11].

Each generated node of the Bayesian Network is a binary variable ({*true, false*}). The transformation takes into account the contributions of three UML submodels: *Infrastructure*, *Attack* and *Protection*.

First, for every <<*Action*>> in the *Attack* model, a BN node is generated: in this case, *true* means that the action occurs. The relationship of sequence between actions is translated into a parental dependence between BN nodes: thus, when a branch is found, a BN node has more than one child. The value of the *occurrenceProb* tagged value is used to build the Condition Probability Table (CPT) of the child nodes.

When a protection device is found in the *Protection* input model, some BN nodes are generated. The first is related to the activation of the device itself: *true* means that the device is on. Table 1 describes a typical CPT for these nodes where *A* is the availability of the sensor.

Then, when an action can be detected by a protection device, a new BN node is generated having as parents the nodes generated by the action and by the device: *true* means that the action is detected by the device. Table 2 describes a typical CPT for these nodes where *fnr* and *fpr* are the false negative and positive rates of the sensor respectively.

The *Infrastructure* model is used to establish the position of the objects and the location of the attack phases.

[3] http://www.cs.cmu.edu/javabayes/.

Table 1 CPT of the "device" variable

True	*False*
A	1 − A

Table 2 CPT of the "detection" variable

Action	Device	*Output = true*	*Output = false*
True	True	1 − fnr	fnr
True	False	0	1
False	True	fpr	1 − fpr
False	False	0	1

The BN model obtained by applying *VAM2BN* is the input of the subsequent M2T transformation which is in charge of translating the BN model into the specific format of the analysis tool.

3.2 Backward Transformation Chains

The *backward transformation* chains carry results obtained by solving the localization and/or the quantitative models back to the UML model or to a presentation layer.

Here below we describe one of the most meaningful *backward transformation* chain realized within the METRIP approach, the one which provides the user with a UML model of the infrastructure augmented with the localization of the protection devices (e.g., the cameras displacement which realizes the full coverage of a site/ asset). Hence, the effect of this transformation is to "integrate" an infrastructure model and a protection model. It consists of a chain of M2M transformations which work on UML models, starting from an initial elaboration of a file containing the localization results.

Figure 12 describes the *backward transformation*. It operates on three levels. From the bottom of the figure: (1) A first elaboration generates the data model of the localization solution from the results obtained by solving the localization model. (2) Two independent M2M transformations are defined: the intermediate M2M transformation in Fig. 12 (2a) generates as many protection device classes (from the *Protection* package) as specified by the localization results and instantiate them with the application points provided by the optimization tool; the intermediate M2M transformation in Fig. 12 (2b) is in charge of erasing from the initial UML model of the infrastructure some outdated information (about the kind of protections and the constraints to be considered in the localization phase). (3) Finally, a third M2M transformation integrates the UML models produced at level 2.

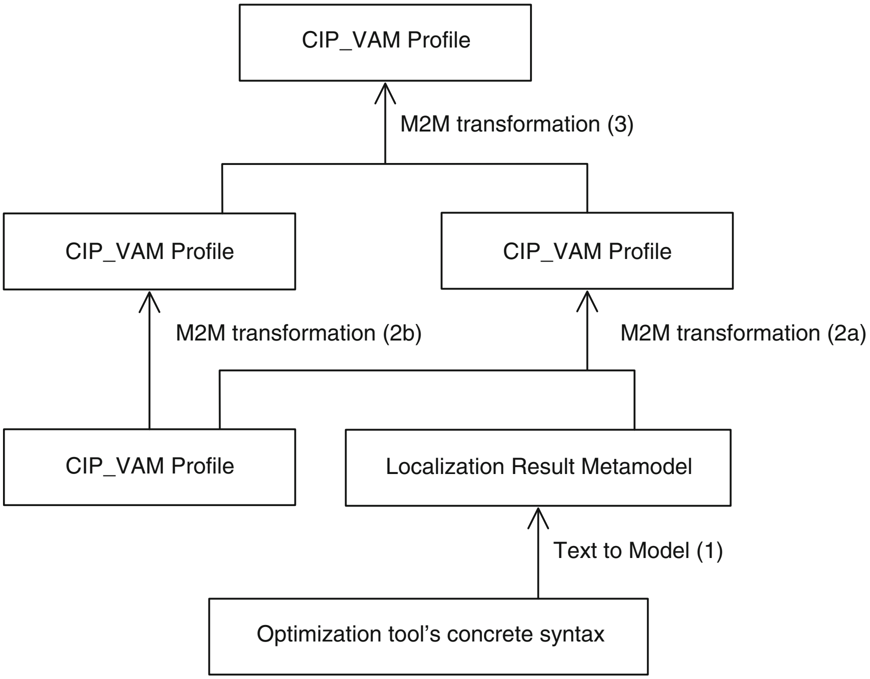


Fig. 12 ODM *backward transformation* chain

Notice that the M2M transformation at level (3) is a multi-input transformation, as well as the transformation (2a). In addition, both the transformation (2b) and the M2M transformation at level 3 are endogenous, i.e. they are transformations between models expressed in the same language (the *CIP_VAM* profile).

Implementation Hints Again, the M2M transformations have been implemented by using ATL and Ecore has been used as intermediate metalanguage.

Instead, the transformation from text (localization information) to the localization result model is implemented by a Java module. As for the VA *backward transformation* chain, it just reverses the VA *forward transformation* chain. Hence, we omit its description.

4 A Railway Station Case Study

In this Section we apply the presented approach to the protection of a real world railway station. Initially the station is assumed to be not equipped with any protection device and we want to provide the localization of proper closed-circuit cameras in order to protect it against some of the possible attacks. The station is built on three levels, trains arrive and depart from the first floor. The ground floor is freely accessible from a pedestrianized square through a main entrance and it

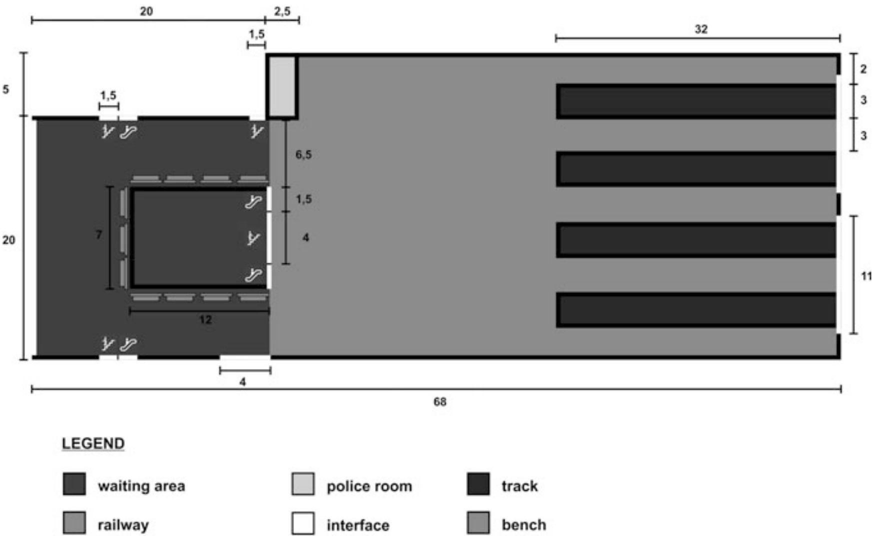


Fig. 13 Layout of the first floor

consists of a wide concourse that houses a ticket office and shops; to reach the upper floor there are staircases and escalators on the two sides. The access on the upper floor is enabled only by crossing turnstiles placed on the top of staircases and escalators. The portion of the station that shall be protected is the first floor, whose layout is visible in Fig. 13 (the dimensions are expressed in meters).

The first floor consists of two functional areas: the *waiting area* (on the left of the figure) and the *railway* (on the right of the figure). The waiting area is accessible from the two sides by four entrances (two staircases and two escalators); a terrace is also present on the extreme left of the waiting area. There are eleven benches for travelers awaiting. On the entrance of the waiting area the turnstiles enable the access of travelers; the waiting area has one exit toward other transportation lines and one exit toward a balcony on the street.

The railway has four tracks (where trains arrive in a direction and depart into the other); five platforms allow to get on/off the trains. The entire area is covered by a glass roof suspended by means of a grid of steel. Trains enter in and exit from the station through two portals which connect the first floor to a tunnel. The travelers can go downstairs and exit from the station through the central staircases (or central escalators). The overall floor is well-lighted by sun during day thanks to the glass roofing and the terrace.

In this case study we consider only bombing attacks: in detail we want to protect the first floor against bombing attacks that can be conducted by placing a bomb either in waiting area (precisely under the benches) or in the tunnel. With the aim to protect the station, two types of closed circuit cameras are considered (with a radius of 12 and 15 m respectively) and explosive detectors. We suppose that a maximum of 45 cameras and 2 explosive detectors maybe bought. Our scope is twofold:

- to localize a set of closed-circuit cameras covering the maximum area and minimizing the costs;
- to evaluate the effect on the vulnerability of the explosive detectors.

In the following, the complete modeling and vulnerability evaluation processes will be illustrated; the modeling process (including attacks and protection devices) applies the *CIP_VAM* profile (Sect. 2) to model the first floor of the station, the two attack scenarios and the two classes of cameras. Then, the *Optimization Data Model* (*ODM*) *transformation chain* described in Sect. 3 is executed in order to generate the input for the optimization module. The optimization module provides the localization of the cameras by solving an optimal covering Integer Linear Programming model, as explained in details in Chap. 6.

This Section ends quantifying the vulnerability of the first floor (with respect to the two considered attacks) with different configurations of the protection system.

4.1 Step 1: Modeling the Infrastructure

According to the *CIP_VAM* profile capabilities, we realized the UML model of the infrastructure to describe the physical layout of the station under analysis. The model of the infrastructure has been realized through a set of Class and Composite Structure Diagrams: UML elements of these two diagram have been extended by the *CIP_VAM* profile in order to annotate domain specific features. Figure 14 shows a first Class Diagram of the station: the three stairs of the station are modeled by the three classes (*GroundFloor*, *FirstFloor* and *Terrace*) stereotyped as *Site*. The other transportation lines have been generically modeled as a site (class *OtherLines*) since they are out of the scope of this work; the external environment has been also modeled by the class *Street*. The waiting area and railway have been modeled by the homonyms subclasses of the *FirstFloor* class (they will be detailed in Figs. 15 and 16). The

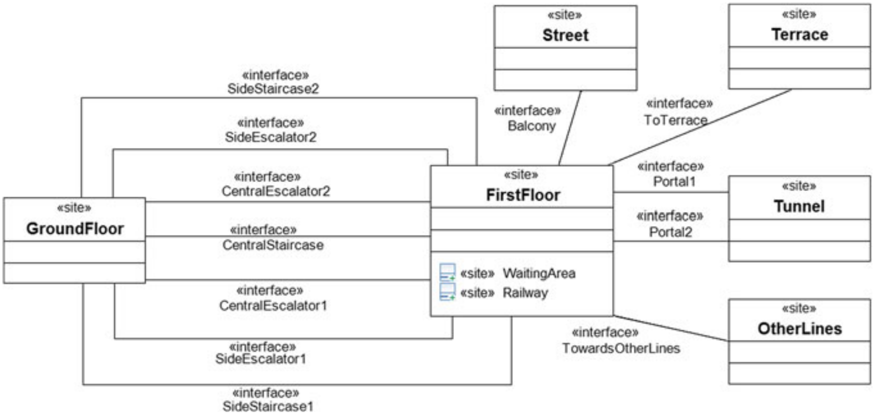

«site» Street
«site» Terrace
«interface» SideStaircase2
«interface» SideEscalator2
«interface» Balcony
«interface» ToTerrace
«interface» CentralEscalator2
«site» FirstFloor
«interface» Portal1
«site» Tunnel
«site» GroundFloor
«interface» CentralStaircase
«interface» Portal2
«site» WaitingArea
«site» Railway
«interface» CentralEscalator1
«site» OtherLines
«interface» TowardsOtherLines
«interface» SideEscalator1
«interface» SideStaircase1

Fig. 14 Class diagram of the station

associations stereotyped as *Interface* represent connections between sites: seven associations between the *GroundFloor* and the *FirstFloor* classes represent the three staircases and the four escalators; the *Balcony* association connects the *FirstFloor* with the *Street* while the *ToTerrace* association has been introduced between the *FirstFloor* and the *Terrace*. Also the two portals have been modeled by a UML association stereotyped as *Interface*, they connect the *FirstFloor* to the *Tunnel*.

Since the area we want to protect is the first floor, this class has been detailed by the Composite Structure Diagram reported in Fig. 15. It shows the structure of the first floor in terms of nested classes: the two aforementioned subsites have been modeled with two classes nested inside the *FirstFloor* class. The *WaitingArea* class, in turn, contains three other classes (*Bench1*, *Bench2* and *Bench3*) stereotyped as *Objects*, which represent the three set of benches present in the station. Similarly the *Railway* class has ten sub-classes which represent the police room, the platforms and the housing tracks. Each housing track, in turn, contains a track that has been modeled by a UML class stereotyped as *Object*.

The Class Diagram of the first floor reported in Fig. 16 highlights some of the tagged values related to *Railway*, *Platform5*, *HousingTrack4*, *RailwayEntrance1* and *Bench3*. The tagged values *shape* and *volume* allow to represent some geometrical features and they are associated with all the stereotypes showed in the Fig. 16; for example, *Railway* is rectangular (*type*=*rectangle*), 25 m long (*length*=(*value*=*25.0*, *unit*=*m*)), 48 m wide (*width*=(*value*=*48.0*, *unit*=*m*)) and 10 m high (*height*=(*value*=*10.0*, *unit*=*m*)). By means of the tag *exposures* we specify that *RailwayEntrance1* is a point of junction between the *Railway* and the *WaitingArea*.

4.2 Step 2: Modeling the Attacks

As said before, we consider a terrorist who wants to place a bomb either into the waiting area or inside the tunnel. The attack model is composed by two UML diagrams, a Use Case Diagram and an Activity Diagram. In particular, Fig. 17

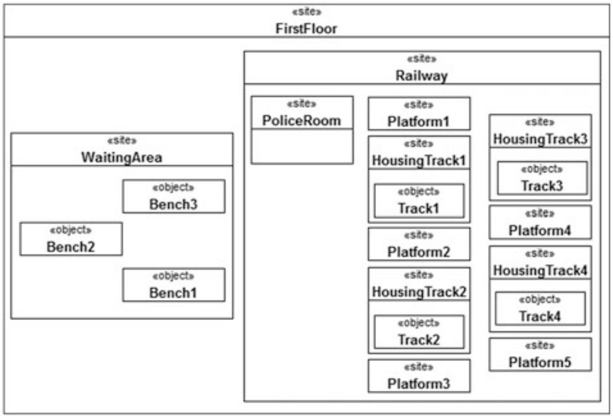


Fig. 15 Composite diagram of the first floor

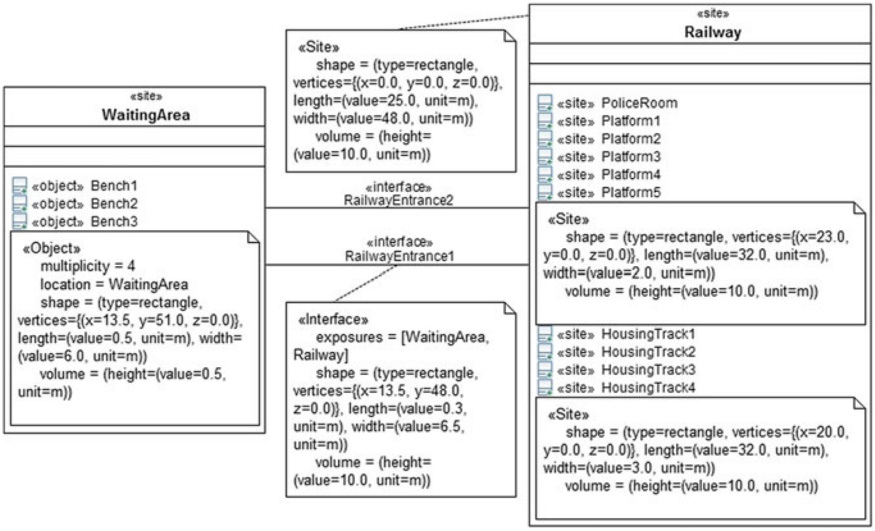

«site»
WaitingArea
«object» Bench1
«object» Bench2
«object» Bench3
«Object»
multiplicity = 4
location = WaitingArea
shape = (type=rectangle, vertices={(x=13.5, y=51.0, z=0.0)}, length=(value=0.5, unit=m), width=(value=6.0, unit=m))
volume = (height=(value=0.5, unit=m))
«Site»
shape = (type=rectangle, vertices={(x=0.0, y=0.0, z=0.0)}, length=(value=25.0, unit=m), width=(value=48.0, unit=m))
volume = (height=(value=10.0, unit=m))
«interface»
RailwayEntrance2
«interface»
RailwayEntrance1
«Interface»
exposures = [WaitingArea, Railway]
shape = (type=rectangle, vertices={(x=13.5, y=48.0, z=0.0)}, length=(value=0.3, unit=m), width=(value=6.5, unit=m))
volume = (height=(value=10.0, unit=m))
«site»
Railway
«site» PoliceRoom
«site» Platform1
«site» Platform2
«site» Platform3
«site» Platform4
«site» Platform5
«Site»
shape = (type=rectangle, vertices={(x=23.0, y=0.0, z=0.0)}, length=(value=32.0, unit=m), width=(value=2.0, unit=m))
volume = (height=(value=10.0, unit=m))
«site» HousingTrack1
«site» HousingTrack2
«site» HousingTrack3
«site» HousingTrack4
«Site»
shape = (type=rectangle, vertices={(x=20.0, y=0.0, z=0.0)}, length=(value=32.0, unit=m), width=(value=3.0, unit=m))
volume = (height=(value=10.0, unit=m))

Fig. 16 Class diagram of the first floor

shows two use cases (representing the attacks) stereotyped as *attack*, and the actor **Terrorist** stereotyped as *Attacker*. The tagged values associated with the *Terrorist* express that these attacks are conducted by a single terrorist exploiting medium skill and very high firmness. The tagged value *threat* (of the *place bomb in tunnel* use case) models the features of the threat while *tactic* specifies the kind of attack (bombing). Finally, the tagged value *duration* expresses that the estimated time needed to the terrorist from the moment he/she enters the station to the moment he/she places the bomb in the tunnel is 20 min.

Figure 18 shows the Activity Diagram which models one of the two attack scenarios: it illustrates the steps necessary to place a bomb in the waiting area. The attacker enters in the station at 8 a.m.: the UML activity *Enter in the station* is triggered by another activity (not showed in the figure) named *8_am*. After entering in the station she/he can choose to use one of the two escalators (other possibilities have been not modeled for sake of simplicity); the two choices has the same probability

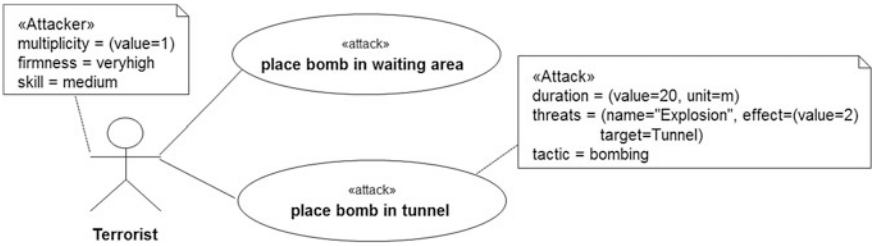


Fig. 17 Attack use case diagram

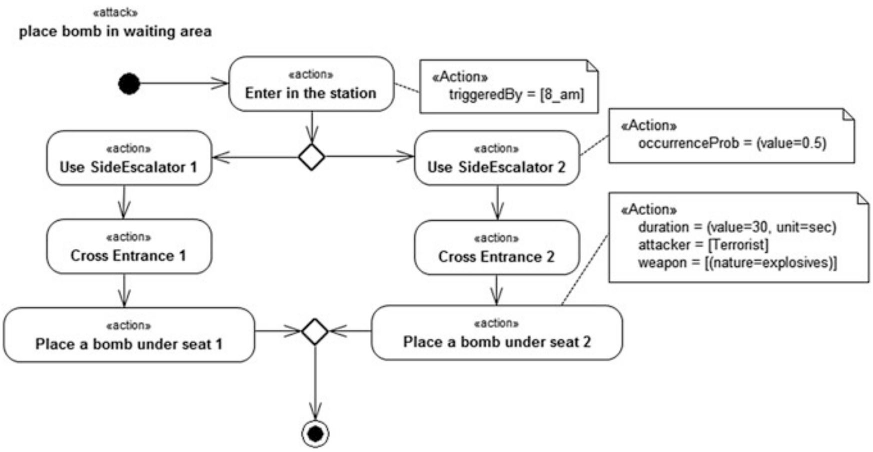


Fig. 18 Attack activity diagram

(the tagged value *occurenceProb* is equal to 0.5 for both the activities). There are two activities representing the crossing one of the two entrances: this level of detail is important since the two entrances could be protected by different devices. The two activities representing the action of placing the bomb close the Activity Diagram: this action has a *duration* of 30 s and is conducted using an explosive *weapon*.

4.3 Step 3: Modeling Possible Protections

As mentioned in the introduction of this Section, the considered protection system include closed-circuit cameras and explosive detectors. We have two different kinds of cameras where the differences are in their sensing radius and in their cost: the first kind of cameras has a radius of 12 m and it has a cost of \$100, the second kind of cameras has a radius of 15 m and a cost of \$150. The false positive rates and false negative rates are respectively 5 and 10 % for both kind of cameras. We also consider two explosive detectors: they both have a false positive rate and false negative rate equal to 1 %. This equipment has a cost of \$10,000.

The two kind of cameras are modeled by applying the *Protection* stereotype; the UML models are reported in Figs. 19 and 20, respectively. Each of them is modeled by a UML class stereotyped as *sensor*, where tags have been used to model their features.

The tagged value *protects*, used to express the site that need to be covered, is set to *FirstFloor* (the entire area); the tagged value *mandatory* expresses that all the interfaces (i.e., *SideStaircase1*, *SideEscalator1*, *Portal1*, *CentralStaircase*, etc.) of the first floor shall be necessary covered by at least one camera; the tagged value *forbidden* is used to say that the *PoliceRoom* shall absolutely not be covered by any cameras (according to privacy laws). Note that, for sake of space, since the two

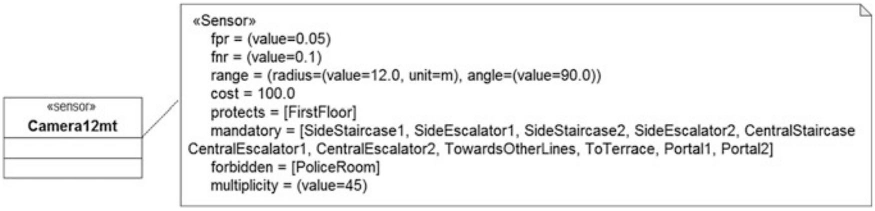

«sensor»
Camera12mt
«Sensor»
fpr = (value=0.05)
fnr = (value=0.1)
range = (radius=(value=12.0, unit=m), angle=(value=90.0))
cost = 100.0
protects = [FirstFloor]
mandatory = [SideStaircase1, SideEscalator1, SideStaircase2, SideEscalator2, CentralStaircase CentralEscalator1, CentralEscalator2, TowardsOtherLines, ToTerrace, Portal1, Portal2]
forbidden = [PoliceRoom]
multiplicity = (value=45)

Fig. 19 12-meters camera

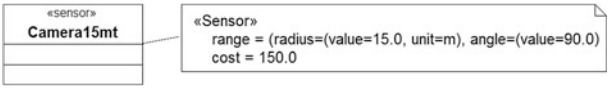


Fig. 20 UML diagram of the cameras: **a** radius = 12 m, **b** radius = 15 m

kinds of cameras are similar, in Fig. 20 only the tagged values that differ from those reported in Fig. 19 have been showed.

In the same way the explosive detectors have been modeled by a UML class stereotyped as *sensor*. In this case the tagged values *protects*, *mandatory* and *forbidden* have not been set since their localization is not required, they will be used to perform a what-if analysis. Again, the *fpr* and *fnr* tagged values are the false positive and false negative rates of the devices.

4.4 Step 4: Application of the ODM Transformation Chain

The localization of closed-circuit cameras and the update of the UML model are performed by applying the forward and backward transformation chains described in Sect. 3. Let us suppose that a what-if analysis should be made to individuate the optimal localization of cameras at the lower cost choosing among the usage of: (i) 12-meters cameras, (ii) 15-meters cameras, or (iii) a mix of both. Hence, the same model has been instantiated three times. The three instances differ in the information about the protection devices: the first two instances model the cases where just one kind of camera is used (Figs. 19 and 20); the third instance models the case where a mix of them is required.

The application of the *forward transformation* chain produces three different files representing the scope of the localization, blocks, points of interest, prohibited localizations and features of protection devices. Here below the XML file is reported containing the Localization Data model obtained by applying the forward transformation chain to the first instance of the model (12-meters cameras). The *scope* field represents the entire area under protection (it is 25.0 m wide, 68.0 m long and 10.0 m high). *ProtectionDevice* represents the features of interest of the cameras: the view ray, the view angle, and the cost that are translated into properties of this field as well as the *maximum* number of cameras to be considered. Note that the *name* property (only for protection devices) reports the XMI identifier of the source UML class representing the camera: this is necessary to identify this object in the backward transformation chain. *ProhibitedLoc* field represent vertexes and measures of the Police Room: its bottom-left vertex is located at coordinates (20.0, 45.0, 0.0) and this room is 5.0 m wide, 2.5 m long and 10.0 m high. In the same way interest points and blocks have been represented in the reported XML file.

```
<scope Lval="25.0" Wval="68.0" Hval="10.0" name="FirstFloor"/>
<protectionDevice RayVal="12.0" AngleVal="90.0" ShadowVal="0.0"
              NumberVal="45" CostVal="100.0" name="_YWj6IPtjEeKi1Y5N6oEoAw"/>
<prohibitedLoc Xval="20.0" Yval="45.5" Zval="0.0" Lval="5.0"
              Wval="2.5" Hval="10.0" name="PoliceRoom"/>
<ipoint Xval="0.0" Yval="59.5" Zval="0.0" Lval="0.3"
              Wval="1.5" Hval="10.0" name="SideStaircase1"/>
<ipoint Xval="0.0" Yval="61.0" Zval="0.0" Lval="0.3"
              Wval="1.5" Hval="10.0" name="SideEscalator1"/>
<ipoint Xval="20.0" Yval="59.5" Zval="0.0" Lval="0.3"
              Wval="1.5" Hval="10.0" name="SideStaircase2"/>
<ipoint Xval="20.0" Yval="61.0" Zval="0.0" Lval="0.3"
              Wval="1.5" Hval="10.0" name="SideEscalator2"/>
<ipoint Xval="0.0" Yval="48.0" Zval="0.0" Lval="0.3"
              Wval="4.0" Hval="10.0" name="TowardsOtherLines"/>
<ipoint Xval="20.0" Yval="48.0" Zval="0.0" Lval="0.3"
              Wval="1.5" Hval="10.0" name="ToTerrace"/>
<ipoint Xval="6.5" Yval="48.0" Zval="0.0" Lval="1.5"
              Wval="0.3" Hval="10.0" name="CentralEscalator1"/>
<ipoint Xval="8.0" Yval="48.0" Zval="0.0" Lval="4.0"
              Wval="0.3" Hval="10.0" name="CentralStaircase"/>
<ipoint Xval="12.0" Yval="48.0" Zval="0.0" Lval="1.5"
              Wval="0.3" Hval="10.0" name="CentralEscalator2"/>
<ipoint Xval="1.0" Yval="0.0" Zval="0.0" Lval="11.0"
              Wval="0.3" Hval="10.0" name="Portal1"/>
<ipoint Xval="13.0" Yval="0.0" Zval="0.0" Lval="11.0"
              Wval="0.3" Hval="10.0" name="Portal2"/>
<block Xval="6.0" Yval="51.0" Zval="0.0" Lval="0.5"
              Wval="6.0" Hval="0.5" name="Bench1"/>
<block Xval="7.75" Yval="60.0" Zval="0.0" Lval="4.5"
              Wval="0.5" Hval="0.5" name="Bench2"/>
<block Xval="13.5" Yval="51.0" Zval="0.0" Lval="0.5"
              Wval="6.0" Hval="0.5" name="Bench3"/>
<block Xval="2.0" Yval="0.0" Zval="0.0" Lval="31.0"
              Wval="3.0" Hval="0.5" name="Track1"/>
<block Xval="8.0" Yval="0.0" Zval="0.0" Lval="31.0"
              Wval="3.0" Hval="0.5" name="Track2"/>
<block Xval="14.0" Yval="0.0" Zval="0.0" Lval="31.0"
              Wval="3.0" Hval="0.5" name="Track3"/>
<block Xval="20.0" Yval="0.0" Zval="0.0" Lval="31.0"
              Wval="3.0" Hval="0.5" name="Track4"/>
```

The XML files obtained by applying the *forward transformation* chain to the other two model instances are omitted, since the only difference is in the values related to the view ray and the cost of the camera.

The application of the described Model-to-Text transformations generate input files for the optimization module. The results obtained provide the localization of the cameras on the first floor of the station according to the optimization objectives. These results are described in Chap. 6, where the reported results say that the best solution is to adopt a mixed coverage as it minimizes the total cost. The localization provides the coordinates of the application points which are used to update the UML model by executing the *backward transformation* chain.

4.5 Step 5: Vulnerability Analysis

In this Section we consider different PPSs based on the infrastructure described above in order to evaluate how the vulnerability of the system changes when the configuration of the PPS varies. The first solution just uses smart 12-meters cameras, an alternative solution adds explosive detectors that are applied on the two side entrances to the waiting area.

Figure 21 shows a possible localization of 12-meters cameras. Notice that the Police Room is not covered by the close-circuit cameras (as expected from requirements).

Considering the attacks partially showed in Figs. 17 and 18, the following scenarios are possible:

- S1: bombing attack in the waiting area where only closed-circuit cameras are installed, in this case the action of placing a bomb under a bench is seen by two cameras (as this area is covered by two cameras according to the localization schema in Fig. 21).
- S2: bombing attack in the waiting area, the explosive detectors are added, hence when the attacker tries to enter in the waiting area the explosive can be detected by these devices.

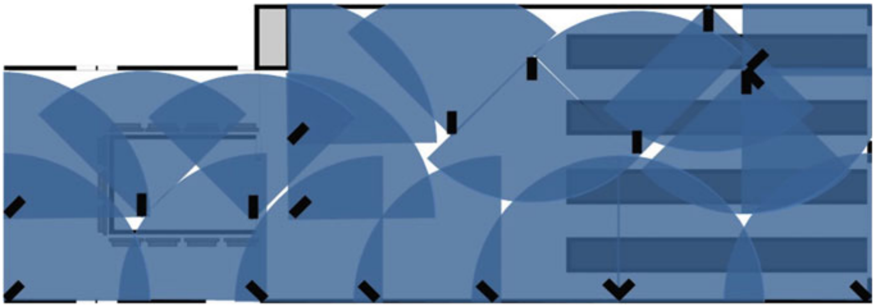


Fig. 21 A possible localization by 12-meters cameras

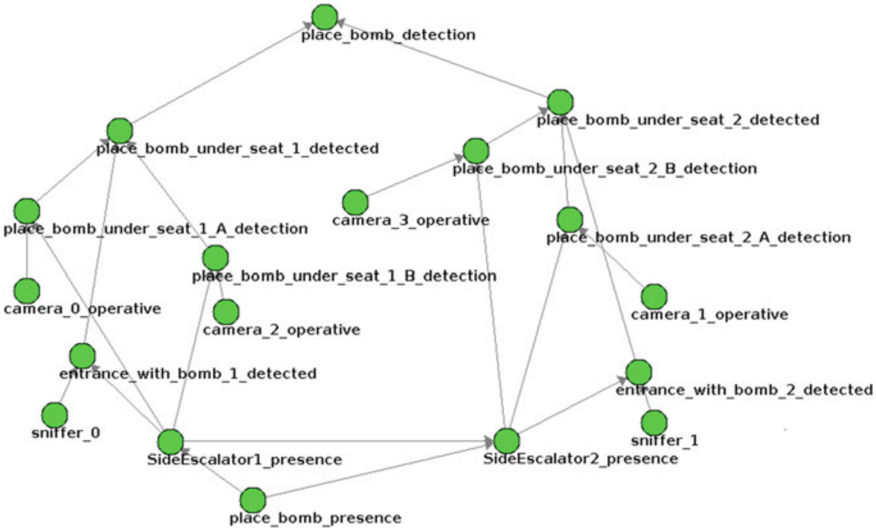

place_bomb_detection
place_bomb_under_seat_2_detected
place_bomb_under_seat_1_detected
place_bomb_under_seat_2_B_detection
camera_3_operative
place_bomb_under_seat_1_A_detection
place_bomb_under_seat_2_A_detection
place_bomb_under_seat_1_B_detection
camera_0_operative
camera_1_operative
camera_2_operative
entrance_with_bomb_1_detected
entrance_with_bomb_2_detected
sniffer_0
sniffer_1
SideEscalator1_presence
SideEscalator2_presence
place_bomb_presence

Fig. 22 The Bayesian network of the S2 scenario

- S3: bombing attack in the tunnel, the attacker enters the tunnel from the end of the platform; in this scenario only one smart camera sees the attacker (the one that is looking to the portal according to the localization schema in Fig. 21).
- S4: bombing attack in the tunnel carried out in presence of the explosive detectors on the entrances.

Starting from the considerations made in Sect. 3, a BN model is generated for each scenario by applying the VA transformation chain. The BN generated for S2 is depicted in Fig. 22.

Each node of the Bayesian Network is characterized by two states: *true* and *false*. The attack starting event is represented by the *place bomb presence* variable that is the parent of two variables: *SideEscalator1 presence* and *SideEscalator2 presence* meaning the possible paths that an attacker can choose in order to reach the waiting area. The choice between the two paths is non-deterministic, but a path depends on the other in order to prevent the possibility of simultaneous attacks (that has not been modeled). Then two identical branches start, consisting of three pairs of nodes. Starting from *SideEscalator1 presence* branch, the three pairs are:

1. (*entrance_with_bomb_1_detected*, *sniffer _0*)
2. (*place_bomb_under_seat_1_A_detection*, *camera_0_operative*)
3. (*place_bomb_under_seat_1_B_detection*, *camera_2_operative*)

Each pair represents the pattern of detection of the attack step by a sensor; in particular let us focus on the first pair: *sniffer_0* is the binary variable representing the probability that the sensor device is available. Its Conditional Probability Table (CPT) is as the one in Table 1. The variable *entrance_with_bomb_1_detected*

Table 3 Analysis results

S1 (%)	S2 (%)	S3 (%)	S4 (%)
3.5	0.067	19	0.36

represents the probability of detection of the action, whose CPT is as the one in Table 2. The other pairs are structured according to the same "pattern". The three variables:

- *entrance_with_bomb_1_detected*
- *place_bomb_under_seat_1_A_detection*
- *place_bomb_under_seat_1_B_detection*

are inputs of *place_bomb_under_seat_1_detection*, representing the fact that the attacker has been detected by at least by one of the three sensors. In order to model this policy a simple OR-logic is implemented by the CPT of the *place_bomb_under_seat_1_detection* node.

The vulnerability of the system has been evaluated for each scenario. The results of such analyses are summarized in Table 3. These results say that adding an explosive detector in case of an attack in the waiting area can increase the protection of the system but that this improvement is more important in case of attack in tunnel (since the vulnerability moves from 19 % to less than 1 %).

5 Related Work

An important contribution to the field of PPS design and vulnerability evaluation was made by Mary Linn Garcia [12, 13]. According to Garcia, the PPS evaluation process encompasses three main phases: (1) identification of PPS objectives, (2) PPS design, and (3) analysis/evaluation of the PPS design which may require one to come back at the previous phase in order to refine/correct the system design. In [12] it is clearly stated that 'the protection objectives must be known before evaluating the facility' even if this point in the current practice is not always considered to be part of vulnerability assessment. This means one must identify the *threats*, estimate the likelihood of *attacks*, define the *assets* to protect, and subsequently build a threat/asset matrix. The process presented in this paper moves from the Garcia's work, trying to take advantages by the integration of the available information about these main aspects and the features of the protection devices. Indeed, one of the original contribution of the METRIP approach was to correlate infrastructures and vulnerabilities with the appropriate protection strategies in order to best defend the asset(s). In order to automate the design and evaluation process we adopted a Model Driven Engineering approach based on UML profiling which well suits the objective of providing the user with interoperable toolchains. At best of our knowledge, few works focus on the design and development of UML profiles for modeling CI vulnerability and protection. In [14] the UML-CI profile is introduced; it is a UML profile aimed at defining different aspects of an infrastructure organization and behavior. The CORAS method[4] is oriented to Model Driven risk analysis of changing systems [15], the CORAS language (now an OMG profile for QoS and Fault Tolerance characteristics and mechanisms specification) is used in order to support the analysis of security threat and risk scenarios in security risk analyses. UMLsec allows for expressing security information in system specification [16], the UML Profile for Modeling and Analysis of Real-Time and Embedded systems (MARTE) [7] is an OMG-standard profile that customizes UML for the modeling and analysis of Non-Functional Properties (NFP) of real time embedded systems and the Dependability Analysis and Modeling (DAM) [17] profile is a specialization of MARTE which enables dependability analysis. One of the most critical issues in the application of transformational processes to critical systems is the correctness assessment of the M2M transformations themselves. Different approaches have been proposed in scientific literature spanning from testing [18] to formal verification [19] but the problem still remains an open issue. This work does not focus on the verification of the transformations: the transformations here introduced have been tested on several significant cases.

6 Conclusions

In this paper a Model Driven process supporting the PPS design and the quantitative evaluation of assets' vulnerability has been described. The definition of the process is driven by a two-fold objective: (1) the automatic generation of quantitative vulnerability models for RIS, and (2) the automatic gathering of information to be provided to proper localization and optimization tools from an high level specification of the system under protection. The proposed process was developed within the METRIP project and it is based on a modeling approach which describes and combines three main aspects involved in the effective design of a PPS: *attacks*, *assets* and *protection technologies and devices*. Hence, the vulnerability evaluation may be performed taking into account the characteristics of the assets, the attack scenarios, and the type and disposition of the protection devices. To this aim, our approach extends the Unified Modeling Language (UML) by applying profiling techniques in order to capture vulnerability and protection modeling issues, and uses proper Model-to-Model transformations to generate formal analysis models and proper data model from UML artifacts. In the paper the resulting *CIP_VAM* profile is described, as well as the transformational approach. The whole process is then applied to a real world scenario, i.e. the protection and the vulnerability analysis of a railway station, in order to demonstrate that the METRIP model-driven process may provide the PPS designer with a practical engineering mean to quickly evaluate different design choices and the vulnerability of RIS assets against concrete attack scenarios.

[4] http://coras.sourceforge.net/index.html.

References

1. Selic B (2012) The less well known UML: a short user guide. In: Proceedings of the 12th international conference on formal methods for the design of computer, communication, and software systems: formal methods for model-driven engineering, SFM'12. Springer-Verlag, Berlin, Heidelberg, pp 1–20
2. Volter M (2011) From programming to modeling—and back again. IEEE Softw 28(6):20–25
3. Selic B (2007) A systematic approach to domain-specific language design using UML. In: 10th IEEE international symposium on object and component-oriented real-time distributed computing (ISORC'07), pp 2–9
4. National Consortium for the Study of Terrorism and Responses to Terrorism (START) (2012) RAND NDSI project: database of worldwide terrorist incidents. http://smapp.rand.org/rwtid/searchform.php
5. METRIP project. *RIS Terrorist Attack Database (RISTAD)*. Available: http://metrip.unicampus.it/index.php/ristad
6. Marrone S, Nardone R, Tedesco A, D'Amore P, Vittorini V, Setola R, De Cillis F, Mazzocca N (2013) Vulnerability analysis and modeling for critical infrastructure protection. In: Seventh annual IFIP working group 11.10 international conference on critical infrastructure protection, 18–20 March 2013
7. OMG (2011) UML profile for MARTE: modeling and analysis of real-time embedded systems, June 2011. Version 1.1, formal/11-06-02
8. Czarnecki K, Helsen S (2006) Feature-based survey of model transformation approaches. IBM Syst J 45(3):621–645
9. Schmidt DC (2006) Model-driven engineering. IEEE Comput 39(2):25–31
10. Charniak E (2012) Bayesian networks without tears: making Bayesian networks more accessible to the probabilistically unsophisticated. In: American Association for artificial intelligence, vol 4, pp 50–63, Maj 2012
11. del Aguila IM, del Sagrado J (2012) Metamodeling of bayesian networks for decision-support systems development. In: Proceedings of 8th workshop on knowledge engineering and software engineering (KESE8), August 2012
12. Garcia ML (2005) Vulnerability assessment of physical protection systems. Butterworth-Heinemann, Boston
13. Garcia ML (2007) Design and evaluation of physical protection systems. Butterworth-Heinemann, Boston
14. Bagheri E, Ghorbani AA (2010) UML-CI: A reference model for profiling critical infrastructure systems. Inf Syst Front 12(2):115–139
15. Lund MS, Solhaug B, Stølen K (2011) Risk analysis of changing and evolving systems using CORAS. In: Foundations of security analysis and design vi. Springer-Verlag, Berlin, Heidelberg, pp 231–274
16. Jürjens J (2005) Secure systems development with UML. Springer, New York
17. Bernardi S, Merseguer J, Petriu DC (2011) A dependability profile within MARTE. Soft Syst Model 10(3):313–336
18. Fleurey F, Steel J, Baudry B (2004) Validation in model-driven engineering: testing model transformations. In: Proceedings of first international workshop on model, design and validation, 2004, pp 29–40
19. Asztalos M, Lengyel L, Levendovszky T (2010) Towards automated, formal verification of model transformations. In: 2010 third international conference on software testing, verification and validation (ICST), pp 15–24

Optimal Location of Security Devices

Antonio Sforza, Stefano Starita and Claudio Sterle

Abstract The design of a security system, in terms of number and position of the security devices composing it, is one of the main issue tackled in METRIP project (MEthodological Tool for Railway Infrastructure Protection). It is a complex problem where a very large set of configurations has to be explored in order to determine the most efficient one, which guarantees the highest protection level. Indeed a good placement of the devices has to satisfy two main targets. On one side it has to guarantee the highest security level, i.e. it has to be able to control the widest achievable area. On the other side, it has to be economically sustainable, i.e. it has to be realized with acceptable costs. In literature this problem is generally referred to as sensor placement problem, widely treated by integer linear programming models and combinatorial optimization methods. In this chapter we will present the main covering models present in literature and adopted in METRIP project for the placement of devices preventing the malicious intrusions in railway assets, with particular reference to the intrusions in a railway station. The applicability of these models will be proved using two test cases which represent two typical railway asset schemes.

Keywords Security system design · Covering problem · Coverage and visibility analysis · Device location · Directional sensor placement

A. Sforza (✉) · C. Sterle (✉)
Department of Electrical Engineering and Information Technology, University "Federico II"
of Naples, Via Claudio, 80125 Naples, Italy
e-mail: Sforza@unina.it

C. Sterle
e-mail: claudio.sterle@unina.it

S. Starita
KBS, Kent Business School, University of Kent, Canterbury, UK
e-mail: ss882@kent.ac.uk

R. Setola et al. (eds.), *Railway Infrastructure Security*, Topics in Safety,
Risk, Reliability and Quality 27, DOI 10.1007/978-3-319-04426-2_9

1 Introduction

The great amount of incidents occurred worldwide shows that terrorists seek targets that have emotional or symbolic value, such as widely recognizable icons and targets whose destruction would significantly damage or disrupt an economy. The economic impact of such attacks is indirect [1, 2]. Data provided by Mineta Transportation Institute's National Transportation Security Center (MTI/NTSC) show as from 1970 to 2011, 2.927 attacks against public transportation systems were committed. About 48 % were carried out on buses, while the 43 % were perpetrated against railway infrastructure systems (in the following referred to as RIS). Even though attacks against buses are more frequent, RIS attacks are in general more lethal, as witnessed by the attacks in Madrid 2004, in London 2005 and in Mumbai 2008.

Hence it is clear that a RIS has a great appeal on assailants, especially in urban areas, because of its intrinsic value, vulnerability and difficulties in guaranteeing its protection, due to its nature, which precludes the passengers' screening and identification, and to its specific features [3]:

- open infrastructure;
- high levels of passenger density;
- hazardous materials on the lines;
- extent of the infrastructures inside the city;
- economic and social relevance of the railway transportation system.

For all these reasons prevention and preparedness to risks in RIS requires: proper analysis of the vulnerabilities of the system; clear awareness of criticalities and possible countermeasures; adequate methods to design, scale and optimize the protection.

METRIP (Methodological Tools for Railway Infrastructure Protection) is an European Project focalized on these challenging aims. The general objective of the project is the development of a methodological tool aimed at increasing the protection of a RIS asset, by the following process [4]:

- identifying the most critical and vulnerable assets;
- defining the attack scenarios to be detected for each asset;
- designing the security system in terms of type, number and position of the protection devices;
- evaluating the effectiveness of the security system in terms of asset vulnerability to an attack.

The tool is composed by three interacting modules briefly described in Sect. 4, with particular reference to the Optimization Module (*OM*), devoted to determine the optimal location of the protection devices composing the security system. This problem is referred in literature to as the sensor placement problem and in this chapter we will survey some covering optimization models which can be used for its solution to design the security system of a RIS asset. We will also give hints explaining how these models can be used to achieve also some specific monitoring tasks.

This chapter is structured as follows. Section 2 provides a brief description of some protection devices which can be employed in a RIS security system. Section 3 is devoted to the sensor placement problem. Section 4 is focused on the Optimization Module of METRIP tool and on the models used in it for the optimal placement of the security devices. Results obtained by presented models on two sample test cases are shown in Sect. 5. Section 6 is devoted to conclusions.

2 Protection Devices for a RIS

A huge number of protection devices can be employed in a RIS security system, some of them, specifically devoted to the detection of particular attacks, as for example Chemical, Biological, Radiological, Nuclear and Explosive (CBRNe) attacks, are installed just on request. On the other side a *Baseline Security System* (BSS) is usually installed for the protection of an asset, not only a RIS asset, with the aim of preventing malicious intrusions. The BSS system is composed by three main classes of protection devices opportunely integrated:

- *Video Surveillance Devices*: fixed perspective cameras (directional cameras); PTZ (Pan-Tilt-Zoom) cameras; omnidirectional cameras; high resolution cameras (particularly suitable for cameras equipped with video-analysis tool).
- *Access Control Devices*: triple technology volumetric sensors; magnetic contacts; proximity readers; access control systems (ACS2/ACS8); infrared barriers.
- *Audio Surveillance Devices*: microphones; sound cards; sound analyzer server.

The placement of some devices, such as for example magnetic contacts, access control systems or sound cards is determined by their specific usage, whereas the placement of other devices, such as cameras, volumetric sensors and microphones, has to be strategically performed. Indeed many types of these devices, differing in performances and costs, are available. Moreover, generally, the higher is the security level guaranteed by a device, the higher is its cost. Hence a good and strategic placement of these devices has to efficiently solve the trade-off between the achievement of higher security levels and the minimization of the costs. Moreover, for some of these devices, in particular for cameras, several constraints have to be taken into account when specific security tasks have to be achieved. For intrusion detection, the complete coverage of the asset is required; a reliable security system, or a system aimed at performing the tracking of objects/people moving in an area, requires that points of the asset have to be covered by more than one camera; the usage of video-analysis algorithms, as face recognition algorithms or, specifically for RIS, yellow line crossing algorithms, requires that cameras have to be opportunely positioned, with respect to the object, in order to guarantee a good quality of the image.

3 State of the Art of the Sensor Placement Problem

Location problems consist in determining the best locations of one or more facilities/devices on the basis of a predefined performance criteria and operational constraints. More precisely given the distribution of a good/service demand, the aim is to determine the location of a set of facilities/devices, minimizing location and service costs (generally related to distance or time parameter). These problems have been widely approached by mixed integer linear programming models and optimization methods. In [5] they are classified in three main groups: p-median models [6, 7], p-center models [6, 8] and covering models [9]. The third group concerns location problems which consists in the placement of a set of facilities, in points of a region of interest, with the aim of satisfying a real or virtual service demand. A point can be covered by a facility just in case the adopted covering criteria is met [9, 10]. A complete review of the main works on covering problems is out of the scope of this chapter, but a good review of the most recent contribution can be found in [11, 12].

The optimal location of protection devices, as said above, is referred to in literature as the sensor placement problem. This problem has been widely treated in literature as a set covering problem, where the facilities to be located are the security devices and the satisfaction of the demand corresponds to the coverage of the set of points schematizing the region of interest to be controlled.

The first attempts to tackle the problem consider it as a variant of the art gallery problem (*AGP*), introduced in [13]. This problem is widely explored in [14] and a review of the most recent advances in the field can be found in [15]. The *AGP* problem consists in opportunely distributing the minimum number of guards in an area such that all its points are observed. In the *AGP* the guards are assumed to have an unlimited omnidirectional monitoring capacity, i.e. they can cover a 360° angle with no distance constraints. These assumptions are too strong and unrealistic for the security devices under investigation, since they are generally directional devices with very different performances and costs. For this reason the sensor placement problem is also referred to as the directional sensor placement problem. The interested reader is addressed to the work by [16] for a complete survey on coverage models and methods for directional sensor placement problem.

In the following we will just summarize the main recent contributions where new issues of the problem are examined and solved. In [17] the authors tackle and solve by integer linear programming models the problem of placing omnidirectional devices, differing for coverage ranges and costs, in a region schematized by a grid of point. They also treat the problem of determining the device placement where each grid point is covered by a unique subset of sensors. This work is extended in [18] where the device detection probability is introduced. Indeed the authors assume that the detection probability of a target decreases exponentially with the distance between the sensor and the target. Hence they solve the problem of locating the minimum number of devices which guarantee that every grid point is covered with a minimum confidence level. In [19] real operational constraints and capabilities of the devices are taken into account for the first time. It tackles the problem of determining the optimal positioning and the number of cameras in a region, given a set of task-specific constraints and a set of possible cameras to use in the layout. It considers very realistic regions, i.e. volumes with holes and static or dynamic objects within it. Then it focuses on planar regions and solve the camera layout problem with certain task-specific constraints by binary optimization over a discrete problem space. In [20] the authors, starting from the idea proposed in [17], tackle the problem of locating directional sensors (i.e. cameras which do not possess circular sensing ranges) with the aim of coverage maximization and the achievement of the coverage at a certain resolution. In [21] the problem is treated with reference to a 3D region in an urban environment. The visibility analysis is tackled by a GIS-based approach and the problem is solved by integer linear programming models. The problem of locating directional sensor in a region of interest characterized by the presence of blocks is treated in [22]. This work, moreover, proposes an original integer linear programming model where the points of the region to be controlled are opportunely weighted in function of their importance. The orientation of directional sensors within a 2D plane is explicitly taken into account in [23]. In [24] a new method for determining the best placement for large numbers of cameras within arbitrary building layouts is described. The method takes as input a 3D model of the building, and uses a genetic algorithm to find a placement that optimizes coverage and overlapping between cameras. The positioning error bounds are taken into account in [25], within an integrated maximal covering and backup covering problem solved by a simulated annealing based approach. The error bound concept is also considered in [26] together with aspects related to lack of knowledge regarding the target to control.

4 The Optimization Module

The decisional process developed by the METRIP tool, briefly introduced in Sect. 1, is performed by three main interacting modules:

- **Unified Modeling Language Module (UMLM)**, devoted to develop the UML models of the:
  - RIS assets (geometry, physical structure and main components);
  - attacks against RIS (effects, used mean, main steps of the attack);
  - protection devices (technological features and cost of each device).
- **Optimization Module (OM)**, devoted to find the optimal location of the security system devices within the asset through integer linear programming (ILP) covering models solved by the optimization software Xpress-MP. The location of the devices is optimized with respect to the covered space of the asset and takes into account its specific geometry.

- **Vulnerability Analysis Module (VAM)**, devoted to the vulnerability evaluation of the asset in relation to the kind of attacks and protection devices.

In this chapter we will focus on the Optimization Module (*OM*) and on the mathematical models implemented in it for the optimal location of the protection devices. The *OM* is devoted to manage a library of optimal covering ILP models used in the design of the security system. These models determine the number and the location of most of the control devices which constitute the *BSS*. The *OM* performs the following main activities:

- Asset discretization.
- Coverage analysis.
- Coverage model selection.
- Solution of the model by the Xpress optimization software and generation of the output for the *UMLM*.

In the following sub-sections we will explain in detail the first three phases. In the next section we will present the results obtained solving the model by the Xpress optimization software.

4.1 Asset Discretization

Given the information about the asset geometry (shape, width and length) provided by the *UMLM*, the area of the asset to be protected, referred to as region of interest, has to be made discrete, i.e. we have to pass from the continuous two-dimensional representation to a discrete representation of the region [21, 22]. This operation is performed building a grid with step size k on the plant of the asset to be controlled. The set of points of the grid is referred to as R and we have to cover/protect these points. Obviously the smaller is the step size of the grid, the higher is the cardinality of R and consequently more detailed is the schematization of the area.

In this phase we define also the set of points where the devices could be placed, referred to as L. Generally L is constituted by the points sited on the edges and corners of the asset walls and of the obstacles present in the region of interest.

In some cases these points have to respect particular conditions. For example, if video-analysis algorithms have to be used, possible location points are the ones which have to be used in order to allow that the algorithms effectively work. In particular if we have to locate cameras equipped with video-analysis algorithms for the control of the yellow line crossing, then the camera has to be installed perfectly aligned with the yellow line. This means that the only possible points for placing these cameras are the ones along the yellow line. Similar considerations could be done for the face recognition algorithm equipped cameras, which, to be effective, require to be placed almost orthogonally with respect to the target.

4.2 Coverage Analysis

The activity of a BSS device can be schematized through a ***coverage area***, i.e. the portion of area that can be controlled by it. It is defined by two parameters:

- θ, *coverage angle*, expressed in degrees (0° ÷ 360°), within which the device is active;
- r, *coverage ray*, maximum distance (expressed in metres) to which the device is still effective.

For example, the area covered by a microphone is a "circle" with a coverage angle $\theta = 360^\circ$, and a certain coverage ray r. Instead the area covered by a camera for a Closed Circuit Television (CCTV) is a "circle sector" with $\theta < 360^\circ$ and ray r.

The coverage area of a security device having a coverage angle lower than 360°, as for example a CCTV, is defined by its orientation. For sake of clarity, let us suppose to have a CCTV camera with a 90° coverage angle. Given a potential location, the camera can be installed with 4 different orientations which cover 4 different circle sectors, e.g. 0°–90°, 90°–180°, 180°–270, 270°–360°. This means that in a certain point of the set L we can locate a single device with a certain orientation, or more devices with different orientations. To enlarge the space of the locations, the orientations taken into account for this camera could generate a certain overlapping of the coverage areas. If, for example, the overlap is equal to 45°, we can generate 8 orientations and so 8 different circle sectors: 0°–90°, 45°–135°, 90°–180°, 135°–225°, 180°–270, 225°–315°, 270°–360°, 315°–45°. To enumerate all the possible orientations for a device located in a point of set L we can define a step δ, δ ∈ [0° ÷ θ]. For each potential location a device can be located using $n = \lfloor 360^\circ/\delta \rfloor$ different orientations. In this way, it is possible to define, as extension of the set L of the potential locations, a set L' of potential locations with orientations, $|L'| = n \times |L|$.

Coverage analysis consists in determining which are the points of R that can be controlled by a device positioned in a potential location with a certain orientation. In the following this set of points will be referred to as S, $S \subseteq R$. This operation is made for each potential location of the set L' and it can be performed in two ways:

1. ***Geometrical coverage***: the sub-set S for each potential location of a device is built with reference only to the angle θ and the ray r of the coverage area, without taking into account the presence of obstacles in the region of interest.
2. ***Physical coverage***: the set of points of S is filtered considering the presence of obstacles which can interdict the activity of the device. Hence a set $S' \subseteq S$ is generated. This analysis is based on geometric considerations which take into account the coverage area of the device and the shape and the sizes of the obstacles. In this case the set of points R to be covered has to be reduced to the set R', which is the union of all the sets S', S' = U[S'].

In Fig. 1 we show an example of asset discretization (a grid with 49 points) and 8 potential locations for the devices. Moreover we show the coverage area and the

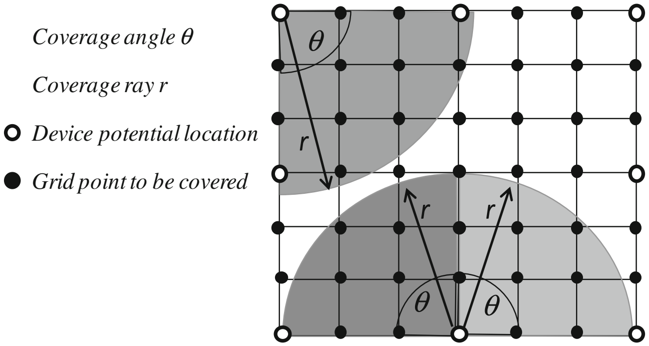
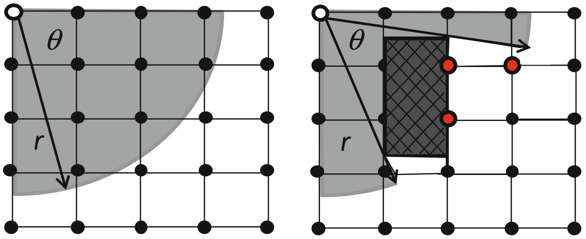


Fig. 1 Asset discretization and coverage area of three devices

Fig. 2 Geometrical and physical coverage of a device



sub-set S of covered points for three devices with a certain orientation. It is important to note, as explained above, that a single device could be located in a point with a certain orientation and that more devices could be located in the same point with different orientations. In Fig. 2 instead we show the difference between the geometrical coverage (sub-set S) and the physical coverage (sub-set S') in case of presence of an obstacle.

The coverage analysis allows to generate the so-called *Coverage Matrix* (*CM*), a binary matrix where the rows correspond to the elements of the set L', i.e. to all the potential locations with orientations, and the columns correspond to the points of the set R to be covered. Hence its dimensions are $(n \times |L|,|R|)$. Its generic element c_{ij} is equal to 1 if device i, $i \in L'$, can cover the point j, $j \in R$, (i.e., in other words, if the point j belongs to the set S' of the device i), otherwise it is equal to 0. The coverage matrix is the fundamental input for all the covering ILP models used in METRIP.

In case of cameras the coverage area is referred to as Field of View (FoV), i.e. the maximum volume visible from a camera, and we do not speak in terms of coverage analysis, but in terms of visibility analysis [19]. Moreover when cameras have to be placed, then two other parameters can be taken into account for specific requirements:

- Spatial Resolution (SP), i.e. the ratio between the total number of pixels on its imaging element excited by the projection of a real object and the object's size.
- Depth of Field (DoF), i.e. the distance between the nearest and farthest objects that appear in acceptably sharp focus in an image.

4.3 Coverage Model Selection

Covering problems can be classified in function of two main objectives (Fig. 3):

- Minimization of number or total cost of control devices to be located,
- Maximization of the region covered by the devices.

The first class of covering problems arises when we have to determine the number of control devices to be located, minimizing the total installation cost and covering all the points of the region of interest or a sub-set of them. Within the first class we can operate the classification of the points of the region in two groups, *important* and *general* points. A point can be classified as important if it is:

- a potential point used by an attacker for the intrusion (window, doors, fences, etc.);
- a valuable point of the RIS (control room, vault, etc.)
- an important point for safety reasons, for instance entrance/exit from elevators and escalators have to be compulsorily controlled by video-surveillance system because the operator has to intervene in case of malfunctioning.

Important points, contrarily to *general points*, have to be compulsorily controlled. If all the points have the same importance, then the problem is referred to as Set Covering Problem (*SCP*) [9], otherwise it is referred to as Weighted Demand Covering Problem (*WDCP*) [22].

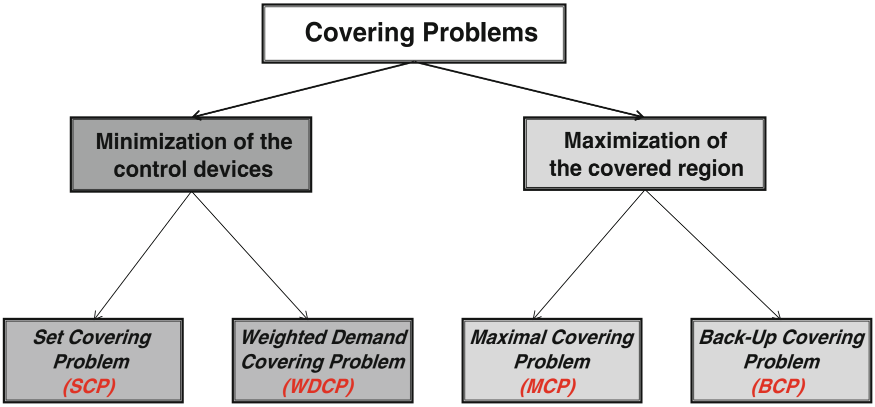

Covering Problems
Minimization of the control devices
Maximization of the covered region
Set Covering Problem (SCP)
Weighted Demand Covering Problem (WDCP)
Maximal Covering Problem (MCP)
Back-Up Covering Problem (BCP)

Fig. 3 Classification of the covering problems

Concerning the second class of covering problems, they arise when we have to determine the position of a prefixed number of control devices in order to maximize primary and/or secondary coverage (also referred to as multiple or back-up coverage) of the region of interest. If the aim is determining the solution which maximizes the primary coverage and consequently the number of primary covered points, then the problem is referred to as Maximal Covering Problem (*MCP*) [10]. If the aim is determining the solution which maximizes the multiple coverage and hence the number of multiple covered points, then the problem is referred to as Back-up Covering Problem (BCP) [27]. In these problems the points to be controlled can be weighted or unweighted, depending on the need of assigning them different importance values.

4.3.1 Minimization of the Control Devices Number

In the formulation of the first class of covering models, the following notations will be adopted:

$R = \{1, \ldots, |\mathrm{R}|\}$ set of points representing the region of interest;
$L' = \{1, \ldots, |L'|\}$ set of device potential locations with orientations;
s_j flag value defined for each j, $j \in R$. It is equal to 1 if the point j has to be compulsorily controlled, 0 otherwise;
h_i installation cost at a potential device location i, $i \in L'$;
α parameter between 0 and 1 regulating the placement of a new device in case a "significant" number of general points of the region of interest is controlled

Moreover the following variables will be used:

- $y_i = \{0, 1\}$: binary variable associated to each potential device location i, $i \in L'$, with a specific orientation. It is equal to 1, if a device is installed at the location i, 0 otherwise.
- $x_j = \{0, 1\}$: binary variable associated to each point j to be covered, $j \in R$. It is equal to 1 if the point j is covered, 0 otherwise.

It is important to underline that, due to the fact that a device can be positioned in a potential location using different orientations, as explained in Sect. 3.2, each y_i variable, $i \in L'$, corresponds to a device in a certain point with a certain orientation.

Set Covering Problem (*SCP*)

The ILP model for the set covering problem is:

$$Min\ z = \sum_{i \in L'} h_i y_i \tag{1}$$

s.t.

$$\sum_{i \in L'} c_{ij} y_i \geq 1 \quad \forall j \in R \tag{2}$$

$$y_i = \{0,\ 1\} \qquad \forall i \in L' \tag{3}$$

The objective function (1) minimize the total installation cost of the control system. Constraints (2) impose that each point $j, j \in R$, has to be covered at least by one device. Constraints (3) are binary constraints for variables y_i, $i \in L'$. Note that, if the cost h_i is equal for all the potential locations i, $i \in L'$, then the model returns the position of the minimum number of control devices to be located in order to cover all the points of the region.

Weighted Demand Covering Problem (*WDCP*)

The ILP model for the weighted demand covering problem is:

$$Min\, z = \sum_{i \in L'} y_i - \alpha \sum_{j \in R} \left(1 - s_j\right) x_j \tag{4}$$

s.t.

$$\sum_{i \in L'} c_{ij}\, y_i \geq 1 \quad \forall j \in R | s_j = 1 \tag{5}$$

$$\sum_{i \in L'} c_{ij}\, y_i \geq x_j \quad \forall j \in R | s_j = 0 \tag{6}$$

$$y_i = \{0,\ 1\} \quad \forall i \in L' \tag{7.a}$$

$$x_j = \{0,\ 1\} \quad \forall j \in R \tag{7.b}$$

The objective function (4) is composed by two terms. The first term minimizes the number of control devices to be located in order to cover all the important points of the region. The second term tries to locate an additional control device if its installation increases the number of controlled general points of a minimum threshold value defined by the parameter α. In order to define the value α, we have to consider that if we want to install a new device just if N^* additional general points are covered, then the value of α has to satisfy the following two conditions: $1 - \alpha \times N^* < 0$ and $1 - \alpha \times \left(N^* - 1\right) > 0$. Constraints (5), as constraints (2), impose that each important point $j, j \in R$, has to be covered at least by one device i, $i \in L'$. Constraints (6) impose that a general point is covered just in case a device able to control it has been installed. Constraints (7a) and (7b) are binary constraints for y_i, $i \in L'$, and x_j, $j \in R$.

4.3.2 Maximization of the Covered Region

In the formulation of the second class of covering models we integrate the previous notations with the following parameters:

- d_j weight associated to a point of the region j, $j \in R$;
- p maximum number of devices to be installed;
- β parameter between 0 and 1 weighting secondary coverage with respect to primary one.

Moreover an additional binary variable will be used:

- $u_j = \{0, 1\}$: binary variable associated to each point j to be covered, $j \in R$. It is equal to 1 if the point j is covered by two or more devices, 0 otherwise.

Maximal Covering Problem (*MCP*)

The ILP model for the maximal covering problem is:

$$Max\, z = \sum_{j \in R} d_j x_j \tag{8}$$

s.t.

$$\sum_{i \in L'} c_{ij} y_i \geq x_j \quad \forall j \in R \tag{9}$$

$$\sum_{i \in L'} y_j = p \tag{10}$$

$$y_i = \{0, 1\} \quad \forall i \in L' \tag{11.a}$$

$$x_j = \{0, 1\} \quad \forall j \in R \tag{11.b}$$

The objective function (8) maximizes the number of covered points of the region, each of them weighted by its importance d_j. If all the points have the same weight, then the model maximizes the number of covered points. Constraints (9) impose that a point j, $j \in R$, is controlled just in case at least one device i, $i \in L'$, among the ones able to control it, is located. Constraint (10) imposes that the number of devices to be located has to be exactly p. Finally constraints (11.a) and (11.b) are binary constraints for variables y_i, $i \in L'$, and x_j,$j \in R$, respectively. Note that using constraint (10) we are implicitly assuming that all the control devices have the same installation cost and moreover this cost does not depend on the position where the device will be located. If we want to take into account different installation costs, this constraint can be generalized using the following budget constraint, where B is the available budget.

$$\sum_{i \in L'} h_i y_i \leq B \tag{12}$$

Back-up Covering Problem (*BCP*)

The ILP model for the back-up covering problem is:

$$Max\, z = (1 - \beta) \sum_{j \in R} d_j x_j + \beta \sum_{j \in J} d_j u_j \tag{13}$$

s.t.

$$\sum_{i \in L'} c_{ij} y_i \geq x_j + u_j \quad \forall j \in R \tag{14}$$

$$\sum_{i \in I} y_i = p \tag{15}$$

$$u_j \leq x_j \quad \forall j \in R \tag{16}$$

$$y_i = \{0,\ 1\} \quad \forall i \in L' \tag{17.a}$$

$$x_j = \{0,\ 1\} \quad \forall j \in R \tag{17.b}$$

$$u_j = \{0,\ 1\} \quad \forall j \in R \tag{17.c}$$

The objective function (13) maximizes the weighted sum of the primary and multiple coverage of the points of the region of interest. The relative weight of these two components is defined by the value of the parameter β. Moreover each point of the region is weighted in function of its importance d_j. Constraints (14) and (15) are the same constraints of the model described for the MCP. Constraints (16) impose that each a point $j, j \in R$, is back-up/multiple covered just in case if it is a primary covered. Finally constraints (17.a), (17.b) and (17.c) are binary constraints for variables y_i, $i \in L'$, x_j and u_j, $j \in R$. Also this model can be generalized by the usage of constraint (12) as done for the *MCP*.

4.4 Framework of the OM

To summarize the main activities performed by the Optimization Module of the METRIP tool can be schematized as reported in Fig. 4.

It is important to note that, as explained in Sect. 1, at first the *OM* receives the input information related to the assets and protections from the *UMLM*, then the *OM* returns the solutions of the covering models to the *UMLM*. This allows to populate the *UMLM* models with additional information which will be used by the *VAM*.

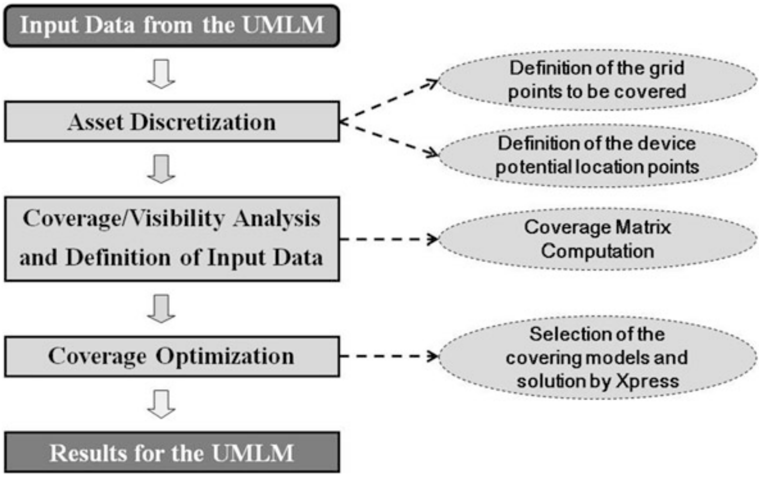

Input Data from the UMLM
Asset Discretization
Definition of the grid points to be covered
Definition of the device potential location points
Coverage/Visibility Analysis and Definition of Input Data
Coverage Matrix Computation
Coverage Optimization
Selection of the covering models and solution by Xpress
Results for the UMLM

Fig. 4 Optimization module main activities

5 Experimental Results

The four presented covering models have been experienced on two test cases which schematize two typical RIS assets: the first is an open space with several entrances along the boundaries, which recalls the idea of a railway station atrium; the second is a scheme of a railway station. The usage of these two particular test cases is motivated by the fact that we wanted to test the model in two opposite situations, i.e. a first situation where no obstacles are present in the area to be controlled, hence geometrical and physical coverage coincide, and a second situation, where instead the presence of blocks significantly affects the covering capabilities of the devices. In both cases the devices to be located are fixed perspective cameras. The characteristics of the used cameras and their orientations are specified for each test case. The models have been solved by the optimization software FICO™ Xpress-MP 7.3 and run on an Intel® Core™ i7, 870, 2.93 GHz, 4 GB RAM, Windows Vista™ 64 bit.

5.1 Open Space Test Case

The tackled open space case is represented in Fig. 5 where the area to be controlled has been discretized with a grid of 441 points. The white and the black circles indicate the side entrances and the possible locations of the cameras (100 points) respectively. Only one kind of camera has been taken into account, referred to as CCTV1 ($\theta = 90°,\ r = 25$). We solve the four presented models using CCTV1 camera with 4 and 8 orientations in the range 0° ÷ 360°. In the first case we have a 400 × 441 coverage matrix, whereas in the second case, a 800 × 441 coverage matrix.

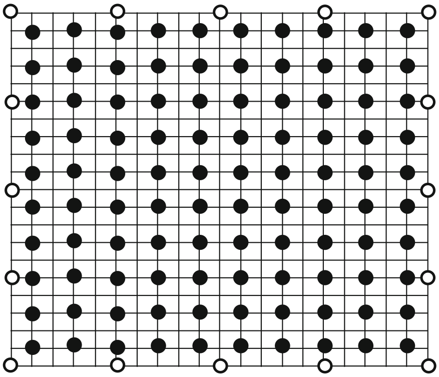


Fig. 5 Open space test case

Results and computation time of the *SCM* and *WDCM* are summarized in Table 1 where: the second column reports the number of cameras to be installed; the third and the forth columns report the number of covered points and the percentage (with respect to the total number of points of the region of interest) respectively; the fifth column reports the computation time in seconds.

In *SCM* the location cost of a camera (h_i, $i \in L'$) has been set to 1, hence it minimizes the number of cameras to be used. In *WDCM*, the parameter α has been set to 0.067. This means (as explained in Sect. 4.3) that the model will locate an additional camera just if it covers at least 10 uncovered general points of the region of interest.

As expected, the *SCM* provides a solution that covers all the points of the region of interest and the introduction of additional camera orientations allows to decrease the number of installed devices from 19 to 18. The *WDCM* provides solution where all the important points are covered and it shows the same reduction, from 15 to 14 cameras when 8 orientations are used. We can also notice that *WDCM*, using 4 cameras less than *SCM*, even if it does not achieve the complete coverage of the region of interest, allows to cover more than 90 % of its points. The highlighted improvement of the solution of the two models using 8 orientations is obvious, even if it is not very consistent. This is basically due to the fact that the region of interest is an open space, free of blocks and hence the usage of more orientations is not very effective.

Table 1 Results of the *SCM* and *WDCM* on the open space scheme

SCM	CCTV	Covered points	COV (%)	CPU time (s)
CCTV1 (4 orient.)	19	441	100	2.4
CCTV1 (8 orient.)	18	441	100	28.3
WDCM (α = 0.067)	CCTV	Covered points	COV (%)	CPU time (s)
CCTV1 (4 orient.)	15	409	92.74	3.3
CCTV1 (8 orient.)	14	414	93.88	13.7

The solutions of the *SCM* and *WDCM* with 4 orientations and 8 orientations are reported in Figs. 6 and 7 respectively, where we indicate the covered, uncovered and important points in light grey, dark grey and white respectively.

Computational results of the *MCM* are summarized in Table 2 where: the second column reports the prefixed value of p, i.e. the number of available cameras; the third and forth columns report the number of covered points and the percentage (with respect to the total number of points of the region of interest) respectively; the fifth and the sixth column report the number of multiple covered points and the related percentage (with respect to the total number of points of the region of interest) respectively; the seventh column reports the computation time. The maximum values of p in the two cases, i.e. 19 and 18, are imposed on the basis of the *SCM* results.

Generally different values of the weight d_j can be chosen for the grid points to be covered in function of their positions within the region of interest. In this experimentation they have been set to 10 for some relevant points and to 1 for the other points. This allows us to compare the *MCM* solutions, where the important points

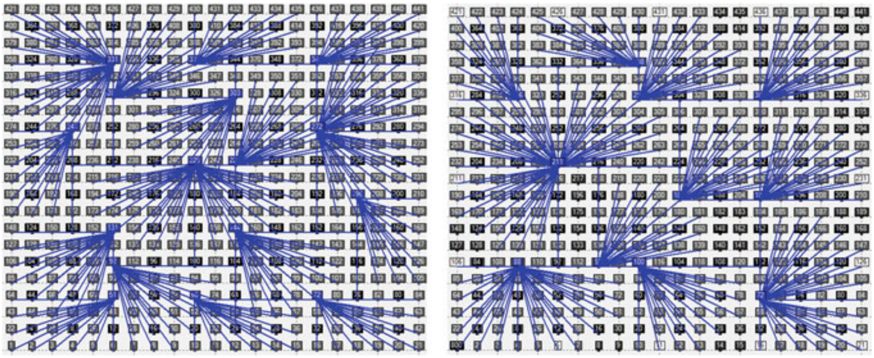


Fig. 6 Solutions of *SCM* and *WDCM* with CCTV1 cameras (4 orientations)

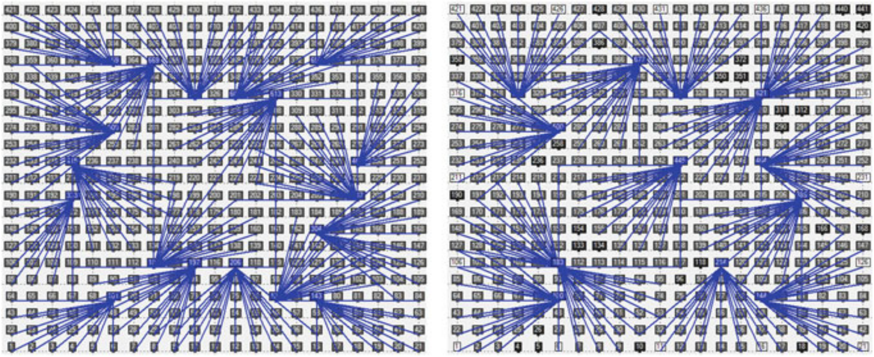


Fig. 7 Solution of *SCM* and *WDCM* with CCTV1 cameras (8 orientations)

Table 2 Results of *MCM* on the open space case

	CCTV	Covered points	COV (%)	M-covered points	M-COV (%)	CPU time (s)
CCTV1 (4 orient.)	8	278	63.04	0	0	3.1
	10	331	75.06	12	2.7	8.3
	13	388	87.98	33	7.5	62.4
	16	426	96.59	57	12.9	85.5
	19	441	100	100	22.7	120.0
CCTV1 (8 orient.)	8	278	63.04	0	0	6.7
	10	334	75.37	5	1.13	41.8
	13	398	90.25	26	5.8	72.6
	16	432	97.96	50	11.3	102.6
	18	441	100	88	19.9	160.9

have higher weight values, and *WDCM* solutions, where the important points have to be compulsorily covered.

It is easy to observe that the computation time increases with the value of p, but in all the cases we find the optimal solution within an acceptable computation time.

In Table 2 we also report the percentage of the multiple-covered points of the region of interest (referred to as M-COV %), since we want to highlight the fact that this coverage model, as the ones presented above, does not provide solution where each point has to be compulsorily covered by just one device.

Also in this case we can notice that using the same number of cameras, the solutions with 8 orientations for each potential location are obviously better than the ones with 4 orientations. Anyway, also in this case the improvement is not so effective because of the structure of the area. This observation can be clearly noticed in Fig. 8 where the percentage of primary and multiple covered points, varying the value of p and using 4 and 8 orientations, are reported. It is easy to see that these two trends are very similar. Finally in Fig. 9, as an instance, we show the solutions obtained with p = 10 and p = 18 using 8 orientations. We can note that in both cases, all the important points are covered by at least one camera and the solution

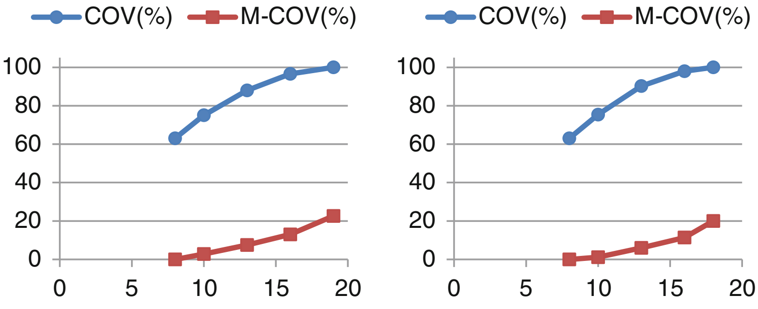


Fig. 8 Primary and multiple coverage solving *MCM* varying p with 4 and 8 orientations

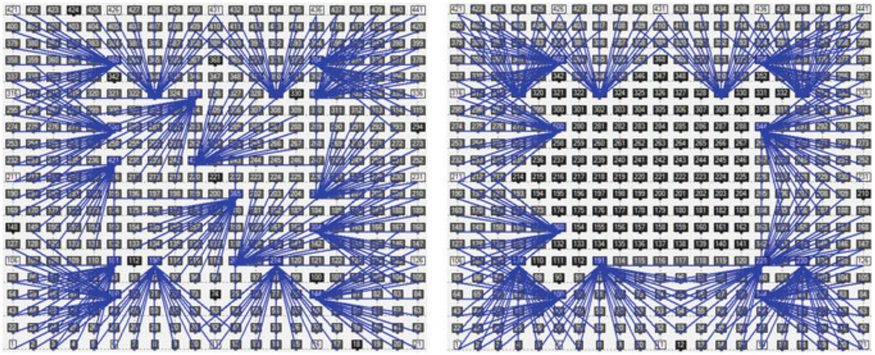


Fig. 9 *MCM* solutions using 10 and 18 cameras (8 orientations)

using 18 cameras is slightly different by the optimal one of the *SCM* because of the different weights of the points.

The results of the *BCM* are summarized in Table 3 The reported information are the same of Table 2, with the addition of the column β, i.e. the weight of the multiple coverage with reference to the primary one. The same d_i values defined for *MCM* have been used. For the sake of brevity, we just present the results with 4 and 8 orientations varying β but fixing the value of p to 19 and 18, i.e. to the number of cameras required for the complete coverage of the area. It is easy to observe that the usage of β values higher than 0 provides an increase of the percentage of multiple-covered points and the usage of β values lower than 0.5 allows to obtain solutions with a good trade-off between primary and multiple coverage of the points. This results is also highlighted in Fig. 10 where the percentage of primary and multiple covered points varying *β* is reported. Finally, as an instance, in Fig. 11 we show the solutions obtained by *BCM* using 18 cameras with β = 0.2 and β = 0.9 respectively. It is important to observe that the solution with β = 0.2 covers almost all the region

Table 3 Results of *BCM* on the open space case

	β	CCTV	Covered points	COV (%)	M-covered points	M-COV (%)	CPU time (s)
CCTV1 (4 orient.)	0	19	441	100	100	22.70	120.0
	0.2	19	428	97.05	137	31.07	97.7
	0.4	19	404	91.61	174	39.46	11.4
	0.6	19	358	81.17	221	50.11	202.3
	0.9	19	336	76.19	259	58.73	244.0
CCTV1 (8 orient.)	0	18	441	100	88	19.9	160.9
	0.2	18	430	97.5	152	34.47	111.2
	0.4	18	420	95.24	160	36.28	94.4
	0.6	18	325	73.70	225	51.02	289.4
	0.9	18	311	70.52	238	53.97	302.8

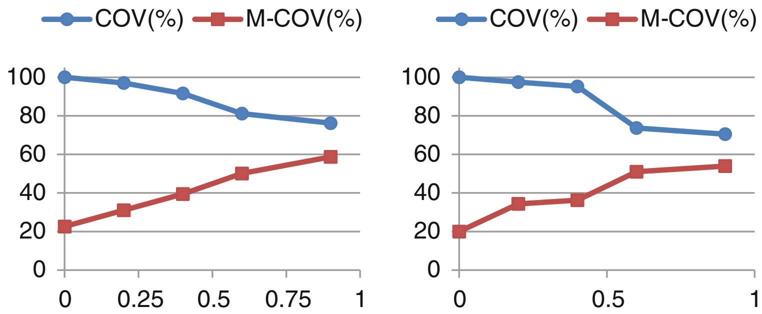


Fig. 10 Primary and multiple coverage solving *BCM* using 19 cameras (4 orientations) and 18 cameras (8 orientations) varying β

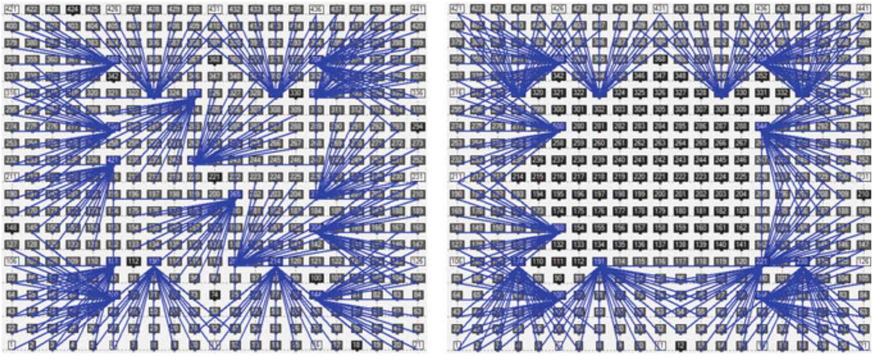


Fig. 11 *BCM* solutions using 18 cameras (8 orientations) with β = 0.2 and β = 0.9

of interest only once, whereas the solutions with β = 0.9 covers the important points of the region of interest (characterized by higher weight values) more than once.

5.2 Railway Station Case

In this section we present the results of the four models on the railway station scheme reported in Fig. 12 The area to be controlled has been discretized by 621 points, which are then reduced to 526 because of the presence of the obstacles (offices, walls and pillars). The potential locations for the cameras are 143, represented by black circles. The important points are represented by white circles and are positioned in correspondence of entrances, elevators, lifts and among the platforms (Fig. 13).

Two kinds of cameras have been taken into account: CCTV1 ($\theta = 90^\circ,\ r = 25$); CCTV2 ($\theta = 30^\circ,\ r = 50$). We solve the models using:

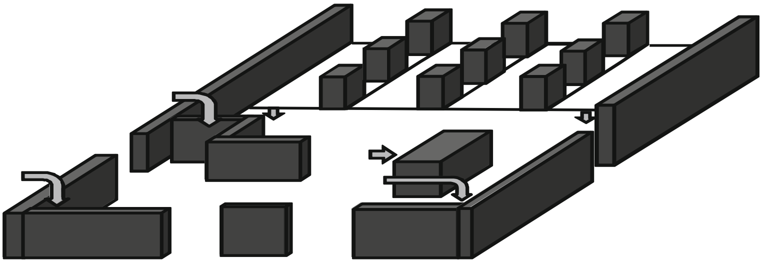


Fig. 12 3D scheme of the station

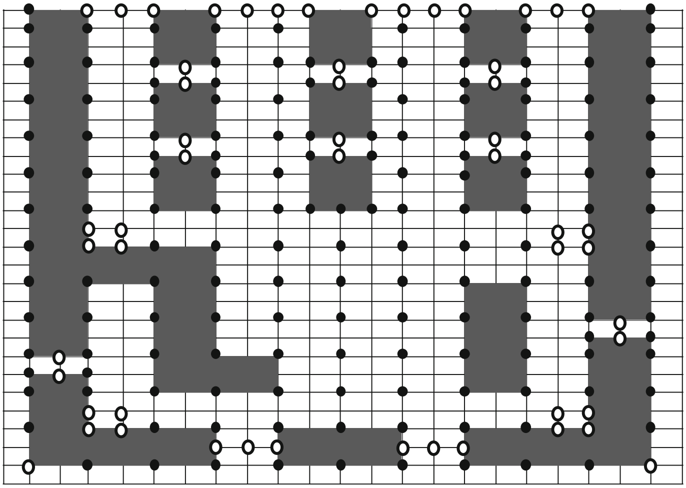


Fig. 13 Discretized scheme of the station with potential camera locations and important points

- CCTV1 with 8 orientations in the range 0° ÷ 360°;
- CCTV1 with 8 orientations in the range 0° ÷ 360° and CCTV2 with 12 orientations in the range 0° ÷ 360°.

In the first case we have a 1,144 × 621 coverage matrix, whereas in the second case we have a 2,860 × 621 coverage matrix.

Computational results of the *SCM* and *WDCM* are summarized in Table 4 where the same information of Table 1 are reported. Also in this case in *SCM* the cost of each camera (h_i, $i \in L'$) has been set to 1, and in *WDCM*, the parameter α has been set to 0.067. As expected the *SCM* provides a solution that covers all the points of the region of interest and the usage of both kind of cameras (i.e. 20 different camera orientations) allows to decrease the number of installed devices from 45 to 39. Hence, contrarily to what occurred for the open space, in this case the reduction of the number of cameras is more consistent. This is due to the fact that geometrical

Table 4 Results of the *SCM* and *WDCM* models on the railway station scheme

SCM	# CCTV	Covered points	COV (%)	CPU time (s)
CCTV1	45	526	100	0.5
CCTV1 + CCTV2	39	526	100	6.3
WDCM (α = 0.067)	# CCTV	Covered points	COV (%)	CPU time (s)
CCTV1	26	366	69.58	1.4
CCTV1 + CCTV2	28	449	85.36	5.5

and physical coverage do not coincide for most of the camera possible positions/orientations.

Concerning instead *WDCM*, it returns solutions that cover all important points but, contrarily to the open space case, they do not cover almost all the region of interest. Moreover we can note that the usage of both kinds of cameras provides an increase of the located ones, contrarily to what occurs for the *SCM*. This can be explained by the fact that, given the presence of the blocks, no additional 90° camera able to cover at least 10 uncovered points could be found. On the contrary, the usage of a 30° camera, allows to achieve this result with two additional cameras. The solutions of the *SCM* and *WDCM* with a single kind of camera (CCTV1) and with both kinds of cameras (CCTV1 and CCTV2) are reported in Figs. 14 and 15 respectively.

Computational results of *MCM* are summarized in Table 5 which reports the same information of Table 2. Also in this case, as done for the open space case, the maximum values of p, i.e. 45 and 39, are imposed on the basis of the *SCM* results and the weight values (d_i) has been set 1 for the generic points and to 10 for the important ones in order to compare the solution with the one of *WDCM*.

The same considerations provided for the open space case can be repeated for the railway station scheme. Indeed we can notice that using the same number of devices, the solutions with two kinds of cameras are significantly better than the ones with one kind of camera. As explained for the *SCM* and *WDCM*, this result

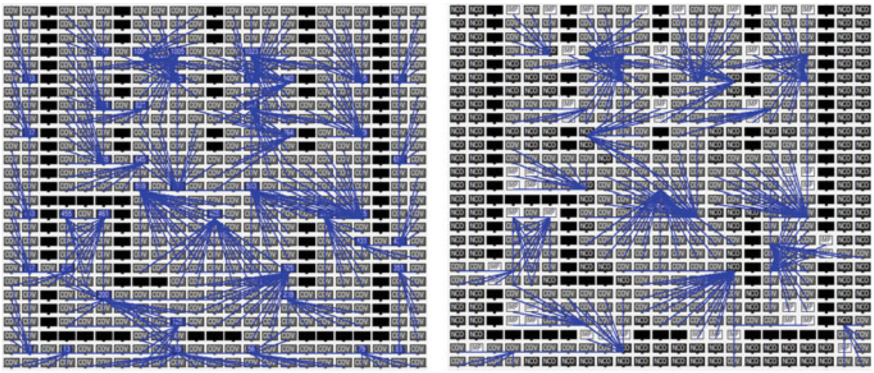


Fig. 14 Solutions of *SCM* and *WDCM* with CCTV1 cameras (8 orientations)

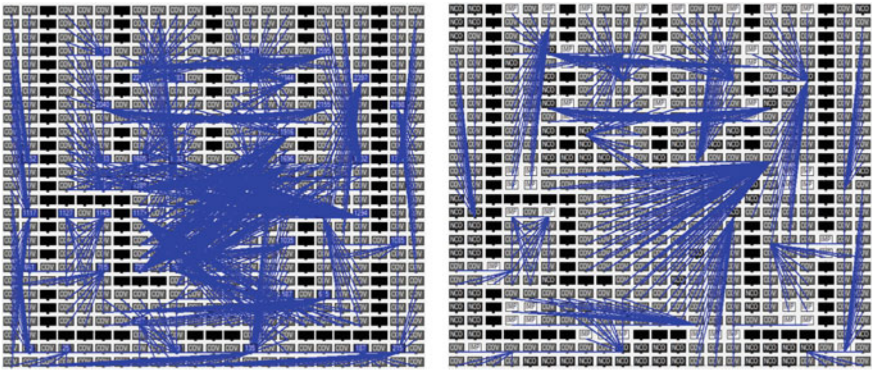


Fig. 15 Solutions of *SCM* and *WDCM* with both cameras (8 + 12 orientations)

Table 5 Results of *MCM* on the railway station scheme

	CCTV	Covered points	COV (%)	M-covered points	M-COV (%)	CPU time (s)
CCTV1	17	347	65.97	22	4.18	2.2
	24	430	81.75	20	3.80	7.9
	31	488	92.78	57	10.84	12
	38	515	97.90	95	18.06	14.48
	45	526	100	171	32.51	11.09
CCTV1 + CCTV2	17	426	80.99	38	7.22	12.5
	24	481	91.45	80	15.21	21.2
	31	509	96.67	161	30.61	43.8
	38	525	99.81	172	32.70	23.7
	39	526	100	174	33.08	50.2

depends on the structure of the station, where many blocks are present. This observation can be also noticed in Fig. 16 where the percentage of primary and multiple covered points varying the value of p, using one kind and two kind of cameras are reported. It is easy to see that these two trends are significantly different for this test case, contrarily to what occurred for the open space case.

Finally, as an instance, in Fig. 17 the solutions obtained using the two kinds of cameras with $p = 31$ and $p = 39$ are shown. Also in this case, as for the open space, we can note that all the important points are covered by at least one camera and that the solution with 39 cameras is different by the *SCM* optimal because of the different weights of the points.

The results of the *BCM* are summarized in Table 6 which reports the same information of Table 3. Also in this case it is easy to observe that the usage of β values higher than 0 provides an increase of the percentage of multiple-covered points and values lower than 0.5 allows to obtain solutions with a good trade-off

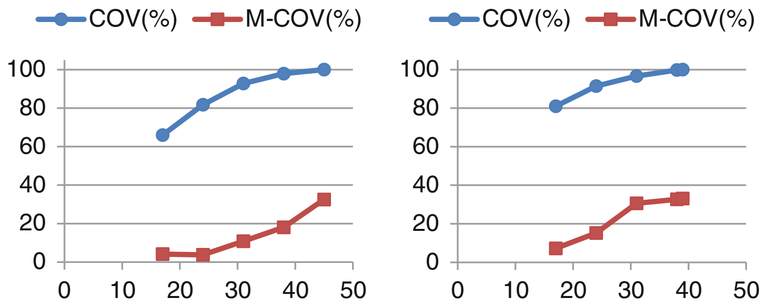


Fig. 16 Primary and multiple coverage solving *MCM* varying *p* with CCTV1 cameras (8 orientations) and with both kind of cameras (8 + 12 orientations)

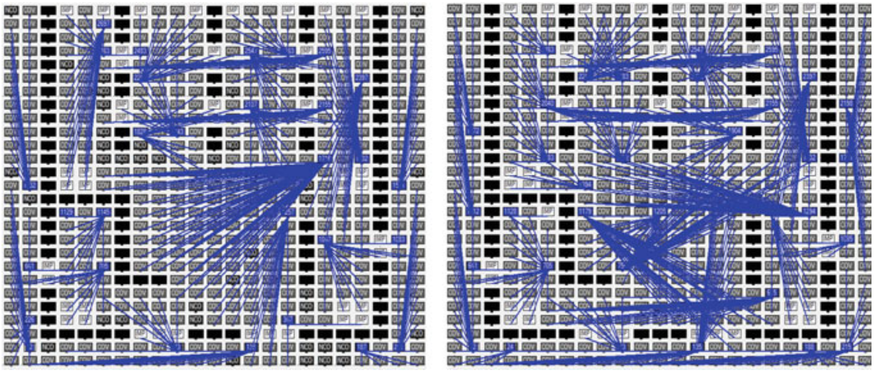


Fig. 17 *MCM* solutions using 31 and 39 cameras (8 + 12 orientations)

Table 6 Results of *BCM* on the railway station case

	β	CCTV	Covered points	COV (%)	M-covered points	M-COV (%)	CPU time (s)
CCTV1	0	45	526	100	171	32.51	11.09
	0.2	45	368	69.97	228	43.35	0.4
	0.4	45	334	63.50	234	44.49	0.2
	0.6	45	328	62.36	241	45.82	0.9
	0.9	45	302	57.41	251	47.72	4.7
CCTV1 + CCTV2	0	39	526	100	174	33.08	50.2
	0.2	39	375	71.29	225	42.78	20.4
	0.4	39	374	71.10	227	43.16	38.4
	0.6	39	361	68.63	239	45.44	43.3
	0.9	39	320	60.84	265	50.38	216.8

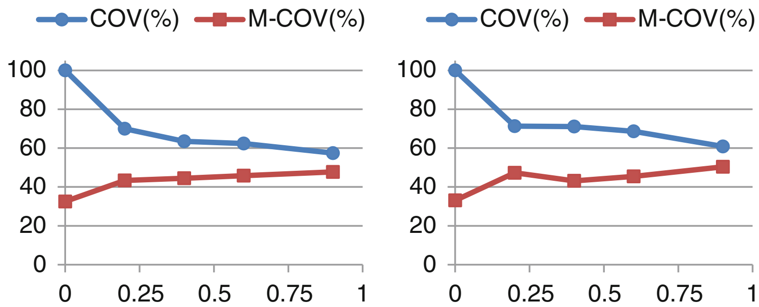


Fig. 18 Primary and multiple coverage solving *BCM* using 45 cameras (8 orientations) and 39 cameras (8 + 12 orientations) varying β

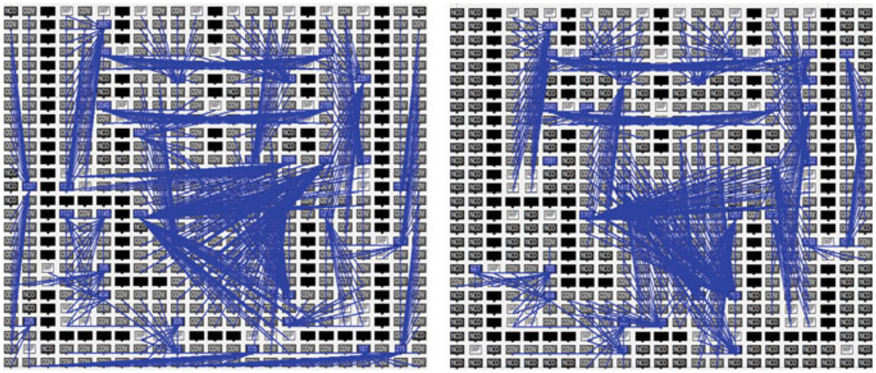


Fig. 19 *BCM* solutions using 39 cameras (8 + 12 orientations) with β = 0.2 and β = 0.9

between the primary and multiple coverage of the points. This results is also highlighted in Fig. 18 where the percentage of primary and multiple covered points varying β is reported.

Finally, as an instance, in Fig. 19 the solutions obtained using p = 39 cameras (8 + 12 orientations) with β = 0.2 and β = 0.9 are shown. It is important to observe how the solution with β = 0.2 covers almost all the region of interest, whereas the solutions with β = 0.9 covers more than once the same zones of railway station scheme.

6 Conclusions

In this chapter we presented the combinatorial optimization models used in the Optimization Module of the methodological tool developed in the European project METRIP, aimed at supporting the design of a security system for the protection of the railway infrastructure system assets.

We described four models that the designer can use alternatively in accordance to the specific security and economic needs that the project has to satisfy. Moreover we also discussed some issues that can be integrated in these models in order to take into account other security requirements related to usage of video-analysis algorithms.

The presented models have been experienced on two different test cases, characterized by very different geometrical properties obtaining good solutions with acceptable computation time, so confirming their effective applicability.

Acknowledgments This work is supported by Ansaldo STS under Grant HOME/2010/CIPS/AG/035 METRIP—MEthodological Tools for Railway Infrastructure Protection, financed by the European Commission, Directorate-General Home Affairs, within the Specific Programme on Prevention, Preparedness and Consequence Management of Terrorism and other Security-related risks.

References

1. Jenkins BM, Butterworth BR (2010) Explosives and incendiaries used in terrorist attacks on public surface transportation: a preliminary empirical analysis. Mineta Transportation Institute
2. Butterworth BR (2011) Empirical data to guide risk mitigation: examples from MTI database. Mineta Transportation Institute National Transportation Security Center
3. Wilson JM, Jackson BA, Eisman M, Steinberg P, Riley KJ (2007) Securing America's passenger-rail systems. Rand Corporation, Santa Monica
4. Sforza A, Sterle C, D'Amore P, Tedesco A, De Cillis F, Setola R (2013) Optimization models in a smart tool for the railway infrastructure protection. Lect Notes Comput Sci 8328:191–196. doi:10.1007/978-3-319-03964-0_17
5. Daskin MS (1995) Network and discrete location: models, algorithms and applications. Wiley, New York
6. Hakimi SL (1964) Optimum locations of switching centers and the absolute centers and medians of a graph. Oper Res 12:450–459
7. ReVelle CS, Swain RW (1970) Central facilities location. Geogr Anal 2(1):30–42
8. Hakimi SL (1965) Optimum distribution of switching centers in a communication network and some related graph theoretic problems. Oper Res 13:462–475
9. Toregas C, ReVelle C, Swain R, Bergman L (1971) The location of emergency service facilities. Oper Res 19:1363–1373
10. Church R, ReVelle C (1974) The maximal covering location problem. Pap Reg Sci Assoc 32:101–118
11. Berman O, Drezner Z, Krass D (2010) Generalized coverage: new developments in covering location models. Comput Oper Res 37:1675–1687
12. Li X, Zhao Z, Zhu X, Wyatt T (2011) Covering models and optimization techniques for emergency response facility location and planning: a review. Math Methods Oper Res 74:281–310
13. Chvàtal V (1975) A combinatorial theorem in plane geometry. J Comb Theory, Ser B 18: 39–41
14. O'Rourke J (1987) Art gallery theorems and algorithms. Oxford University Press, New York
15. Ghosh SK (2010) Approximation algorithms for art gallery problems in polygons. Discrete Appl Math 158(6):718–722
16. Guvensan MA, Yavuz AG (2011) On coverage issues in directional sensor networks: a survey. Ad Hoc Netw 9(7):1238–1255

17. Chakrabarty K, Sitharama S, Cho E (2002) Grid coverage for surveillance and target location in distributed sensor networks. IEEE Trans Comput 51(12):1448–1453
18. Dhillon SS, Chakrabarty K, Iyengar SS (2002) Sensor placement for grid coverage under imprecise detections. In: Proceedings of the 15th international conference on information fusion vol 2, pp 1581–1587
19. Erdem UM, Sclaroff S (2006) Automated camera layout to satisfy task-specific and floor plan-specific coverage requirements. Comput Vis Image Underst 103:156–169
20. Hörster E, Lienhart R (2006) On the optimal placement of multiple visual sensors. In: Proceedings of the 4th ACM international workshop on Video surveillance and sensor networks (VSSN), pp 111–120
21. Murray AT, Kim K, Davis JW, Machiraju R, Parent R (2007) Coverage optimization to support security monitoring. Comput Environ Urban Syst 31(2):133–147
22. Yabuta K, Kitazawa H (2008) Optimum camera placement considering camera specification for security monitoring. Int Symp Circ Syst ISCAS 2008:2114–2117
23. Osais Y, St-Hilaire M, Yu F (2009) On sensor placement for directional wireless sensor networks. In: Proceeding of IEEE international conference on on communications (ICC'09), Dresden, Germany, pp 1–5
24. Van Der Hengel A, Hill R, Ward B, Cichowsi A, Detmold H, Madden C, Dick A, Bastian J (2009) Automatic camera placement for large scale surveillance networks. In: 2nd international conference on pervasive technologies related to assistive environments, (PETRA)
25. Debaque B, Jedidi R, Prevost D (2009) Optimal video camera network deployment to support security monitoring. Inf Fusion 1730–1736
26. Mostafavi SA, Dehghan M (2011) Optimal visual sensor placement for coverage based on target location profile. Ad Hoc Netw 9:528–541
27. Hogan K, ReVelle C (1986) Concepts and applications of backup coverage. Manage Sci 32:1434–1444

The METRIP Tool

Stefano Marrone, Nicola Mazzocca, Concetta Pragliola, Antonio Sforza, Claudio Sterle and Valeria Vittorini

Abstract This chapter describes the results of the work conducted within the METRIP project in order to define a tool-chain supporting the methodological approach to the protection of railway infrastructures. The proposed tool-chain allows for: (a) modelling the RIS infrastructure, attack scenarios and protection technologies, (b) generating quantitative models to perform vulnerability analyses, and (c) generating and solving integer linear programming covering models to determine the optimal design choice in the development of physical protection systems. The chapter illustrates the functional and logical architecture of the tool-chain and describes the realization of a prototype to demonstrate the feasibility and effectiveness of the proposed approach.

Keywords Railway infrastructure protection · Tool-chain · Optimal coverage · Integer linear programming · Vulnerability analysis

S. Marrone (✉)
Seconda Università di Napoli, Dipartimento di Matematica e
Fisica, viale Lincoln, 5, 81100 Caserta, Italy
e-mail: stefano.marrone@unina2.it

N. Mazzocca · A. Sforza · C. Sterle · V. Vittorini
Department of Electrical Engineering and Information Technology (DIETI),
University "Federico II" of Naples, Via Claudio, 80125 Naples, Italy
e-mail: nicola.mazzocca@unina.it

A. Sforza
e-mail: sforza@unina.it

C. Sterle
e-mail: claudio.sterle@unina.it

V. Vittorini
e-mail: valeria.vittorini@unina.it

C. Pragliola
Ansaldo STS, Via Nuova delle Brecce 260, 80147 Naples, Italy
e-mail: Concetta.Pragliola@ansaldo-sts.com

R. Setola et al. (eds.), *Railway Infrastructure Security*, Topics in Safety,
Risk, Reliability and Quality 27, DOI 10.1007/978-3-319-04426-2_10

1 Introduction

The METRIP project arises with the aim of proposing smart methodologies for railway infrastructure protection and realizing a prototypal tool which provides the designer/analyst of a Physical Protection System[1] (PPS, Chap. 8) with three main integrated functionalities: modelling the Railway Infrastructure System (RIS), attack scenarios and protection devices; defining optimal location of one or more kind of protection devices of a PPS and performing vulnerability analysis.

Hence, a tool-chain has been designed to support the METRIP process defined in Chaps. 8 and 9. It consists of three main components corresponding to the three functionalities to be realized: UML modelling module (*UMLM*), Optimization module (*OM*) and Vulnerability Analysis Module (*VAM*).

A functional view of the tool-chain is represented in Fig. 1, where the interactions between the three modules are shown. The straight lines represent the main interactions between the user and the modules, and the dotted lines represent automatically performed operations.

UMLM aids the modelling of railway infrastructures, attack scenarios and protection devices, according to the UML CIP_VAM profile defined in Chap. 8. The annotated UML models are input for the *OM* and *VAM* components.

OM supports the generation and solution of optimization models and methods which provide the optimal solution in terms of placement of *PPS* protection devices, according to what described in Chap. 9.

VAM is in charge of generating and solving vulnerability models, according to the approach defined in Chap. 8.

The tool-chain user interface provides the user with three integrated perspectives: CIP_VAM modelling, Optimization and Analysis. By means of the modelling perspective, the user creates a high level model, and then two use case scenarios are possible:

- Generation and solution of the optimization models and related input/output data;
- Generation and solution of vulnerability analysis models.

The first use case is directed to the design of the PPS by means of the automated generation of input data about geometrical and functional asset properties and technological protection device features. Optimization models and algorithms are then in charge of defining the set of all possible solutions and then determining the best one. The generation process of the input data and the pre-processing required for their usage in the *OM* are described in Chaps. 8 and 9 respectively. In particular the METRIP tool, using the UMLM functionalities, generates the information needed by the *OM* and stores them in the configuration file. Then it invokes the optimization tools (models) by providing them with proper commands and inputs. Finally it retrieves the results produced by the *OM* and it updates the UML models

[1] Also referred as baseline security system (*BSS*, Chap. 9).

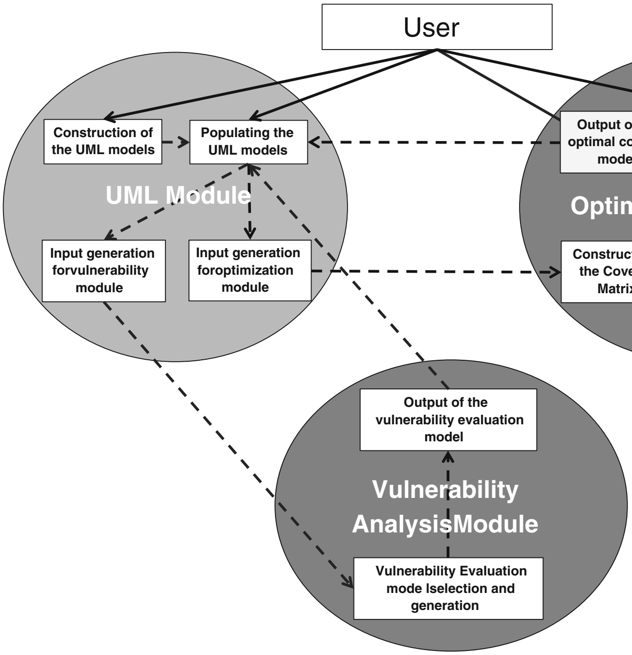

User
UML Module
Construction of the UML models
Populating the UML models
Input generation forvulnerability module
Input generation foroptimization module
OptimizationModule
Output of the optimal coverage model
Model Calibration and Setting
Construction of the Coverage Matrix
Coverage Model selection and generation
Vulnerability AnalysisModule
Output of the vulnerability evaluation model
Vulnerability Evaluation mode lselection and generation

Fig. 1 METRIP tool chain modules and interactions

of the protection devices by annotating the information about the located PPS devices, provided by the optimization models.

The second use case consists in the possibility to compute several vulnerability indices for the evaluation of the system obtained by the composition of both system-to-protect and the PPS. The tool-chain may be also used to perform what-if analyses and evaluate different design choices. The designer and/or the analyst are in charge of modifying the models and re-executing the location and/or the vulnerability analysis in order to obtain different solutions to be compared using different performance criteria.

Applications of the described use cases to a real transit system and ad-hoc generated test problems are reported in Chaps. 8 and 9 respectively. In particular in Chap. 8, after the UML modelling phase, both the use cases have been tackled, i.e. the solution of the optimal full coverage problem (set covering problem, Chap. 9) of a station area, by means of closed-circuit cameras, and the vulnerability evaluation of the resulting protection system against bombing attack scenarios. Moreover in Chap. 8 the impact of different solutions on vulnerability is also evaluated. In Chap. 9, instead, different covering optimization problems have been applied to two different railway test problems schematizing an atrium of a railway station and a complex railway station scheme respectively.

In this chapter we focus on the tool-chain definition. A reference architecture is presented in Sect. 2, it is described starting from the three perspectives defined before. Section 3 contains a specification of the *UMLM*, *OM* and *VAM* components. Section 4 draws a map of available tools and technologies that maybe used to implement the tool-chain and instantiate the reference architecture introduced in Sect. 2. Section 5 describes a prototype implementation. Finally Sect. 6 contains some closing remarks.

2 A Reference Architecture

The logical architecture of the METRIP tool-chain is shown in Fig. 2. It describes the large-scale organization of the tool-chain into four levels. “Higher” levels call upon the services of “lower” levels but not vice versa. The calls to lower level services are represented by arrows. The four levels are: (1) Presentation: it is realized by the *UI* package. (2) UML Modelling: it is realized by the *CIP_VAM Modelling Perspective* package. (3) Evaluation: it is realized by the *Optimization Perspective* and *Analysis Perspective* packages. (4) Services: it is realized by the *Technical Services package*.

The Presentation level provides a user interface (*UI*) to specify user’s preferences, inputs and commands (*dashboard* package, which may contain widgets objects), and visualizes evaluation results (*Presentation windows* package).

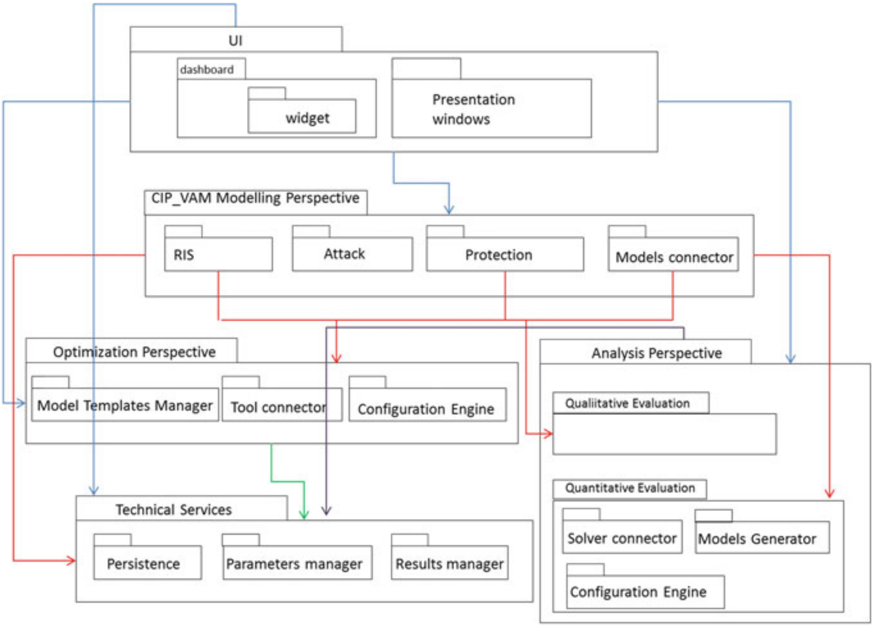


Fig. 2 Tool-chain logical architecture

The UML Modelling level provides support to build and handle UML models stereotyped by the CIP_VAM profile.

The package *Models connector* is in charge of creating links about UML models (e.g. link among RIS and Attack models, or among Protection and RIS models).

The Evaluation level is the core of METRIP tool. It realizes the *OM* and *VAM* components.

As for the *Optimization Perspective* subsystem, the *Model Templates Manager* contains objects to handle and instantiate different optimal covering/location models, as required by the designer/analyst (through the dashboard). The *Tool connector* is in charge of guaranteeing the interoperability with the optimization tool. At this aim, it provides the interface towards the optimization tool (e.g. it generates the proper commands for its execution). The *Configuration Engine* generates the file(s) containing the information needed to instantiate the optimization models. At this aim it provides the necessary inputs according to the proper data format and retrieves the needed parameters from the RIS and Protection UML models. Both the *Tool connector* and the *Configuration Engine* must be customized according to the adopted optimization tool and the kind of the model to be instantiated.

As for the *Analysis Perspective* subsystem, the *Qualitative Evaluation* package contains objects to perform the evaluation of the indices required by the designer/analyst (through the dashboard). The *Quantitative Evaluation* package is in charge of generating and solving the models for the vulnerability analysis. The *Solver connector* is in charge of guaranteeing the interoperability with the analysis engine/tool. As for the *Configuration Engine*, the *Solver connector* provides the interface towards the analysis tool (e.g. it generates the proper commands for its execution). The *Model Generator* is in charge of generating the analysis models: it retrieves the needed information from the RIS, Attack and Protection UML models. The *Configuration Engine* generates the input file(s) for the tool according to the proper data format. The *Solver connector*, the *Model Generator* and the *Configuration Engine* must be customized according to the adopted analysis tool.

The Service level includes the *Technical Services* subsystem which consists of general purpose objects providing technical services in support of higher levels. The *Persistence* package is in charge of managing the necessary repositories and provides DB functionalities. The *Parameters Manager* contains objects to gather the initial values for the model parameters and handle them. The *Result Manager* contains objects to gather the results obtained by the execution of the optimization and analysis phases. It communicates them to the user by updating the UML models and/or by providing them back to the *Presentation* level.

3 Component Specifications

The reference architecture presented in Sect. 2 supports the process described in Chaps. 8 and 9. The analysis models and the input for the optimization phase are built automatically from the UML models according to a model-driven engineering approach [1], which is based on the definition and implementation of proper model transformations [2]. Here below we summarize the functional specifications that the components of the tool-chain must meet.

3.1 System Level Specifications

The METRIP tool-chain aids the modelling of railway infrastructures, attack scenarios and protection devices according to the UML CIP_VAM profile [3]. These models are the input for both the optimization and analysis use cases. All the models, the intermediate and final artefacts or the overall modelling and analysis processes have to be stored in proper repositories. It should be also possible to retrieve information about assets, attacks and protection devices from a proper PPS Database. Some tasks are not automatable. Specifically, the user is in charge of:

- specifying available UML models of both the RIS target and the protection devices to be located;
- selecting the optimization model to be executed;
- selecting the vulnerability model to be generated;
- providing the parameters to properly tune an optimization model or a vulnerability model, if needed;
- specifying the command to generate the configuration file;
- modifying the models and re-executing the localization and/or the vulnerability analysis in order to obtain different solutions to compare and perform what-if analyses.

These actions may be accomplished through the User Interface. A complete version of the tool-chain should:

1. generate the information needed to the optimization tool and store them into the configuration file, invoke the optimization tool by providing it with proper commands and inputs, retrieve the results produced by the optimization tool, update the UML models of the protection devices by annotating them with the localization information obtained from the solution of the optimization model.
2. generate the information needed to the analysis tool and store them into the configuration file, invoke the analysis tool by providing it with proper commands and inputs, retrieve the results produced by the analysis tool, update the UML model by annotating them with the vulnerability information obtained from the solution of the analysis model.
3. evaluate the vulnerability indices specified by the user and provide him/she with the results of the evaluation.
4. define proper workspaces in order to define and user's project areas, collect and manage the artefacts produced within a project.

Specifically, the tool-chain supports the design of a PPS by optimizing a chosen protection criterion (i.e. with a specific optimization model) within an unprotected railway asset in terms of number and position of a specific kind of protection devices. The integration of an already installed PSS within a railway asset with a specific kind of protection devices is also allowed. In this case the user should load all the information related to the pre-installed devices, in order to opportunely fix the values of the related optimization model variables.

Through the vulnerability analysis, the tool-chain allows the evaluation of the effectiveness, in terms of different protection criteria, of a PPS solution and enables the possibility for a security expert to modify the solution obtained by the optimization module on the base of his/her experience. In this case the user should intervene directly in the variable fixing of the tool, or opportune interfaces should be realized.

It could be enabled the possibility to take into account the usage of a given set of video-analysis algorithm in the design of the PSS (i.e. yellow line, face recognition) or constraints on the placement of several devices in function of their security needs. In this case, the optimization models should be integrated with specific constraints which better define the relative position between a set of points to be controlled and the position of the protection device.

3.2 UML Modelling Module (UMLM)

The role of the UML module (*UMLM*) is to provide the user with a workbench to edit, save and modify UML models annotated by the CIP_VAM profile.

Thus, it should provide three different views: Infrastructure, Protection Systems and Attack Scenario. A complete version of the tool-chain should provide the user with a user-friendly interface and mask the UML extensions and data types described in the CIP_VAM UML profile by graphical icons, so raising the usability of the tool-chain. For each one of the three views, the *UMLM* allows to:

- create, save, load and modify new UML models;
- populate UML models with data to characterize RIS assets, attacks and devices.

These functionalities may be partially provided by relying on existing and assessed environments.

3.3 Optimization Module (OM)

OM uses as input the information about the asset and the protection devices provided by *UMLM*. On this basis, the *OM* performs at first a pre-processing of these data in order to make them usable by the optimization solver and then it manages a library of optimal covering Integer Linear Programming (ILP) models. These models determine the number and the location of most of the control devices which constitute the PSS [4], and are derived by the main covering models present in literature [5, 6].

In particular, the pre-processing performs the coverage analysis and it generates the so-called *coverage matrix* which is the main input for the optimization models.

The *OM* returns the optimal location of a specific kind of PSS or of a specific class of PPS devices within a railway asset, schematized by its two dimensional representation. In this case with the expression "class of protection devices" we refer to devices providing the same security service, e.g. CCTVs, volumetric sensors, etc., but with different technical features and performances.

Hence, the complete version of the *OM* provides the following functionalities:

1. discretization of the asset under investigation with a two-dimensional grid of points;
2. generation of the potential protection device locations;
3. coverage analysis for the protection device of the class of protection devices under investigation within the two dimensional representation of the asset under investigation;
4. optimization model selection and generation. The optimization model can be solved by an open source or a commercial optimization solver;
5. output generation and graphical representation (depending on the functionalities of the optimization software used for the optimization module). The output is generated and saved in a file which contains for each kind of protection device the number and the specific positions. This output is returned to the *UMLM*.

The discretization of the asset and the generation of the potential locations (points 1 and 2) are automatically performed by using a step size which depends on the geometrical information about the asset under investigation. Indeed the whole grid of points is built in a way which guarantees that the optimization models have dimensions—in terms of variables and constraints—that allow the solution with an acceptable computation time by standard optimization methods. The discretization grid can be integrated by the user with other "important" points which have to be protected and it may be also modified by the presence of blocks or other limitations on the points to be controlled. Similarly, the grid of localizations can be integrated or modified by introducing new possible locations or deleting existing ones.

The coverage analysis (point 3) performs both the geometrical (no obstacles in the area) and physical visibility analysis (presence of obstacles) for a specific kind of protection device. The user has to choose the device to be installed, for which the related technical features are already reported in the related UML model.

As for the point 4, the user has to interact with the *OM* in order to choose the optimization model and define the related parameters. The choice has to be done on the basis of the designer target.

The usage of the optimization module does not require the knowledge of optimization theory, but the knowledge of the solving approaches used by a commercial solver could allow a faster solution of the proposed ILP models and the overcome of problems related to the size of the problem under investigation.

3.4 Vulnerability Analysis Module (VAM)

The *VAM* module (*VAM*) is in charge of generating and solving qualitative and quantitative formal models for the vulnerability evaluation ("analysis models"). Its input consists of a set of UML models annotated by the CIP_VAM profile and its ultimate goal is to evaluate vulnerability indices and measures. For example, the probability that an intrusion event happens given that it is attempted.

Hence, the module implementation is dependent from the specific formalism adopted to build the model (e.g. Markov chains [7], Bayesian Networks [8], Stochastic or Timed Petri Nets [9], etc.) and from the specific analysis tool used to solve the model ("solvers"). A complete version of *VAM* should:

1. generate analysis models by exploiting model-to-model transformation techniques;
2. allow for sensitivity analysis by varying some meaningful parameters, where this is made possible by the solver and the type of the analysis;
3. solve the analysis models by using proper solvers. Solvers may be available external and third party tools. Hence, wrappers must be able to provide the solvers with the required input and launch their execution;
4. use configuration information to set the proper workflow;
5. provide the user with the results of the evaluation (output of the solver) by updating the UML models or give them back to an user interface;
6. use persistence mechanisms to store models, configurations, results and other artefacts in proper repositories.

4 Enabling Technologies and Tools

Sections 4 and 5 illustrate a prototype tool-chain implementation and provide some hints about the technologies which have been employed. The objective of the prototype is to demonstrate the feasibility and some of the advantages of the approach developed within the METRIP project. It implements a reduced set of the functionalities described in the previous part of the chapter, specifically the core functionalities needed to realize the optimization and vulnerability use cases.

Figure 3 reports a set of technologies and tools that maybe used to implement or instantiate the components of the too-chain.

Papyrus[2] and Visual Paradigm[3] are different alternatives for implementing the CIP_VAM profile into an existing UML-based modelling environment. Visual Paradigm is a complete commercial tool. Papyrus is now part of the Eclipse Modelling Projects; it provides to the user with a full set of tools for model editing,

[2] http://www.eclipse.org/papyrus/.

[3] http://www.visual-paradigm.com/.

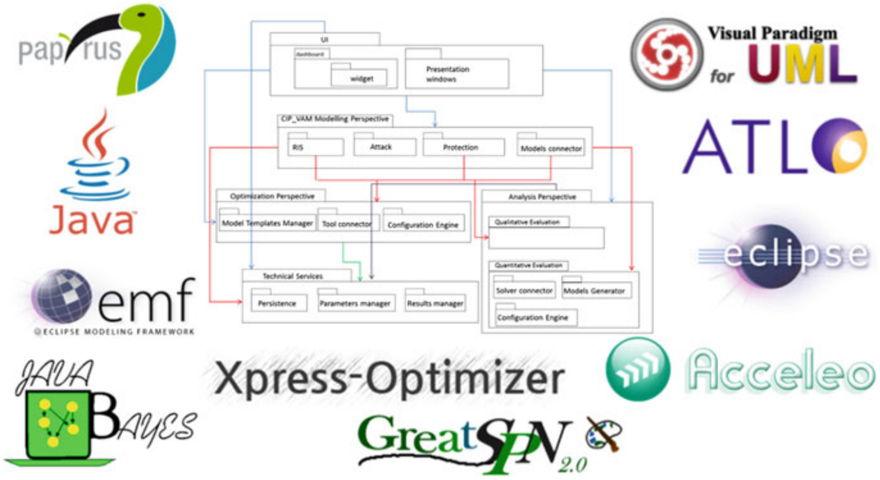


Fig. 3 Technologies and tools

analysis, validation and management. Another part of the Eclipse Modelling Projects is constituted by the Eclipse Modelling Framework (EMF)[4] which aids the software developer by providing tools for a lightweight meta-modelling. Using EMF and Eclipse requires a slight greater effort in the implementation of the user interface because Papyrus and Visual Paradigm specifically address the management and the usage of UML profiles.

A first prototype of the METRIP tool-chain has been built by using Papyrus instead of Visual Paradigm and EMF because of: (1) the availability of a more ready-to-use interface rather than EMF and (2) a tighter integration with other Eclipse toolsets (Acceleo, ATL, EMF) rather than Visual Paradigm.

GreatSPN and JavaBayes are two different examples of existing analysis tools that may be integrated into the chain to perform a quantitative evaluation. GreatSPN[5] is a well-known tool for the analysis of Generalized Stochastic Petri Nets (GSPN). JavaBayes[6] is an implementation of Bayesian networks in Java, which is distributed under the GNU license. The tool-chain may automate the generation of formal models, such as GSPN and BN based models, by means of model transformations from CIP_VAM annotated UML models to the target formalism. The resulting models are solved by using the proper tools (e.g., GreatSPN and JavaBayes).

Xpress Optimizer[7] is a commercial tool that provides a wide set of optimization algorithms for solving large-scale optimization problems. In particular we use Xpress-MP in order to solve the optimal covering/location ILP models [10, 11].

[4] http://www.eclipse.org/modelling/emf/.

[5] http://www.di.unito.it/ ~ greatspn/index.html.

[6] http://www.cs.cmu.edu/ ~ javabayes/Home/.

[7] http://www.fico.com/en/products/fico-xpress-optimization-suite/.

ATL (Atlas Transformation Language) [12] has been adopted to implement model-to-model transformations [13], Acceleo[8] may be used to implement model-to-text transformations. They both are integrated under Eclipse. Hence, Eclipse provides a complete integrated support to the implementation of the prototype tool-chain by means of assessed and widely used technologies available under the Eclipse Public License. For this reason we adopted Eclipse for the development of the prototype.

5 Prototype Implementation

Figure 4 provides a synthetic view of the tool-chain which emphasizes the integration among the components. In practice, *UMLM* is realized by the Modelling Service, by its on-top presentation wizards (Infrastructure, Protection, Attack), and by a part of the ATL transformation service (the one that generates the input file for the *OM*); the *OM* is realized by the Optimization Service and by the Localization Back-end; VAM is realized by the Vulnerability Analysis Service, by a part of the ATL Transformation service (the one that generates the quantitative models) and by the Analysis Back-end. They all use information provided through the Configuration and the Studio wizards.

At the state, the Modelling Service is provided by Visual Paradigm or Papyrus, the Optimization Service is provided by Xpress-MP, the Vulnerability Analysis Service is provided by GreatSPN and JavaBayes but it may be provided by other analysis tools according to type of the vulnerability measures and indices to be evaluated. The ATL transformation service is developed from scratch. It realizes the model generator of the *VAM* module, the generation of the input file for the *OM* module and the update of the functionality which updates the UML models using the obtained results.

The wizards implement: (a) the features needed to generate the configuration information for the optimization and analysis use cases (Config. wizard and Studio wizard in Fig. 4); and (b) an user friendly interface based on graphic elements on top of the Modelling Service.

The Location and Analysis Back-ends realize all the functionalities needed to integrate the above components, i.e. the automation of the workflow, the management of the artefacts and the implementation of the technical services.

[8] http://acceleo.org/.

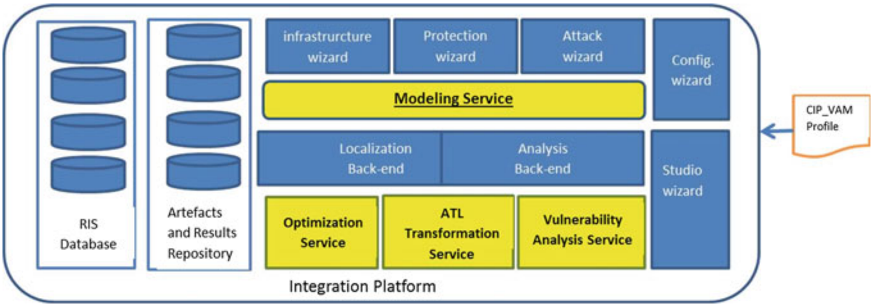


Fig. 4 METRIP tool chain

5.1 *Model Transformations*

The ATL transformation service is in charge of automating the generation of the quantitative analysis models and of the input file to the OM component. In addition, it provides the functionality used to update the UML model with the results obtained by solving the analysis and the optimization models.

It is realized by implementing proper model-to-model (M2M) and model-to-text (M2T) transformations. Indeed, a number of transformations are needed to realize the automation of the generation process. Two different sequences of M2M and M2T transformations have been implemented to generate models and input for the location optimization. These sequences are named *OMD forward transformation chain* and *VAM forward transformation chain*, respectively. Similarly, two backward transformation chains have been implemented in order to process the results files and update the UML model. Figure 5 provides a *specification* of the forward and backward transformation chains which are defined in Chap. 8. In Fig. 5 the sequence from the *CIP_VAM MODEL* to the *Solver/Target tool input file* represents the forward transformation chains, the sequence from *Solver/target tool Output file*

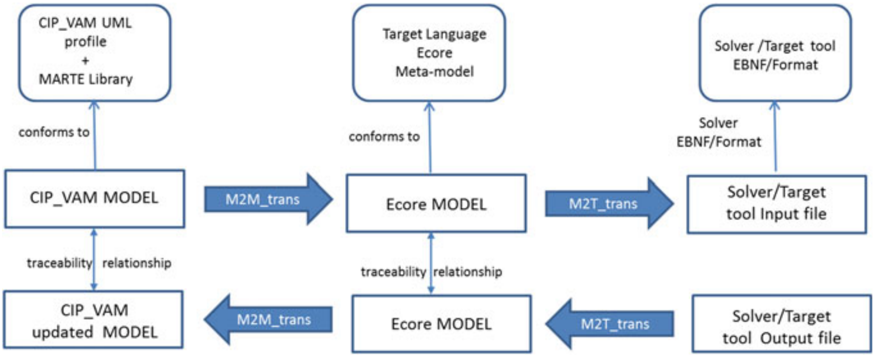


Fig. 5 Forward and backward transformations

to the *CIP_VAM MODEL* represents the backward chains. Here, the meta-models have been instantiated by Ecore. As for the optimization use case, the *Solver/Target tool EBNF/format* specified is the format of the input file required by *OM* (ODM forward transformation chain). It is a plain text file. The *Solver/Target tool Output file* is the file produced by Xpress-MP, which contains the results of the optimization problem, i.e. the localization of the protection devices (ODM backward transformation chain). As for the vulnerability analysis use case, the format of the *Solver/Target tool Output file* depends on what formalism has been used to represent the model and what analysis tool will be employed.

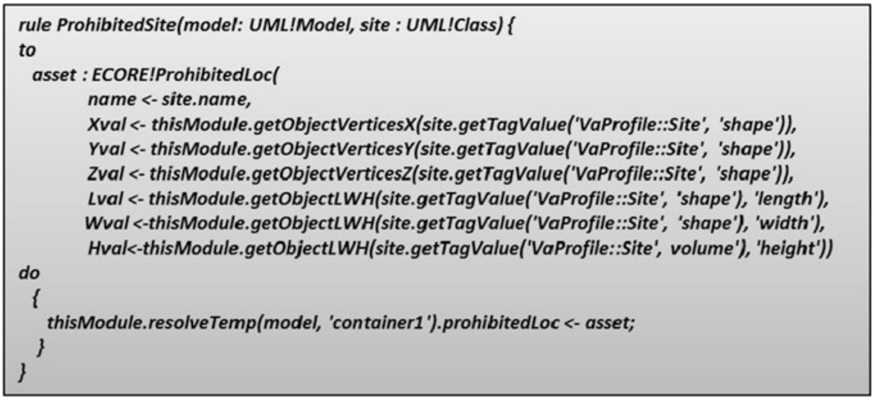
This two-step approach (M2Ms and M2Ts) is necessary in order to cope with the complexity of a transformational process. M2Ms often focus on abstract syntaxes, thus the programming effort is conceptually high (because source and target languages can be very different and belonging to different domains), on the other hand they may ignore low level details. On the contrary, M2Ts have to cope with a richness of details in order to generate models according to the concrete syntax of the used solvers. Hence, the gap between the source meta-model and the abstract syntax of the target concrete language should be as small as possible.

Another key issue in implementing the transformation chains is traceability. Since the CIP_VAM updated model generated from the backward transformation chain is very close to the source CIP_VAM model, the necessity to correctly link the modified/generated UML elements with the existing ones is strong. An example is constituted by the necessity to remember the specific kind of protection devices from the initial CIP_VAM UML model (where they are to allocate) and the final CIP_VAM updated UML model (where single protection devices has been allocated). For example, traceability links are necessary in order to create a <<Sensor>> UML element specifying its location information with the same features (except for the multiplicity) of the former not-allocated <<Sensor>> element.

As explained before, the M2M transformations have been developed in ATL. Some implementations hints are given with reference to the ODM forward transformation chain. It consists of two main "steps" a M2M and a M2T transformation. The M2M transforms a CIP_VAM annotated UML model into an Ecore model conforms to the meta-model reported in Chap. 8. Such meta-model defines the elements for representing the Localization Data (i.e. the input to OM). Two excerpts of this M2M forward transformation are reported below.

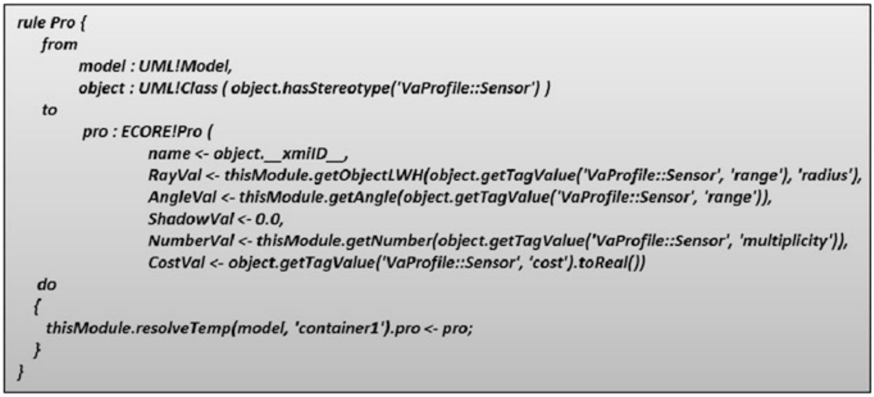
The first snippet in Fig. 6 is an *ATL called rule* which generates information related to the areas of the RIS asset in which sensors must not be placed since they are not allowed. For each UML class annotated with the <<Site>> stereotype, a ProhibitedLoc element of the target model is generated: the value of the EAttributes of the EClass are filled with the values of the tagged values of the <<Site>> stereotype.

The second code snippet reports the *ATL matched rule* that maps the UML model of the protection devices (to be localized) to the Pro EClass of the target language. The protection devices are annotated with the <<Protection>> stereotype. Note that in order to allow traceability between the original UML model and the final updated model, the name of the Pro EClass is set with the xmiID of the UML class (Fig. 7).



```
rule ProhibitedSite(model: UML!Model, site : UML!Class) {
to
  asset : ECORE!ProhibitedLoc(
          name <- site.name,
          Xval <- thisModule.getObjectVerticesX(site.getTagValue('VaProfile::Site',  'shape')),
          Yval <- thisModule.getObjectVerticesY(site.getTagValue('VaProfile::Site',  'shape')),
          Zval <- thisModule.getObjectVerticesZ(site.getTagValue('VaProfile::Site',  'shape')),
          Lval <- thisModule.getObjectLWH(site.getTagValue('VaProfile::Site',  'shape'), 'length'),
          Wval <-thisModule.getObjectLWH(site.getTagValue('VaProfile::Site',  'shape'), 'width'),
          Hval<-thisModule.getObjectLWH(site.getTagValue('VaProfile::Site',  volume'), 'height'))
do
  {
    thisModule.resolveTemp(model, 'container1 ').prohibitedLoc <- asset;
   }
}
```

Fig. 6 Prohibited site called rule–OMDM2M excerpt



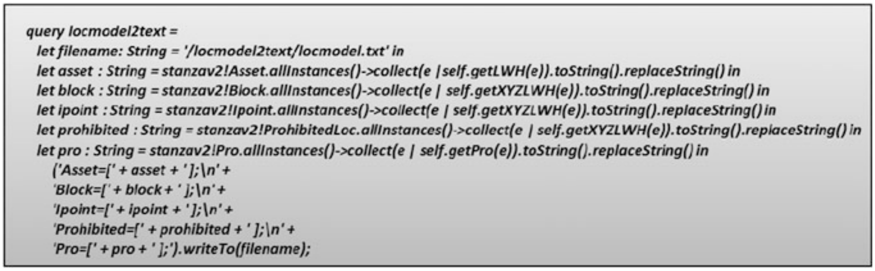
```
rule Pro {
   from
        model : UML!Model,
        object : UML!Class ( object.hasStereotype('VaProfile::Sensor') )
   to
         pro : ECORE!Pro (
                  name <- object.__xmiID__,
                  RayVal <- thisModule.getObjectLWH(object.getTagValue('VaProfile::Sensor', 'range'), 'radius'),
                  AngleVal <- thisModule.getAngle(object.getTagValue('VaProfile::Sensor', 'range')),
                  ShadowVal <- 0.0,
                  NumberVal <- thisModule.getNumber(object.getTagValue('VaProfile::Sensor', 'multiplicity')),
                  CostVal <- object.getTagValue('VaProfile::Sensor', 'cost').toReal())
  do
  {
   thisModule.resolveTemp(model, 'container1').pro <- pro;
  }
}
```

Fig. 7 Protection device matched rule–OMDM2M excerpt

The second transformation (M2T) generates the textual input for the *OM*. It is realized by an *ATL query* and a little portion of this query is reported in Fig. 8.

5.2 User Interface

Papyrus has been used for the creation and editing of CIP_VAM annotated UML models. An exhaustive guide of the Papyrus Eclipse tool is outside of the scope of this report; we will show here some snapshots of the Papyrus framework when creating and editing a CIP_VAM annotated UML model. Figure 9 depicts the user look-and-feel in creating a CIP_VAM model while Fig. 10 focuses on the setting of the tagged values for an element of the UML model stereotyped with the <<Site>> stereotype.



```
query locmodel2text =
  let filename: String = '/locmodel2text/locmodel.txt' in
  let asset : String = stanzav2!Asset.allInstances()->collect(e |self.getLWH(e)).toString().replaceString() in
  let block : String = stanzav2!Block.allInstances()->collect(e | self.getXYZLWH(e)).toString().replaceString() in
  let ipoint : String = stanzav2!Ipoint.allInstances()->collect(e | self.getXYZLWH(e)).toString().replaceString() in
  let prohibited : String = stanzav2!ProhibitedLoc.allInstances()->collect(e | self.getXYZLWH(e)).toString().replaceString() in
  let pro : String = stanzav2!Pro.allInstances()->collect(e | self.getPro(e)).toString().replaceString() in
     ('Asset=[' + asset + ' ];\n' +
     'Block=[' + block + ' ];\n' +
     'Ipoint=[' + ipoint + ' ];\n' +
     'Prohibited=[' + prohibited + ' ];\n' +
     'Pro=[' + pro + ' ];').writeTo(filename);
```

Fig. 8 OMD forward transformation chain-M2T excerpt

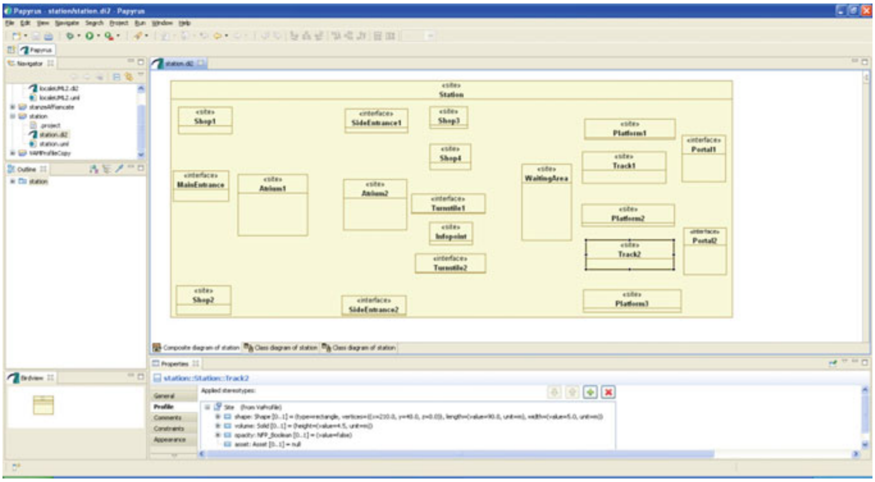
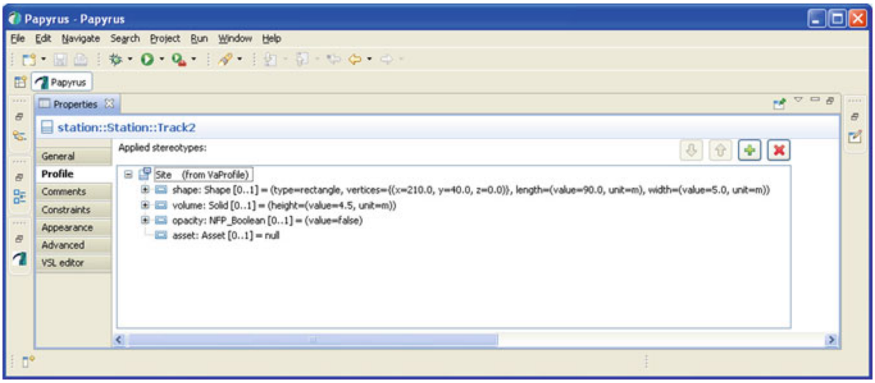


Fig. 9 UML modelling with Papyrus



station::Station::Track2

Applied stereotypes:

```
⊟ Site   (from VaProfile)
   ⊞ shape: Shape [0..1] = (type=rectangle, vertices=((x=210.0, y=40.0, z=0.0)), length=(value=90.0, unit=m), width=(value=5.0, unit=m))
   ⊞ volume: Solid [0..1] = (height=(value=4.5, unit=m))
   ⊞ opacity: NFP_Boolean [0..1] = (value=false)
     asset: Asset [0..1] = null
```

Fig. 10 Setting CIP_VAM tagged values

In order to facilitate the editing as well as the other phases of the METRIP process, a simple graphical console has been also developed in Java. The console provides the user with some functionalities for the management of projects.

A project can be in one of the following states: *NEW*, the initial state in which the model is created on the base of a predefined template; *MODELLED*, the state in which the initial model is edited in Papyrus by pressing the "Edit Project" button; *PROTECTED*, where a PPS has been added to the model by invocating the backend transformation chain after the "Generate PPS" button; *ERROR*, where some errors occur. We recall that the current prototype of the tool-chain only implements a reduced set of functionalities. It mainly realizes the basic features of the *OM* and *VAM* components.

5.3 Localization Back-End

The Optimization Module (*OM*) has been developed using the Eclipse integrated development environment. The generation of the *coverage matrix* (Sect. 3.3) is in charge of the Optimization Back-end. It is built by a Java program.

The optimization models used to define the localization of the protection devices are generated by using the Mosel language of the optimization software Xpress-MP. In the following we will provide some details about their implementations.

Concerning the coverage matrix generation algorithm, for the development of the related Java code, the following main classes have been defined:

- **Room**: this class defines the area to be protected, schematized by a rectangle, by four parameters: length, width and two step size along the x and y axis. The two step size is computed automatically by the OM, as already explained in previous section.
- **Points**: this class defines the list of points of the asset which have to be controlled. These points are defined by two parameters, i.e. the related x and y coordinates with respect to a reference coordinate system with its origin in the bottom left corner of the asset. This class allows also integrating the grid by additional important points and/or the elimination of points for specific constraints in the design of the system.
- **Camera**: this class defines the security device to be used in the design of the security system by three parameters: the coverage ray, the coverage angle and a boolean parameter which defines the possibility of using overlapping positions for the placement of the device.
- **Obstacle**: this class defines the presence of one or more blocks within the asset to be protected. All the obstacles are schematized by a rectangle in two dimensions and are characterized by four values, i.e. the x and y coordinates of the bottom left corner of the block, with respect to the coordinate reference system with the origin in the bottom left corner of the asset under investigation. The other two parameters are the dimensions along the x and y axis.

It is important to underline that the developed algorithm performs a two dimensional analysis. However the modification of the classes to three dimensional case is straightforward and for this reason the information to the third dimension are already considered in the *UMLM*.

Once the coverage matrix has been generated, a specific optimization model is re-called. The ILP file .lp of the optimization models integrated within the OM is obtained by the usage of pre-charged model, written using FICO® Xpress Optimization Suite software. In particular we used the Xpress-Mosel version and the IVE visual development studio on Windows for Xpress-Mosel [10, 11]. The originality of the Mosel language is that there is no separation between a modelling statement (e.g. declaring a decision variable or expressing a constraint) and a procedure that actually solves the problem (e.g. call to an optimizing command). This makes the solution of a complex optimization model much easier and the usage of the integrated optimization tools more straightforward.

6 Conclusions

The protection of critical infrastructures is a very hard problem and only the integration of different skills and competences could allow to effectively solve its main issues.

In this context METRIP approach represents a significant attempt to tackle the problem, with particular reference to the railway infrastructure system, by an interdisciplinary approach involving different computer science fields.

Hence, in this chapter, we showed the integration, within the METRIP prototypal tool, of the three main modules of the METRIP approach, i.e. the UML module (*UMLM*), the Optimization Module (*OM*) and the Vulnerability Analysis Module (*VAM*), presented in Chaps. 8 and 9.

To conclude, it is also important to highlight that the METRIP approach and tool, even if specifically presented for the railway infrastructures, can be easily generalized and applied to other critical infrastructure systems, where the same or similar complex modelling and optimization problem arise.

This possibility of extending their usage to other critical infrastructure systems is made even more concrete by the structure of the METRIP approach and by the architecture of the METRIP tool. Indeed the modular structure of the METRIP approach and the tool-chain at the base of the prototypal tool allows to sequentially and iteratively integrate them with new module and functionalities without the need of completely redesigning them.

Acknowledgments This work is supported by Ansaldo STS under Grant HOME/2010/CIPS/AG/035 METRIP—MEthodological Tools for Railway Infrastructure Protection, financed by the European Commission, Directorate-General Home Affairs, within the Specific Programme on Prevention, Preparedness and Consequence Management of Terrorism and other Security-related risks.

References

1. Schmidt DC (2006) Model-driven engineering. IEEE Comput 39(2):25–31
2. Sendall S, Kozaczynski W (2003) Model transformation: the heart and soul of model-driven software development. IEEE Softw 20:42–45
3. Marrone S, Nardone R, Tedesco A, D'Amore P, Vittorini V, Setola R, De Cillis F, Mazzocca N (2013) Vulnerability modelling and analysis for critical infrastructure protection applications. Int J Crit Infrastr Prot 6 (3–4):217–227. ISSN 1874-5482. http://dx.doi.org/10.1016/j.ijcip.2013.10.001
4. Sforza A, Sterle C, D'Amore P, Tedesco A, De Cillis F, Setola R (2013) Optimization models in a smart tool for the railway infrastructure protection. Lecture notes in computer science, 8328 LNCS, pp 191–196. doi:10.1007/978-3-319-03964-0_17
5. Toregas C, ReVelle C, Swain R, Bergman L (1971) The location of emergency service facilities. Oper Res 19:1363–1373
6. Church R, ReVelle C (1974) The maximal covering location problem. Pap Reg Sci Assoc 32:101–118
7. Trivedi KS (2002) Probability and statistics with reliability, queuing, and computer science applications. Wiley, New York. ISBN 0-471-33341-7
8. Heckerman D, Geiger D, Chickering DM (1995) Learning Bayesian networks: the combination of knowledge and statistical data. Mach Learn 20(3):197–243
9. Peterson JL (1981) Petri net theory and the modelling of systems. Prentice Hall. ISBN 0-13-661983-5
10. FICO$^{\text{TM}}$ Xpress Optimization Suite (2009) Xpress-Optimizer reference manual. Release 20.00
11. Christelle G, Prins C, Sevaux M (2002) Applications of optimization with Xpress-MP. Dash Optimization, Paris
12. Jouault F, Allilaire F, Bézivin J, Kurtev I (2008) ATL: a model transformation tool. Sci Comput Program 72(1–2):31–39
13. Jouault F, Kurtev I (2006) Transforming models with ATL. In: Satellite events at the MoDELS 2005 conference. Springer, pp 128–138

Optimizing Investment Decisions for Railway Systems Protection

Maria Paola Scaparra, Stefano Starita and Claudio Sterle

Abstract As demonstrated by recent events, railway systems are often the target of terrorist bombings and attacks. To preserve public safety and essential economic functions, railroad networks should be made as secure and resilient as possible. However, railway protection investments may involve significant and often unaffordable capital expenditure. Given the limited resources available for protection efforts, it is essential that a strategic approach to the planning of security investments is adopted. This chapter presents a mathematical model for identifying the optimal allocation of protective resources among the components of a railway network. The aim is to minimize the impact on passenger flow of worst-case disruptions which might affect both railway stations and tracks. The proposed model is tested on an Italian railroad network to demonstrate how the model results can be used to inform policy making and protection investment decisions.

1 Introduction

In light of numerous recent terrorist attacks to transportation systems, the issue of protecting critical transportation infrastructures has become a necessity. Railways, in particular, have often been the target of terrorist activity. Examples include the 1995 Paris metro bombing, the 2004 Madrid train bombing, the 2005 London underground suicide attacks, and the 2010 Moscow bombing. These events have demonstrated that rail systems are a crucial yet sensitive component of a nation's

M.P. Scaparra (✉) · S. Starita
University of Kent, Canterbury Kent CT2 7PE, UK
e-mail: M.P.Scaparra@kent.ac.uk

S. Starita
e-mail: ss882@kent.ac.uk

C. Sterle
University of Naples Federico II, Naples, Italy
e-mail: claudio.sterle@unina.it

R. Setola et al. (eds.), *Railway Infrastructure Security*, Topics in Safety, Risk, Reliability and Quality 27, DOI 10.1007/978-3-319-04426-2_11

infrastructure and that disruptions in railroad services can have a significant adverse impact not only on the economy but also on public health and safety.

In some countries like the US, the rail industry and the government have undertaken extensive efforts to protect the movement of freight and passenger trains. Nevertheless, rail security remains an exercise in risk mitigation, as opposed to risk prevention, and protection efforts are mostly undermanned and underfunded [1]. Undoubtedly, railway protection presents some inherent difficulties, due to the specific characteristics of rail systems. First of all, railways are geographically extensive, open and easily accessible infrastructures. As an example, the Italian railroad comprises 16,741 km of operational rail lines, and 2,260 passenger stations. Strengthening all these assets to targeted safety levels may require unacceptable expenditures. In addition, effective security improvements specific to rail transport are difficult to identify and implement. Security mechanisms used by other transportation modes (e.g., aviation passenger screening) cannot be readily applied in the rail environment. Given these difficulties, it is key that protection expenditures are invested wisely in a manner that optimises both service efficiency and public safety.

Railway security can be improved by optimizing the allocation of protection devices within a single asset (e.g., security cameras in a station) but also through a cost efficient allocation of protective resources across the entire railway network. This involves identifying the most critical network components whose loss or temporary closure might have the greatest impact on daily service provision and allocating protection resources among these components so as to make the overall system as robust as possible to external disruptions.

Several quantitative models and analytical approaches have been developed in recent years to identify critical components of and sound protection strategies for distribution and transportation networks. These can be broadly categorized into protection models to counter probabilistic risks and models to counter strategic or premeditated risks [2]. Probabilistic models deal with protection investments against random disruptions (e.g., accidental failures or natural hazards) and imply that the probability of failure of single assets is known or can be estimated, for example through the analysis of historical data or by using domain-specific information provided by structural engineers. Protection models for strategic risks consider protection investments to minimize the impact of worst-case scenario disruptions. These are suitable to model man-made or intentional disruptions (e.g., terrorist attacks or labour union strikes). However, they can be applied to natural disasters as well, if the aim is to protect the system against worst-case scenario losses or if failure probabilities cannot be easily obtained or accurately estimated.

Modeling strategic disruption risks requires emulating the *game* played between a network *attacker* (or *interdictor*) and a network *defender*. Game theory has, therefore, been widely used to model and design defensive strategies against malicious attack. Defender-attacker games can be expressed mathematically as bilevel optimization models where the upper level problem of optimally allocating protection resources has embedded within it a lower-level problem which endogenously generates worst-case scenario losses [3–5].

This chapter considers a bilevel optimization model to deal with security resource allocation in railway systems. We model the rail system as a network of nodes and links, where the nodes represent the stations and the links are the track segments. A limited budget is available for increasing the system security through the protection of nodes and or links. Different security measures can be employed, depending upon the asset to be protected. For example, a link containing a bridge or a tunnel can be protected through monitoring devices or structural reinforcement. A station can be protected by increasing surveillance and patrolling, or installing security cameras. Obviously, different costs are incurred for protecting different components (e.g., protecting a high-traffic commuter station requires significantly more protective resources than protecting a small station or a secondary rail track). Costs also depend on the type of security measure adopted. We assume that a protected component becomes completely invulnerable to possible disruptions. Likewise, if a failure occurs, the affected component becomes completely inoperable and unable to provide service. The aim of the model is to identify a cost-efficient allocation of the available budget so as to minimize the impact of worst-case scenario disruptions to the system. We focus, in particular, on passenger traffic and measure the disruption impact in terms of lost customer flow or demand. More specifically, we assume that if a node or a link fails, traffic must be rerouted through alternative paths on the network. However, detour routes may not exist or be too long from a user point of view. In this case, passengers may resort to different transport modes or abandon the trip all together. The amount of customer flow which is lost provides an indication of the disruption extent. To evaluate the worst-case amount of disrupted flow, we use an adaptation of the flow interdiction model proposed by Murray et al. [6]. A common assumption in interdiction modeling is that there is a limit to the number of components that can be lost simultaneously. Without loss of generality, we also assume that interdiction resources are limited and that the amount of resources needed to disable a component varies according to the component size and topology.

2 Background

The use of network optimization models as a tool for identifying the most vital components of a network dates back several decades (see, for example, the seminal works by [7–9]). Many optimization models, also known as *interdiction* models, have been developed throughout the years to assess the importance and criticality of network components in different settings [10, 11]. These models identify the network links or nodes that, if lost or damaged, have the worst-case impact on system performance. System performance can be measured in a variety of ways, depending upon the topology of the system, the operational protocol in use, and the type of service provided. Typical system performance measures include travel time, connectivity, average throughput or flow, transportation cost, demand coverage, and recovery times among others.

Interdiction models are a useful tool for assessing facility importance and several authors have suggested using the outcome of interdiction models to prioritize protection and or recovery investment efforts [12–14]. However, it can be easily demonstrated that securing those assets that are identified as critical in an optimal interdiction solution does not necessarily provide the greatest protection against malicious attacks [15]. Protection decisions must, therefore, be explicitly captured within a modeling framework to guarantee that security investments are optimized. Optimization models which incorporate protection decisions embed interdiction models to evaluate the worst-case scenario loss in response to each protection strategy.

Most of the protection models existing in the literature have been developed for allocating protection resources among service and supply facilities (e.g., warehouses, distribution centers and power plants) within distribution type networks [5, 16, 17]. Within the transportation literature, only a few papers have addressed the problem of optimizing protection investments among systems components and most of them have dealt with stochastic models to hedge against random disruptions rather than intentional attacks. As an example, Liu et al. [18] propose a stochastic optimization model for allocating limited retrofit resources over multiple highway bridges to improve the reliability of transportation networks. The benefit of retrofit is quantified as savings in reconstruction and travel delay costs. Fan and Liu [19] present a two-stage stochastic model for distributing security resources among road segments so as to minimize total physical and social losses caused by random disasters. Peeta et al. [20] optimize investment decisions for strengthening a highway network. They assume that the network links are subject to random failures due to earthquakes and protection investments reduce failure likelihood. The objective is to maximize the post-disaster connectivity for first responders and minimize the travel time in the surviving network. Miller-Hooks et al. [21] analyze the optimal investment allocation of a fixed budget between preparedness activities (e.g., protection) and recovery activities. They focus on intermodal freight transport networks and measure network resilience as the expected fraction of demand that can be satisfied post-disaster.

To the best of the authors knowledge, the only defender-attacker game- theoretic approach to hedge against intentional disruptions in transportation networks is the one proposed by Cappanera and Scaparra [22]. Their model aims at identifying the set of components to harden in a freight transport network so as to minimize the length of the shortest path between a supply node and a demand node after a worst-case disruption of some unprotected components. Disruption results in traffic delays and network performance is measured in terms of total travel time.

Focusing on protection models specifically designed for railway systems, the literature is even more sparse. Peterson and Church [23] propose a modeling framework for identifying the impact on rail operations when one or more bridges and tunnels are lost. This model is useful for estimating freight rail network vulnerability but does not explicitly identify countermeasures for protection. Perea and Puerto [24] present a model to distribute security resources over a railway network so as to minimize the probability of a successful bombing attack. They provide some theoretical results on the optimal protection strategy but do not propose an efficient solution technique to make the model applicable to real-size rail networks.

In this chapter, we attempt to redress this shortcoming in the literature by proposing a model which allocates security resources among railway network components while taking into account railroad specific properties and performance measures.

3 The Railway Protection Investment Model

To formulate the railway protection investment problem mathematically, we consider a railway network as composed of a set of nodes N (the stations) and a set of arc A (the track segments). We assume that the daily traffic flow between any two stations s and t is known and that, in case of disruption, passengers are willing to use alternative railroad routes only if they are not significantly longer than their normal journey time. We call these routes *acceptable paths* and we compute them in a pre-processing phase. This evaluation is done by comparing each alternative path between an origin and a destination node with the shortest path: all the paths whose length exceeds a given threshold are discarded. The threshold is computed by adding a tolerance parameter to the length of the shortest path.

The other model assumptions can be summarized as follows:

- An interdicted element is excluded from the network.
- Both arcs and nodes can be interdicted. This assumption is made to simulate the disruptions of tunnels, bridges and stations at the same time.
- All the arcs directly linked to an interdicted node are interdicted as well.
- A protected element cannot be interdicted.
- A limited amount of interdiction resources is available.

The mathematical model uses the following notation.

Sets and Indices

N = set of nodes

A = set of arcs

$s \in N$ = index used for flow sources

$t \in N$ = index used for flow destinations

$i \in N$ = index used for network nodes

$j \in A$ = index used for network arcs

f_{st} = traffic demand between s and t

N_{st} = set of acceptable paths that connect s and t

$\beta \in N_{st}$ = index used for network paths

$N(\beta)$ = set of nodes along path β

$A(\beta)$ = set of arcs along path β

q = protection budget (or amount of resources available to the defender)

p = amount of resources available to the attacker

q_i^n = estimate of the amount of resources needed to protect node i

p_i^n = estimate of the amount of resources needed to disrupt node i
q_j^n = estimate of the amount of resources needed to protect arc j
p_j^a = estimate of the amount of resources needed to disrupt arc j

Decision variables:

$$X_i^n = \begin{cases} 1 & \text{if node } i \text{ is disabled} \\ 0 & \text{otherwise;} \end{cases}$$

$$X_j^a = \begin{cases} 1 & \text{if arc } j \text{ is disabled} \\ 0 & \text{otherwise;} \end{cases}$$

$$Y_i^n = \begin{cases} 1 & \text{if node } i \text{ is protected} \\ 0 & \text{otherwise;} \end{cases}$$

$$Y_j^a = \begin{cases} 1 & \text{if arc } j \text{ is protected} \\ 0 & \text{otherwise;} \end{cases}$$

$$Z_{st} = \begin{cases} 1 & \text{if the flow between } s \text{ and } t \text{ is lost} \\ 0 & \text{otherwise;} \end{cases}$$

The railway protection investment model can be formulated as the following bilevel problem:

$$\min_{\mathrm{Y}} \ F(\mathrm{Y}) \tag{1}$$

$$\sum_i q_i^n Y_i^n + \sum_j q_j^a Y_j^a \leq q, \tag{2}$$

$$Y_i^n \in \{0,1\} \quad \forall i \in N, \tag{3}$$

$$Y_j^a \in \{0,\ 1\} \quad \forall j \in A, \tag{4}$$

$$\text{where } F(\mathbf{Y}) = \max_{\mathbf{X}} \quad \sum_s \sum_t f_{st} Z_{st}, \tag{5}$$

$$\text{s.t.} \quad \sum_i p_i^n X_i^n + \sum_j p_j^a X_j^a \leq p, \tag{6}$$

$$X_i^n \leq 1 - Y_i^n \quad \forall i \in N, \tag{7}$$

$$X_j^a \leq 1 - Y_j^a \quad \forall j \in A, \tag{8}$$

$$\sum_{i\in N(\beta)} X_i^n + \sum_{j\in A(\beta)} X_j^a \geq Z_{st} \quad \forall s, t, \beta \in N_{st}, \tag{9}$$

$$X_i^n \in \{0,\ 1\} \quad \forall i \in N, \tag{10}$$

$$X_j^a \in \{0,\ 1\} \quad \forall j \in A, \tag{11}$$

$$Z_{st} \in \{0,\ 1\} \quad \forall s, t \in N. \tag{12}$$

In this leader-follower model the leader chooses the optimal strategy to minimize the objective function F (1), that is the amount of flow that cannot be served after the interdiction. Constraint (2) is the budget constraint: the leader can allocate at most q protection resources among the nodes and arcs of the network. Constraints (3) and (4) are the binary restrictions on the protection variables. The lower level program (5–12) is the interdiction model used to evaluate worst-case losses. The aim of the follower is to choose the attack strategy that maximizes the amount of flow disrupted (5). Constraint (6) is the follower resource constraint: the attacker has at most p resources to interdict the nodes and arcs of the network. Constraints (7) state that protected nodes cannot be disrupted. Similarly, constraints (8) state that protected arcs cannot be disrupted. Constraints (9) state that the flow between s and t can be considered disrupted ($Z_{st} = 1$) only if all the acceptable paths between s and t are disrupted, i.e., at least one of their nodes or arcs is interdicted. If there is at least one acceptable path without interdicted components, the value of the variable Z_{st} is forced to be zero. Finally, constraints (10–12) are binary restrictions on the interdiction and path variables.

4 Solution Methodology

Different methodologies have been used in the literature to solve this type of defender-attacker models. These include: reformulation, dualization, and decomposition [25–27]. To solve the bilevel problem (1–12), we used a decomposition method based on super valid inequalities. Namely, the bilevel model is split into two interlinked subproblems: an upper level protection master problem, and a lower level interdiction subproblem. Each protection strategy identified by the master problem is fed into the subproblem to determine an optimal interdiction plan. Special cuts, called super valid inequalities (SVI), are then generated based on the solution to the interdiction problem and added to the master problem, which then computes a new protection strategy. The process is iterated until a sufficient number of SVIs has been added to make the protection problem unfeasible. This approach had been previously used to solve a two-level protection model in Losada et al. [28].

The decomposition algorithm was implemented in C++ inside the Visual Studio environment. At each iteration, both the master problem and the sub-problem were solved using the IBM ILOG optimization software Cplex 12.5.

5 Case Study and Analysis

To demonstrate the practical applicability of our approach, we applied the model to the railway network infrastructure of Campania, a region in Southern Italy. The region Campania is populated by almost 6 million people, making it the second-most-populous region of Italy. Its capital city is Naples. The railway network under consideration is composed by a primary network which connects major cities in Italy and has high traffic (high speed and inter-regional rail services), a secondary network which connects an highly populated urban centre to outer suburbs (Cumana, Circumlfegrea, Circumvesuviana and north-east metro services), and some complementary lines which connect small regional centres. The overall network is depicted in Fig. 1. The network has 26 nodes, corresponding to cities and towns in the region, and 37 arcs.

In the absence of real data on passenger traffic between pairs of stations, we have generated estimates of the origin-destination flows as a function of the size of the connected cities, and the frequency and capacity of the trains operating on the

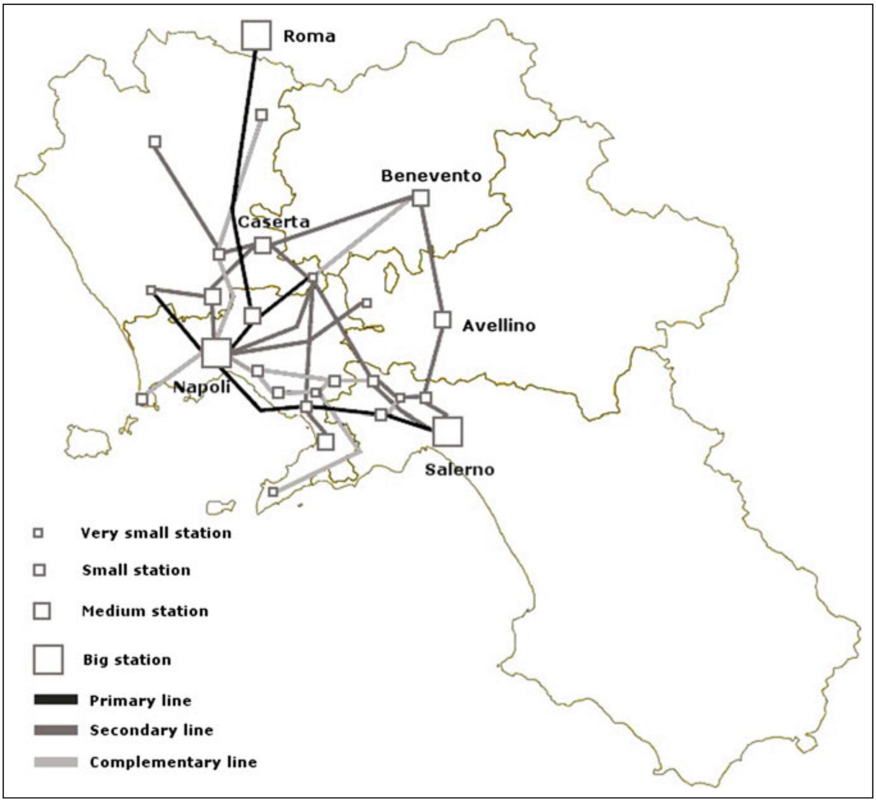


Fig. 1 Campania rail network

network. We assumed that disrupting an arc requires one unit of resource ($p_j^a = 1$), whereas the cost of protecting an arc, q_j^a, depends upon the number of tunnels and bridges along the arc. We do not consider the protection of arcs without tunnels or bridges. To generate realistic values for the interdiction and protection resources associated with the nodes (q_i^n and p_i^n), we have divided the stations in four groups according to their dimension. The values chosen for the stations in each group are shown in Table 1. Obviously, bigger stations require more resources to be protected/disrupted. As an example, Caianello is a very small station and only requires 2 units, whereas Naples is the biggest station and requires 12 units.

In our empirical study, we have analyzed and compared protection strategies to hedge against disruptions of different magnitudes. Specifically, we considered small, medium, large and very large disruptions. The amount of interdiction resources associated with each event size are displayed in Table 2. With this choice, a small disruption can only affect a very small station, whereas a very large event is able to interdict a big station and a few other smaller assets.

The analysis also considers different budget levels. These were chosen as a percentage of the budget needed to protect the whole network.

Some preliminary results are displayed in Table 3, which shows the total amount of flow which is lost in different disruption scenarios and for different protection investment levels. It can be seen that even a small disruption can have a considerable impact on traffic flow if protective measures are not carried out: the worst-case loss

Table 1 Resources needed to protect/interdict a node

Node dimension	Interdiction/protection resources
Very small	2
Small	4
Medium	8
Big	12

Table 2 Disruption scenarios

Size	Resource units
Small	2
Medium	5
Large	10
Very large	20

Table 3 Percentage of lost flow for different disruption scenarios and protection budget levels

	No protection	1 %	5 %	10 %
Small	38	18	10	5
Medium	67	39	20	16
Large	88	75	35	28
Very large	98	96	77	54

after a small disruption can result in a loss of 38 % of the total flow. This can reach 67, 88 and 98 % for medium, large, and very large disruptions respectively. The effect of protecting even as little as 1 % of the assets can be considerable, if protection resources are allocated optimally. This is true especially for small and medium size disruption scenarios, where the total losses can be reduced from 38 to 18 % for small events and from 67 to 39 % for medium events. For large and very large events, greater protection investments are needed to get significant reductions in flow losses. As an example, an optimal investment equal to 5 % of the protection cost of the total network, can more than halve the flow loss resulting from a large disruption (from 88 to 35 %).

To provide a better understanding of how increasing budget levels may affect the system losses in case of disruption, in Fig. 2 we show the percentage marginal reduction in flow losses for each percentage point increase in protection resources. We let the budget vary between 1 and 10 % of the protection cost of the whole network.

This analysis sheds light on possible tradeoffs between protection expenditures and flow loss reductions in case of worst-case system disruptions. As an example, if a large disruptive event is considered, a 1 % investment results in a worst-case loss reduction of about 15 % (first segment of the third bar in the chart). However, if an investment of 2 % can be made, the benefit is more than doubled, bringing an additional 25 % flow loss reduction and an overall reduction of 40 %.

The differences between the four disruption scenarios can be further analyzed through the graphs plotted in Figs. 3, 4, 5 and 6. For each scenario, the corresponding graph displays the contribution of a percentage point increment in protection resources on the overall objective improvement.

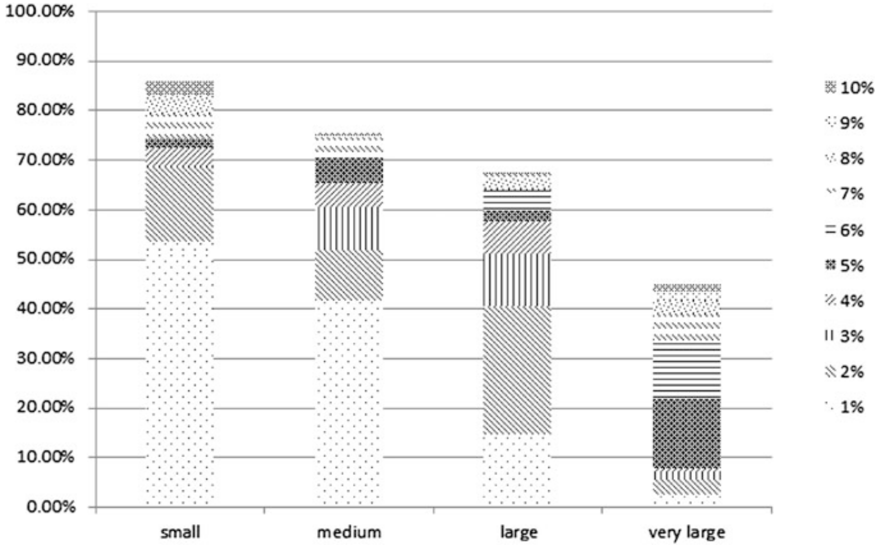


Fig. 2 Marginal percentage decrease in flow loss due to percentage point increments of the protection budget

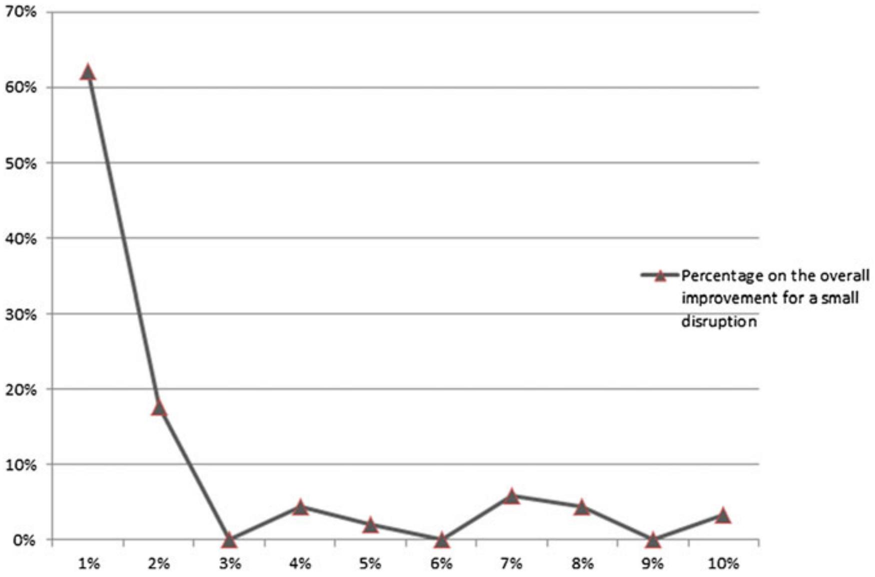


Fig. 3 Analysis of the contribution of percentage point increases of the protection resources on the overall improvement for small disruptions

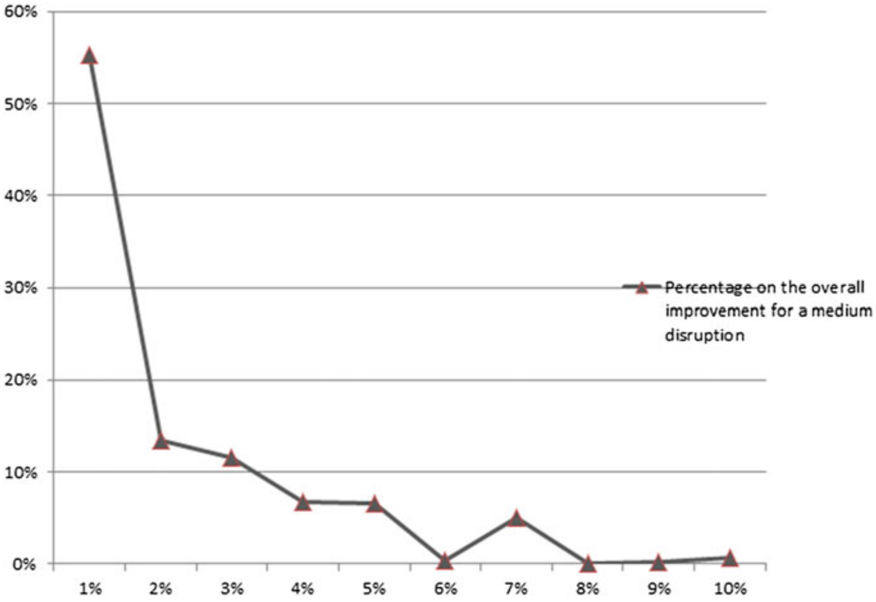


Fig. 4 Analysis of the contribution of percentage point increases of the protection resources on the overall improvement for medium disruptions

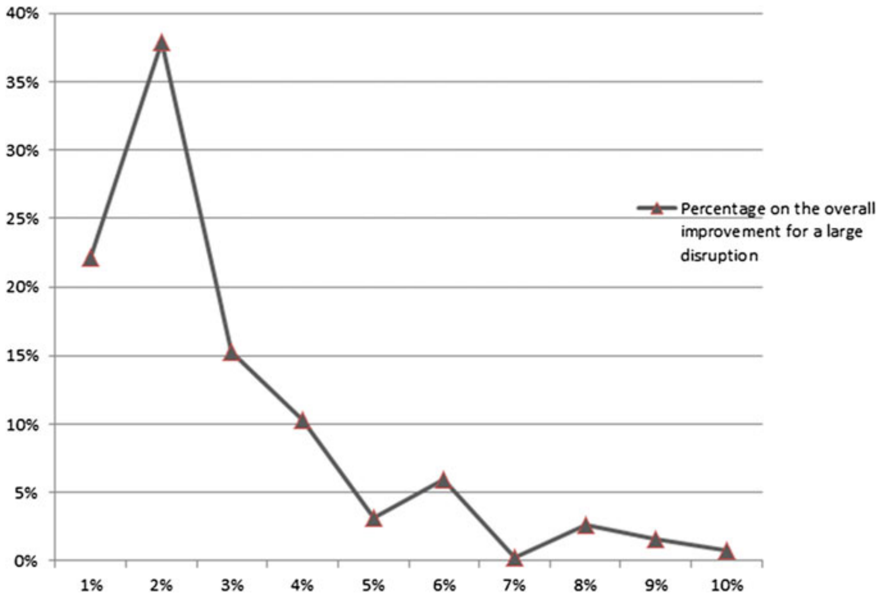


Fig. 5 Analysis of the contribution of percentage point increases of the protection resources on the overall improvement for large disruptions

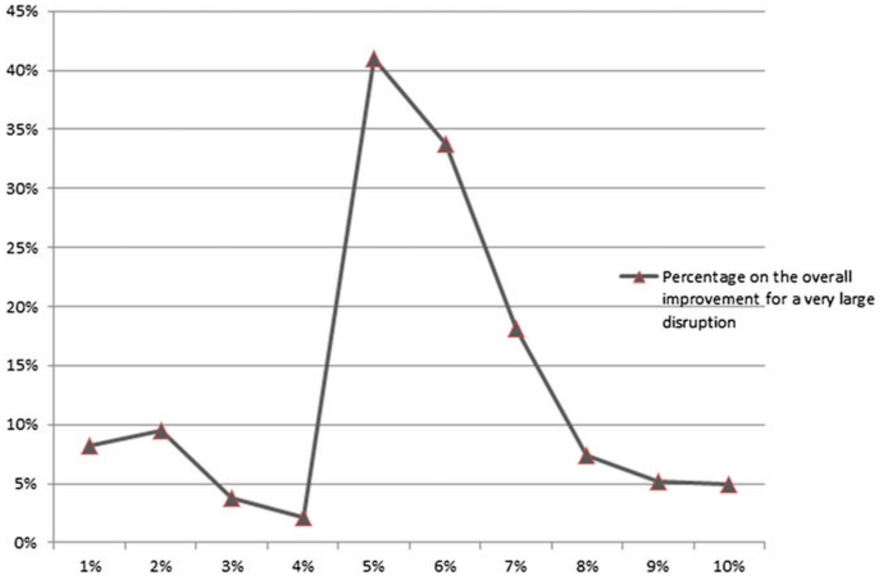


Fig. 6 Analysis of the contribution of percentage point increases of the protection resources on the overall improvement for very large disruptions

The first clear difference is that in the scenarios with low and medium level disruptions (Figs. 3 and 4) the first percentage point increase is responsible for more than half of the overall benefit. To reach similar results for large disruptions, a two point increment is needed (Fig. 5). When very large disruptions are considered, the first few increments have a somewhat limited effect on reducing flow losses whereas a peak can be noticed in correspondence of a 5 % investment (Fig. 6). An additional percentage point increase, results in another significant flow loss reduction. This seems to indicate that if large disruptions are anticipated, a protection budget in this range (5–6 % of the total protection costs) should be warranted to maximize the benefits of security investments.

It is clear that the protection strategies identified by the model may differ quite significantly, depending on the magnitude of the disruption given in input to the model (parameter p). Our next analysis aims at identifying protection plans which are robust across all scenarios, so as to hedge against the uncertainty characterizing the size and extent of disruptive events. To this end, we evaluate how the optimal solution identified for a given disruption size performs in all the other scenarios.

The results of this analysis are shown in Tables 4 and 5 for two budget levels, equal to 5 and 10 % of the resources needed to protect the whole network. These cases correspond to values of q equal to 17 and 35 respectively. The tables show the percentage flow loss increase which is observed when the optimal protection strategy computed for a given scenario (*supposed scenario*) is used in a different scenario (*actual scenario*). The last two columns display the maximum and average increase across all the other scenarios. From the analysis of Table 4 ($q = 17$), it is clear that the

Table 4 Cross-comparison of different optimal protection plans

Supposed scenario	Actual scenario				MAX (%)	AVG (%)
	Small (%)	Medium (%)	Large (%)	Very large (%)		
Small	0	98.8	75.2	20.3	98.8	48.6
Medium	21.8	0	0	22.5	22.5	11.1
Large	21.8	0	0	22.5	22.5	11.1
Very large	133.8	104	78.1	0	133.8	79

Relative flow loss increase in percentage. *Case* q = 17

Table 5 Cross-comparison of different optimal protection plans

Supposed scenario	Actual scenario				MAX (%)	AVG (%)
	Small (%)	Medium (%)	Large (%)	Very large (%)		
Small	0	138.4	106.3	74.8	138.4	79.9
Medium	85.7	0	8.6	71.6	85.7	41.5
Large	98.1	3.2	0	74	98.1	43.8
Very large	126.1	19.9	19.7	0	126.1	41.4

Relative flow loss increase in percentage. *Case* q = 35

Table 6 Optimal protection plans for different disruption scenarios and different protection budgets

Disruption size	Protection resources			
	q = 1 %	q = 2 %	q = 5 %	q = 10 %
Small	Naples-Barra Naples-Afragola	Naples-Barra Naples-Afragola T.Annunziata-C.Stabia	Torregaveta-Naples Naples-Afragola Naples-Barra S.Maria C.V.-Caserta T.Annunziata-C.Stabia T.Annunziata-Nocera	Torregaveta-Naples Rome-Afragola Naples-Afragola Naples-Barra Naples-T.Annunziata T.Annunziata-C.Stabia T.Annunziata-Nocera
Medium	Naples-Barra T.Annunziata-C.Stabia	Barra Naples-Barra T.Annunziata-C.Stabia	Barra T.Annunziata Naples-Aversa Naples-Afragola Naples-Barra Naples-T.Annunziata T.Annunziata-C.Stabia T.Annunziata-Nocera	Barra T.Annunziata S. Giorgio a C. Torregaveta-Naples Naples-Aversa Naples-Afragola Naples-Barra Naples-T.Annunziata S.Maria C.V.-Caserta S. Giorgio a C.-T.Annunziata O. T.Annunziata-C.Stabia T.Annunziata-Nocera
Large	Naples-Barra T.Annunziata-Nocera	Barra Naples-Afragola Naples-Barra	Barra T.Annunziata Naples-Aversa Naples-Afragola Naples-Barra Naples-T.Annunziata T.Annunziata-C.Stabia T.Annunziata-Nocera	Barra T.Annunziata S. Giorgio a C. Torregaveta-Naples Naples-Aversa Naples-Afragola Naples-Barra Naples-T.Annunziata Barra-P.Marino T.Annunziata-C.Stabia T.Annunziata-Nocera T.Annunziata O.-P.Marino

(continued)

Table 6 (continued)

Disruption size	Protection resources			
	$q = 1$ %	$q = 2$ %	$q = 5$ %	$q = 10$ %
Very large	Naples-Afragola Sarno-Codola	Naples-Aversa S.Maria C.V.-Caserta T.Annunziata-C.Stabia T.Annunziata-Nocera	Naples Barra Naples-Barra	Naples Barra T.Annunziata Nocera Naples-Aversa Naples-Afragola Naples-Barra Naples- T.Annunziata T.Annunziata-C.Stabia T.Annunziata-Nocera Nocera-Codola Sarno-Codola

Table 7 Post-protection worst-case losses in different disruption scenarios and for different protection budgets

Disruption size	Protection resources			
	$q = 1$ %	$q = 2$ %	$q = 5$ %	$q = 10$ %
Small	Rome-Afragola T.Annunziata-C.Stabia	Rome-Afragola Naples-T.Annunziata	Rome-Afragola Sorrento-T.Annunziata O.	Naples-S.Maria C.V. S.Maria C.V.
Medium	Barra P.Marino-Sarno	V.Literno-Naples Rome-Afragola Naples-Aversa Aversa-Caserta T.Annunziata-C.Stabia	Torregaveta-Naples Rome-Afragola Barra-P.Marino S.Giorgio a C.-T.Annunziata O. P.Marino-Sarno	Nocera Rome-Afragola
Large	Barra Torregaveta-Naples Naples-Afragola S.Maria C.V.-Caserta Afragola-Cancello T.Annunziata-C.Stabia Naples-T.Annunziata P.Marino-Sarno	Cancello V.Literno-Naples Torregaveta-Naples Naples-Aversa Barra-P.Marino S.Maria C.V.-Caserta T.Annunziata-Nocera P.Marino-Sarno	Cancello Torregaveta-Naples Rome-Afragola Rome-Afragola Aversa-Caserta T.Annunziata-C.Stabia Naples-T.Annunziata S.Giorgio a C.-T.Annunziata O. Nocera-Codola Nocera-Salerno	S.Giorgio a C. Rome-Afragola S.Maria C.V.-Caserta
Very large	Naples Cancello S.Maria C.V.-Caserta Caserta T.Annunziata-C.Stabia Nocera-Codola Nocera-Salerno Mercato-Salerno	Naples Cancello Nocera Aversa-Caserta Mercato-Salerno	Cancello S.Giorgio a C. V.Literno-Naples Torregaveta-Naples Naples-S.Maria C.V. Naples-Aversa Naples-Afragola Naples-T.Annunziata S.Maria C.V.-Caserta Aversa-Caserta Barra-P.Marino T.Annunziata-C.Stabia P.Marino-Sarno Nocera-Codola Nocera-Salerno Mercato-Salerno	Cancello S.Giorgio a C. Afragola Aversa-Torregaveta-Naples S.Maria C.V.-Caserta Aversa-Caserta Barra-P.Marino P.Marino-Sarno Nocera-Salerno

optimal solution for medium and large events is the same. It is also the solution that works better across the different scenarios, with an average error of 11.1 % and a maximum error of 22.5 %. In the second case (Table 5), all the solutions are different and the best choice, in terms of average percentage increase of disrupted flow, is the optimal protection strategy computed for very large disruptions. Nevertheless, assuming a medium size disruption may result in a better compromise solution: the average percentage increase is really close to the one obtained for very large events (41.5 vs. 41.4 %) but the maximum value is considerably smaller (85.7 vs. 126.1 %). Overall this analysis indicates that the assumptions made on the disruption size may have a significant impact on the identification of effective protection strategies. In general, avoiding the extreme cases and assuming medium to large disruptions leads to the most robust defensive plans.

Finally, in Tables 6 and 7 we display the solutions to the model for different disruption scenarios and protection budget levels. Table 6 shows the network components chosen for protection, whereas Table 7 shows the interdiction plans (i.e., the worst-case losses) after protection.

We can see that Afragola and Barra appear quite often in the protection and disruption strategies. This can be explained by noticing that the first station is a crucial node of the high speed service and its disruption affects the connection between Rome and Naples; the second station belongs to the Circumvesuviana railway network and intercepts a huge portion of the traffic generated by that service. It is interesting to note that Cancello appears very frequently among the components to be interdicted, in spite of being a very small station. This may be due to its very central position. Cancello, in fact, intercepts the flow between the largest cities of the region and this makes it an attractive target for an intelligent attacker. Finally, it can be noted that Naples only appears in a few solutions probably because, although it is the most important station, is also the most difficult and expensive asset to protect and or disrupt.

6 Conclusions and Discussion

To increase railway system security, it is crucial that scarce protection resources are allocated across the network assets in the most cost-efficient way. This chapter has presented an optimization model for the strategic planning of protection investments. The proposed model identifies the optimal allocation of defensive resources to hedge against worst-case scenario flow losses due to malicious attacks. We have demonstrated how the model results can be used to identify the optimal investment level to achieve a desirable degree of protection, and highlighted possible trade-offs between protection expenditure and traffic flow preserved. Finally, we have shown how to select robust solutions that perform well under disruptive scenarios of different magnitude.

The proposed model can be extended in several ways to capture additional realism and the complexities characterizing railway systems. As an example, our model objective is to minimize the amount of passenger flow which is lost after a disruption. Other performance measures could be considered which combine both system cost and customer disutility into a multi-objective model. These measures should include issues such as delays, increased travel time and duration of the disruption. We also made the assumptions that protected components are completely immune to failure and that attacks on unprotected components are always successful. Other modeling frameworks should be developed to model different degrees of protection and interdiction. For example, partial protection could be considered where protected components only preserve part of their operational capabilities or have shorter recovery times or smaller failure probabilities depending on the level of protection investment.

References

1. Hartong M, Goel R, Wijesekera D (2008) Security and the US rail infrastructure. Int J Crit Infrastruct Prot 1:15–28
2. Golany B, Kaplan EH, Marmur A, Rothblum UG (2009) Nature plays with dice—terrorists do not: allocating resources to counter strategic versus probabilistic risks. Eur J Oper Res 192:198–208
3. Brown G, Carlyle M, Salmeron J, Wood K (2006) Defending critical infrastructure. Interfaces 36:530–544
4. Liberatore F, Scaparra MP, Daskin M (2012) Optimization methods for hedging against disruptions with ripple effects in location analysis. Omega 40:21–30
5. Scaparra MP, Church RL (2008) A bilevel mixed integer program for critical infrastructure protection planning. Comput Oper Res 35:1905–1923
6. Murray AT, Matisziw TC, Grubesic TH (2007) Critical network infrastructure analysis: interdiction and system flow. J Geogr Syst 9:103–117
7. Corley HW, Sha DY (1982) Most vital links and nodes in weighted networks. Oper Res Lett 1:157–160
8. Golden B (1978) A problem in network interdiction. Naval Res Logist Q 25:711–713
9. Wollmer R (1964) Removing arcs from a network. Oper Res 12:934–940
10. Church RL, Scaparra MP, Middleton RS (2004) Identifying critical infrastructure: the median and covering facility interdiction problems. Ann Assoc Am Geogr 94:491–502
11. Wood KR (1993) Deterministic network interdiction. Math Comput Model 12:1–18
12. Matisziw TC, Murray AT (2009) Modeling s-t path availability to support disaster vulnerability assessment of network infrastructure. Comput Oper Res 36:16–26
13. Salmeron J, Wood K, Baldick R (2004) Analysis of electric grid security under terrorist threat. IEEE Trans Power Syst 19:905–912
14. Ukkusuri SV, Yushimito WF (2009) A methodology to assess the criticality of highway transportation networks. J Transp Secur 2:29–46
15. Church RL, Scaparra MP (2007) Protecting critical assets: the r-interdiction median problem with fortification. Geog Anal 39:129–146
16. Aksen D, Aras N, Piyade N (2013) A bilevel p-median model for the planning and protection of critical facilities. J Heuristics 19:373–398
17. Bricha N, Nourelfath M (2013) Critical supply network protection against intentional attacks: a game-theoretical model. Reliab Eng Syst Saf 119:1–10
18. Liu C, Fan Y, Ordez F (2009) A two-stage stochastic programming model for transportation network protection. Comput Oper Res 36:1582–1590

19. Fan Y, Liu C (2010) Solving stochastic transportation network protection problems using the progressive hedging-based method. Netw Spat Econ 10:193–208
20. Peeta S, Salman FS, Gunnec D, Viswanath K (2010) Pre-disaster investment decisions for strengthening a highway network. Comput Oper Res 37:1708–1719
21. Miller-Hooks E, Zhang X, Faturechi R (2012) Measuring and maximizing resilience of freight transportation networks. Comput Oper Res 39:1633–1643
22. Cappanera P, Scaparra MP (2011) Optimal allocation of protective resources in shortest-path networks. Transp Sci 45:64–80
23. Peterson SK, Church RL (2008) A framework for modeling rail transport vulnerability. Growth Change 39:617–641
24. Perea F, Puerto J (2013) Revisiting a game theoretic framework for the robust railway network design against intentional attacks. Eur J Oper Res 226:286–292
25. Bard JF (1998) Practical bilevel optimization. Kluwer Academic Publishers, Boston
26. Dempe S (2002) Foundations of bilevel programming. Kluwer Academic Publishers, Dordrecht
27. Gümüş ZH, Floudas CA (2005) Global optimization of mixed-integer bilevel programming problems. CMS 2:181–212
28. Losada C, Scaparra MP, O'Hanley JR (2012) Optimizing system resilience: a facility protection model with recovery time. Eur J Oper Res 217:519–530

The Security into the Metro System: The Copenhagen Metro Experience

Klaus Hestbek Lund, Annarita Tedesco and Michele Bigi

Abstract The security threats for Mass Transit Transportation Systems (MTTSs) in railway infrastructure systems, originate from a multiplicity of threat sources and constantly increase, both in terms of frequency and gravity. Cityringen, the new metro line of Copenhagen, is a fully automated metro in the heart of the city. It has been designed and planned in order to satisfy the main security requirements in MTTSs using both vulnerability analysis and risk assessment activities. This chapter describes criteria and options selected to equip stations and vehicles with state of the art passenger safety and security systems, including dynamic passenger information displays, call-points and high quality live video surveillance systems, and to manage crises situations.

1 Introduction

In this chapter, the issues concerning the development of a Passenger Security System (PSS) in the experience of the Copenhagen Metro System will be addressed.

For a comprehensive understanding about the topic, a deep analysis about the main threats for a Metro system or for a transportation system in general, must be taken into account. Observations and considerations in the Railway Infrastructure Systems scenario are usually very general and can be applied to different application domains. Nevertheless, it is important also to understand the specific society and how community weights the perennial conflict between security versus privacy.

K.H. Lund · M. Bigi (✉)
Metroselskabet, Metrovej, 2300 København S, Denmark
e-mail: MIB@m.dk

K.H. Lund
e-mail: KHL@m.dk

A. Tedesco
Ansaldo STS, Naples, Italy
e-mail: annarita.tedesco@ansaldo-sts.com

R. Setola et al. (eds.), *Railway Infrastructure Security*, Topics in Safety, Risk, Reliability and Quality 27, DOI 10.1007/978-3-319-04426-2_12

It is also worth to mention the increased need for a security system in the Mass Transportation System at the light of the last 15 years events. Different countries react in different way to this escalation of threats, often increasing of the prevention of threats and increasing the security level of the mass transportation system as well.

In the specific experience, the Danish society is well known as a culture where privacy of the single person is considered at the top of the scale of the civil rights. As said there is always a trade-off between security and privacy. Anyhow different solution can be done in order to decrease the level of feeling of be observed and still keep a good security level. In the specific case a huge effort has been used in the integration of cameras or visible devices in the stations.

Another aspect of the security is how to grant a certain feeling of security to passenger. Many requirements have been pointed on the coverage of stations and the vehicles. Beside the discrete but constant presence of cameras, perception of security has been taken in account within the architectural solution. Keep all the zones as safe as possible, with proper illumination, avoiding hidden areas, privileges of open airy ambient and so on. An intrinsically safety built in the station can have a huge impact in the privacy feeling for passenger and in the security level perceived by passengers.

At last, in the specific Copenhagen Metro driverless Metro, the security has been taken in consideration in the operational phase as well, grants with a proper coverage of personal moving around the Metro in the stations and vehicles, during all the 24 h duty. Moreover, the Personal Security operator will have intelligent video surveillance helping him to monitor the many different sites, spotting automatically the more delicate situation.

2 The Threats

In recent years Mass Transit Agencies around the world are facing with considerable challenges when addressing the issue of security threats. These security threats, originating from a multiplicity of threat sources—are constantly increasing both in terms of frequency and gravity.

The sources of the threats could be divided into 3 main categories:

- Crime
- Public Disorder
- Terrorism

Each of the threats sources should be developed into a list of hostile activity tactics relevant to the particular transit system.

When considering possible hostile activities scenarios the following basic assumptions are applied:

The adversary shall try to inflict as much damage as possible by targeting the most critical assets.

The potential damage of a hostile activity is maximal in relation to the specific threat. Meaning that the adversary shall carry the hostile activity at most favorable location and time to inflict the most damage.

The adversary shall try to minimize the possibility that he will be detected prior and after carrying out the hostile activity.

The threat is one of the components in the process of risk assessment and the model used for ranking the hostile activities scenarios (threats) is based on the following elements:

Attractiveness—the attractiveness model is usually based on the weighting of the following parameters, which influence tactic attractiveness:

- Harm to people;
- Damage to equipment and infrastructure;
- Disruption of operations;
- Accessibility—the adversary's accessibility to the asset.

Deterrence or visible security—the model takes into consideration the influence of deterrence measures on the adversary's intent to carry out the hostile activity.

Capability—the adversary's capability to carry out the hostile activity in the chosen scenario in terms of operational capability.

The threat definition is changing between countries and cities all over the world, usually influenced by political and socio-economic factors.

Selected common Applicable Scenarios in mass transit systems are presented in the Table 1.

Table 1 Possible threat scenarios for a Mass Transit Transportation System

Threat source	Tactic/Action
Crime	Pick pocketing
	Graffiti
	Vandalism
Public disorder	Riding without paying
	Violence
	Hooliganism
	Drunkenness
Terror	IED (Improvised Explosive Device)
	Car bomb
	Attack with fire arms
	Spreading of dangerous substances
	Suicide bomber
	Attack with "cold weapons" (axe, knife)
	Hostage taking

3 The Vulnerabilities

Vulnerability Analysis involves the evaluation of the adversary's chances of realizing a chosen threat scenario against the system.

Vulnerability analysis identifies weakness in the design, security, operational, and management elements of the system that may support the likelihood that an evaluated threat will result in harm.

The vulnerability of each asset is evaluated according to security controls in place to mitigate each scenario, and on a probabilistic evaluation of the security system's effectiveness against the chosen scenario in terms of deterrence, detection, delay, prevention and response.

Vulnerabilities are evaluated according to the following topics:

- Security policy and procedures;
- Security systems and means;
- Management of security.

The security activity of front line employees and security personnel.

The probability of occurrence of hostile activity is determined by combining the threat ranking for each hostile activity scenario with the vulnerability ranking associated with each hostile scenario.

The probability of occurrence, together with the **consequences analysis** creates the components of the **Risk Assessment**. The performance of Risk Assessment is crucial and fundamental and should be executed prior to any selection and implementation of countermeasures.

4 Metro Copenhagen

Cityringen shall be a fully automated driverless metro ring line under the central part of Copenhagen. The alignment will cover important city areas as illustrated in Fig. 1.

The project is under construction with forecast opening 2019, it is a new Metro path which will enlarge the first Metro opened in 2002. The line shall consist of two single track tunnels each approximately 16 km in length, 17 underground stations with island platforms, 3 crossover facilities and 3 construction and ventilation shafts. In addition, Cityringen will include an automated control and maintenance centre (south of the line) at Vasbygade built for operation and maintenance of the system.

Cityringen will have 2 line, M3 and M4, and shall be fully independent of the existing metro (line M1 and M2). Cityringen shall operate 24 h/7 days a week with a planned operational headway of approximately 100 s. During rush hours in the first years of operation. Cityringen is expected to serve up to 240,000 passengers per day or 72 million passengers per year.

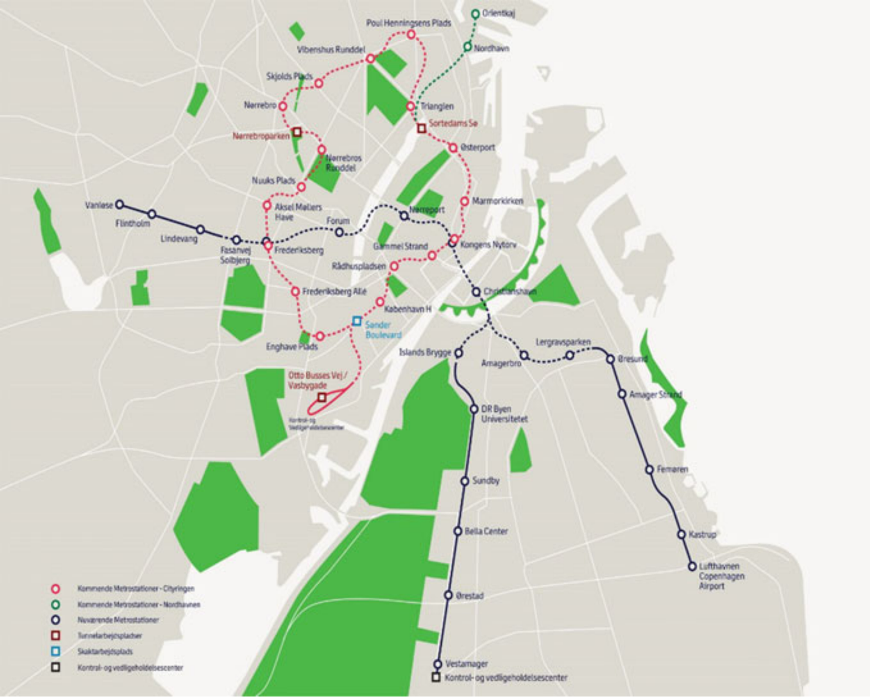


Fig. 1 Cityringen map (*red path*) and existing metro (*blue path*)

Cityringen shall be operating in two modes on shared tracks: M3 and M4. M3 is a circular line (in both directions) whereas M4 is a pendulum line between Nordhavn (future extension) and København H (Main station).

Cityringen shall have transfer facilities to the existing metro stations at Kongens Nytorv and Frederiksberg. Further transfer facilities will be provided connecting to the existing regional railway stations at København H station, at Østerport Station and at Nørrebro Station.

Where possible, the stations shall be daylight lit structures of high architectural quality. All platforms shall be provided with Platform Screen Doors and served by stairs, escalators and lifts.

Stations and vehicles shall be equipped with state of the art passenger safety and information systems including dynamic passenger information displays, call-points and high quality live video surveillance systems (Fig. 2).

The Passenger Vehicles shall consist of 28 3-car articulated trains of approximately 39 m in length, a width of 2.65 m and a floor height of 0.81 m. The trains shall run on steel wheels on steel rails. The trains shall be comfortable with floors at platform level. Materials shall meet high qualitative and aesthetic requirements with high fire resistance and be “fit for purpose” for the expected use.

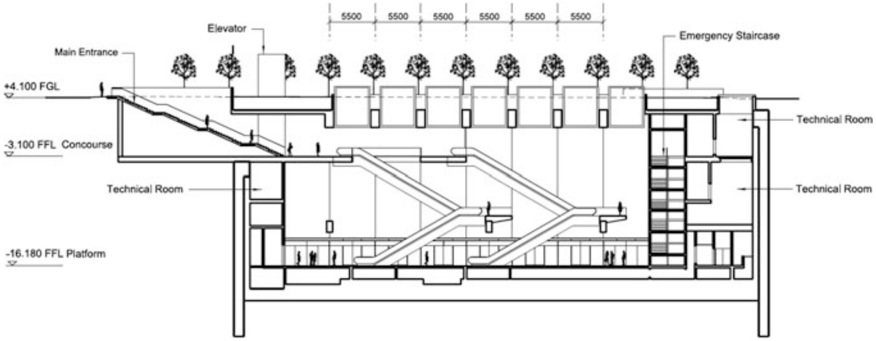


Fig. 2 Cross station of a typical station

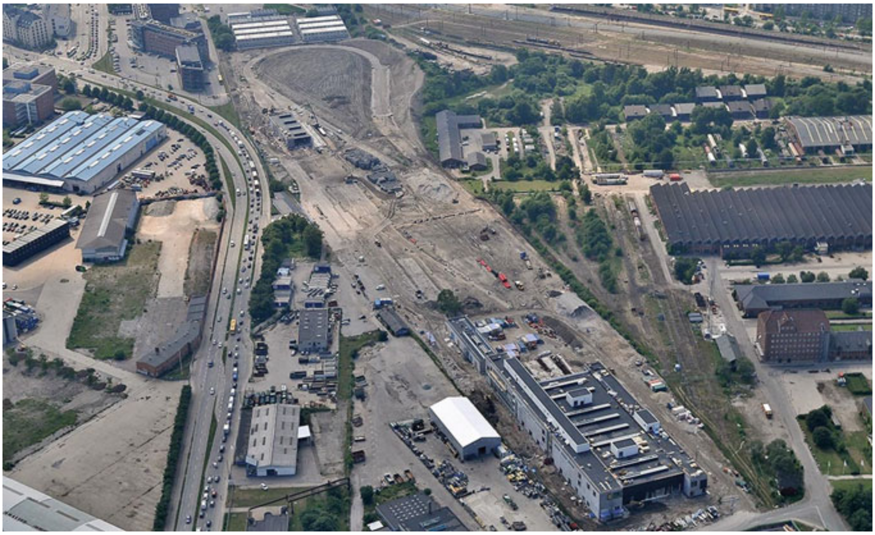


Fig. 3 Control and maintenance center site

The Control and Maintenance Centre (CMC), in Fig. 3, shall provide facilities for operation and maintenance, storage, administration and facilities for the staff. Main Control Centre (MCC) and Emergency Control Centre (ECC) shall provide a good working environment and facilities for train operation, surveillance and passenger service during normal and fall-back operation.

5 Cityringen Security Features

The Passenger Security shall include facilities to support security of passenger within the premises of Cityringen. Security provides a protection against intentional damages; in this contest all the public areas are developed toward the goal to give a maximum security feeling to passenger. As general requirement, all the public area in the stations and the vehicles has to be covered by CCTV, live video and stored footage shall be available at the control center. All the operators have possibility to monitor the footage in a common video wall or in a separate personal screen. Beside the control room, a separate police room is present, where officer can monitor all the cameras in case of events where the security level is increased. All the not public areas must be protected from intrusion. Moreover a deep analysis shall be performed in order to have stations giving a "security feeling" to all passengers, e.g. illumination of stations, not presence of dark corner, good presence of emergency telephone, cameras position.

Other requirements arise from specific procedures such:

Automatic Vehicle Rescue: The trains coupling is surveilled by Control Centre via CCTV in front of trains.

Crowd Control: Detection and handling overcrowding.

CMC Intrusion Control: Due to the proximity of the city the CMC automatic area is believed to be prone to intrusion with the aim to vandalize the stabled trains.

Train removal: When vehicles are removed from service they shall always be stopped for checking by a service staff or by CCTV to ensure they are empty when they run to CMC.

Passenger Blocking of Vehicle Doors/PSD: If a door fails to close (in 3 attempts) the nearest CCTV camera shall zoom in on the unclosed door and show the picture in the CCR at the Train Dispatcher desk.

Emergency Stop Handle (ESH) activated by a Passenger: The nearest CCTV camera shall zoom in on the area at the ESH and present the picture in the CCR.

Station Vehicle Emergency Stop: When the STES is activated a CCTV camera shall automatically zoom in on the STES button area and the picture shall be shown on the Train Dispatcher's WS in the control room.

Activation of Flood Gates: CCTV cameras are covering the floodgates areas.

The implementation of the requirements above shall follow all the Danish legislation on camera surveillance and storage of recording as stated in the different codes of law. In particular shall follow the "TV-overvågningsloven" (TV surveillance code), "Persondataloven" (Privacy and Personal Data code) and "Straffeloven" (Penal code). The application of the codes above give an extra effort for the supplier in order to guarantees a certain level of privacy for all the video footage.

5.1 Security Solution

The adopted security solution is based on the two main elements: Operations Security and Security Systems.

5.2 Operations Security

Concerning the security, the employees shall identify and complete a set of documents and procedure, including Security Master Plan, Security Procedures, Training plan and procedure, etc. The aim is to take in charge of all security aspects in a normal service operation. All the scenarios involving security aspect must be defined and procedure shall be developed.

6 System Description and Architecture

6.1 General

The solution for the security systems in the Copenhagen Cityringen, is based on an Integrated Security System (ISS). The systems shall be monitored and controlled from a main control center with automatic fall back to a emergency control center in an event of a major failure or disaster.

The Security Management System (SMS) is the platform for the security systems integration, the security command and control system and the core of the ISS.

The Human Machine Interface (HMI) implemented in the SMS has been adapted for Cityringen and has undergone a Human Factor Analysis performed according to DS/EN ISO 11064 part 5.

Integrated Security System (ISS).

The Cityringen ISS consists of the following systems:

- Access Control and Intrusion Detection System (ACS and IDS)
- Closed Circuit Television Surveillance System (CCTV)
- Perimeter Intrusion Detection System in the CMC (P-IDS)
- Security Management System (SMS)

The ACS and IDS, CCTV and P-IDS systems are integrated with the SMS, so that they will function as one system rather than four separate systems.

The integration assures efficient and user friendly system operation and management.

The integration allows:

Controlling of all security systems from the SMS operator station, rather than controlling of each system from a separate station.

Setting of users and system parameters of all systems from the SMS administration station.

Receiving and displaying of all alert and fault messages from the security systems, creating and managing of events and managing and controlling of the video display scenarios in the MCC and ECC from the SMS stations.

Creating of configurable links between the events created by the security systems and the display scenarios, so that programmable event driven display scenarios are allowed. This will allow creating of unlimited links between alarms created in the Access Control and Intrusion Detection system, the Perimeter Intrusion Detection system and video analytic detection function of the CCTV system and the CCTV display functions.

As an example, a video stream of a camera viewing an automatic platform door will be automatically displayed when the door is disrupted on the video wall or on one of the CCTV viewing stations. In a similar way, a video stream of a camera viewing a section of a perimeter fence will be automatically directed to the video wall or to designated CCTV viewing station and displayed according to preconfigured display scenario, when an intrusion attempt in this section has been detected by one of the intrusion detection systems (CCTV video analytic channel or the P-IDS). These are only two examples of the ISS capabilities.

Another significant advantage of the ISS, is the ability to allow the CMC perimeter protection to be based on two different detection technologies. This, as illustrated in the following, will assure high level of detection while keeping the false alarm rate extremely low.

The Fig. 4 presents the ISS architecture.

6.2 Closed Circuit Television System (CCTV) and Video Analytics

The CCTV system is installed in the Cityringen stations, ventilation shafts, emergency exits, pump sump, CMC areas and perimeter and in the train cars.

The system allows continuous viewing and recording of the cameras installed in the various stationary and mobile locations and detecting of the specified events by using of the video analytics capabilities of the system.

Microphones are installed in the vicinity of all cameras, excluding external train cars, portal tunnel entrance and doors, CMC areas and perimeter and crossbeams cameras. The microphones allow continuous recording of audio synchronized with the video signals of the cameras and detection of audio level higher than determined.

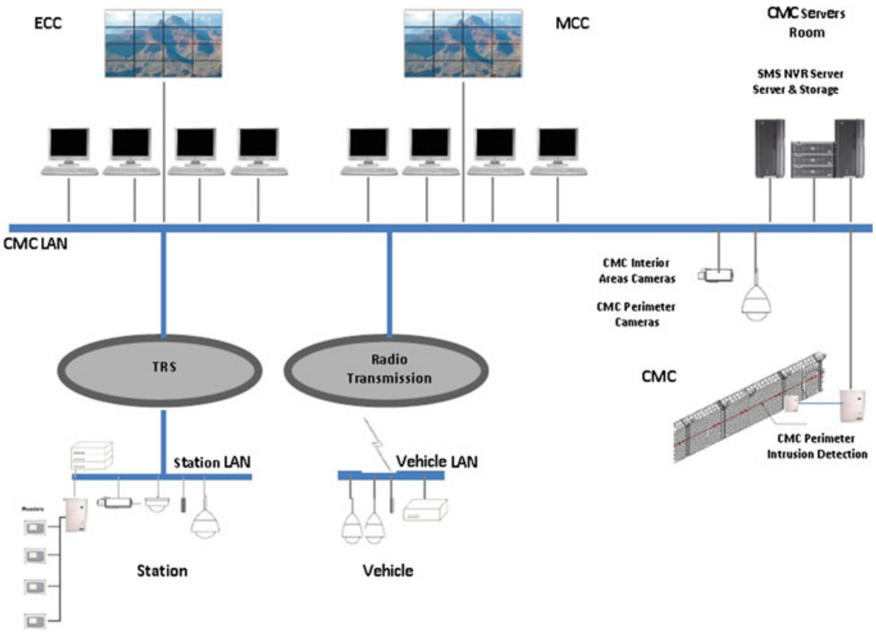


Fig. 4 ISS architecture

The audio channels can be configured separately, so that any channel may be enabled or disabled according to the user's requirement.

The CCTV system allows continuous recording of all cameras and microphones. All cameras are continuously recorded, excluding cameras in emergency exits and ventilation shafts. These cameras recording are events driven by the video analytics function of the camera channel. These cameras are recorded for duration of the event and 5 min from the event's termination.

The system allows storage of the recorded data for duration of at least 30 days, in full resolution and frame rates as determined for the various camera types and locations.

The live video images include titles indicating the cameras location. Recorded images also contain the time and date of the recording.

The recording equipment is located in the stations, CMC control centers and in the train cars.

The system allows transferring of the recorded data on from the onboard recoding units in the train cars to the stationary recording storage in the stations and in the CMC. Transferring of the recorded data is carried out via the Train Radio Communication system.

The live and recorded video streams are transmitted from the station to the control centers via the Cityringen Transmission System.

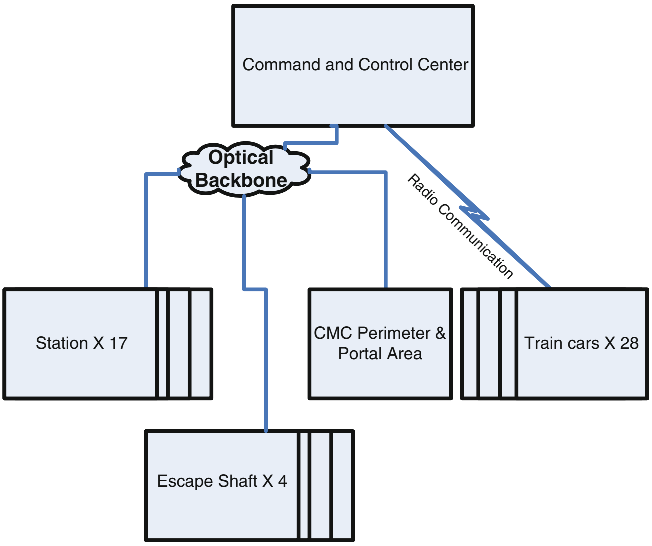


Fig. 5 CCTV system architecture

The system detects and reports on any attempt of covering or tampering with a camera.

The solution allow to identify a person at lighting conditions (over 1 Lux) and Identify a metal objects, e.g. knives, in well illuminated area (e.g. station public area with >50 Lux). Moreover the system has the capability to automatically detect the presence of new objects in specific area, empty vehicle, object at tunnel entrance, etc.

All installed equipment, both cameras and central equipment, consist of self-test and diagnostic features which will allow automatic reporting on a system element malfunction.

Equipment installation is according to the best installation practice, to assure maximal MTBF and system availability and minimal MTTR. Moreover, all equipment installed in public areas shall be mounted in an anti-vandal housing.

In Fig. 5 the CCTV system architecture illustrated.

6.3 Intrusion Detection and Access Control System

The installed system provides a comprehensive integrated solution for intrusion detection and access control in the line stations, ventilation shafts, pump sump, technical rooms and CMC.

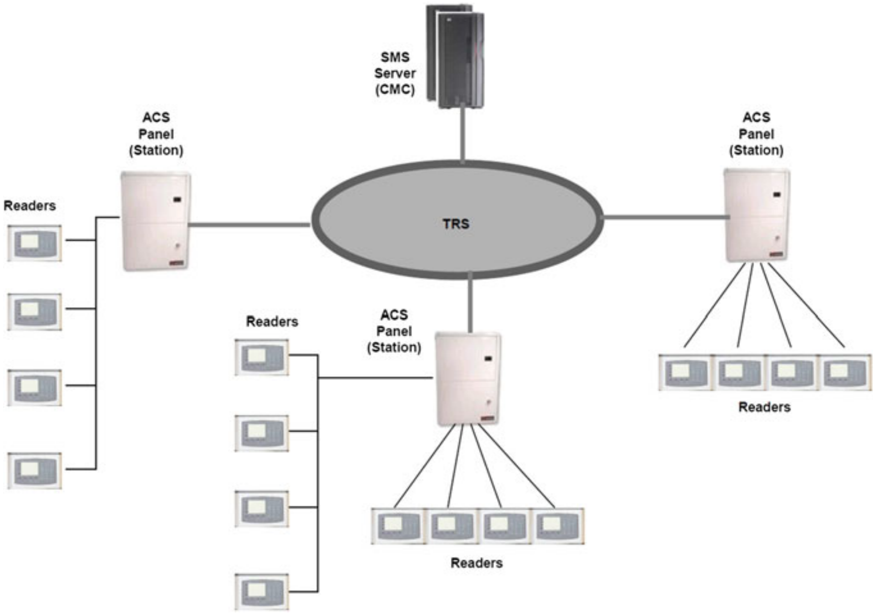


Fig. 6 System architecture

The intrusion detection points can be divided into partitions, which can be armed/disarmed independently, by using a keypad, card reader or from the SMS management system.

If required, passing of an authorized card at the card reader installed at the entrance door to a protected area, will disarm the intrusion detection in that area. Alternatively, or in addition to, the intrusion detection system may be disarmed by a dedicated keypad or from the SMS application in the MCC.

The intrusion detection and access control equipment is installed on doors in stations, shafts, CMC areas.

All alarms and equipment failure will also automatically transmitted to SCADA system and Data Warehouse.

The Fig. 6 presents the system architecture.

The Fig. 7 presents a typical architecture of a station's system.

6.4 Perimeter Intrusion Detection System

As mentioned, due to the perimeter geography and structure, and in order to assure system performance which will be efficient and effective, the perimeter intrusion detection of the CMC and portal area is based on two separate system based on

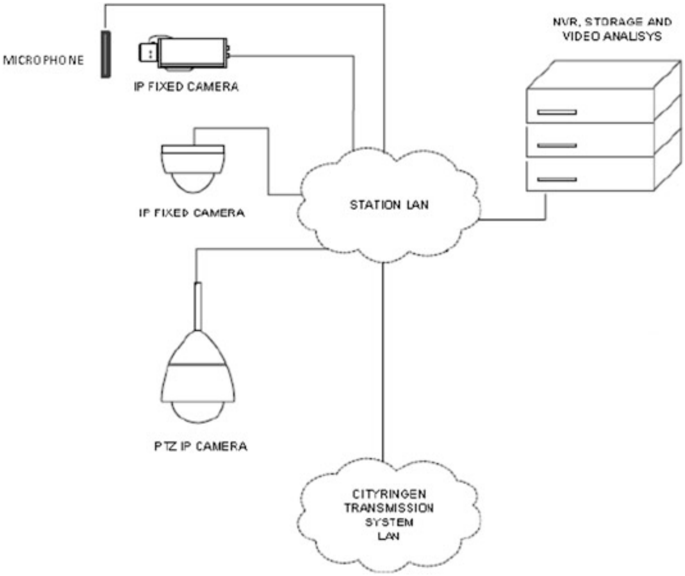


Fig. 7 System architecture—station

different detection technologies, integrated at the SMS level into one detection system.

The detection will be carried out by cameras installed along the perimeter fence, configured with video analytic detection functions and simultaneously by a separate Perimeter Intrusion Detection (P-IDS) system based on vibration detection technology.

Both systems (CCTV and P-IDS) are fully integrated with the SMS.

Consequently, according to the specific conditions and constrains of each individual perimeter zone, the system allows determining if an alarm will be generated by the video analytic function of a camera viewing the area, or by the P-IDS in that area or only if both systems detect an alarm condition simultaneously (AND logic).

This assures high level of detection while keeping the false alarm rate extremely low, in compliance with the tender documents requirements. In this way, the system ensures a probability of detection of at least 99.7 % with an accuracy of about 8 m.

The integrated system assures that the following types of intrusion attempts are detected:

Climbing or attempting to climb the fence.

Detecting of a person or an object of a configurable size within a configurable distance from the fence.

Tampering with the fence.

Detecting of a disguised person violating the detection rules.

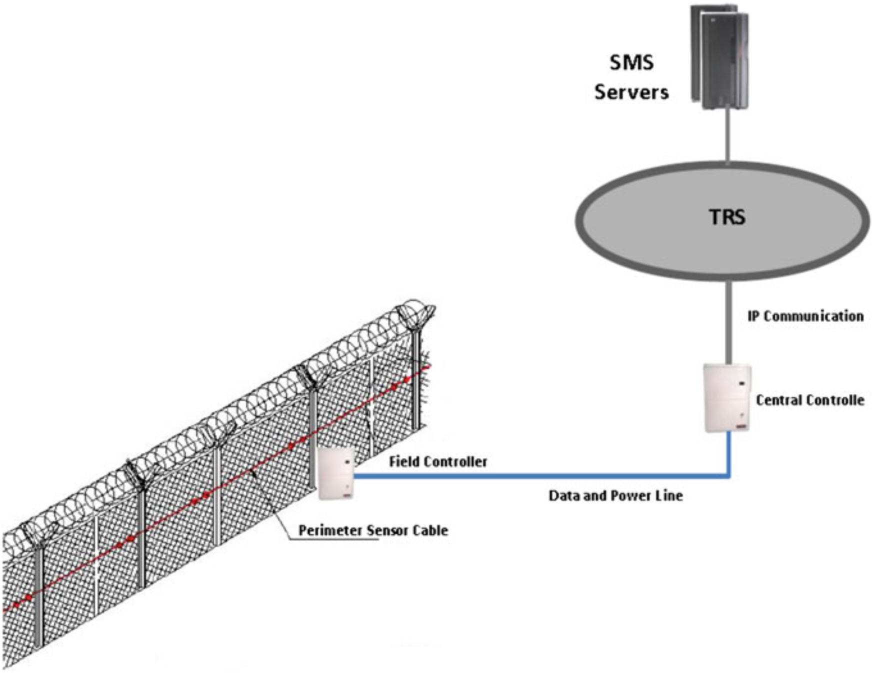


Fig. 8 Perimeter intrusion detection

The integrated system allows identifying of the intrusion location in an accuracy of 8 m.

In an alarm event, the system automatically displays the image of the camera viewing the alarming area.

The PTZ camera is automatically directed to the alarm areas and its image is displayed on the video wall in the MCC and ECC and on the relevant video viewing stations, according to the display scenarios, as determined by Cityringen.

The integrated system is capable of screening create false alarm caused by:

- Animals or objects smaller or bigger that configured size.
- Weather conditions such as rain, snow, fog. Winds up to 60 km/h
- Car headlights.
- Motion of trees and bushes.
- Shadows.
- Activities out of the detection zones.

The system detects any attempt of vandalism or intended destruction or tampering of any part of the field elements of system such as vibration detectors, vibration sensors cable, data cable or field controllers. Shorting or cutting any system's cables, damaging field units, power supplies etc. will cause proper alarm activation.

Moreover, the system consists of automatic self-test functions for proper functionality of sensor lines, field Controllers and data communication lines. Malfunction of each of the above mentioned system elements is reported immediately to the MCC as “real time” fault message.

Figure 8 presents the Perimeter Intrusion Detection system architecture.

7 Reliability and Redundancy

The system design and architecture assures, that potential points of failure are minimized as possible.

All main system components, such as control rooms, servers, video recorders, are based on hot-back up architecture which assures that in case of failure in one of central elements, the system’s operation shall not be interrupted.

Additionally, in case of a major failure in the main communication system which provides communication services between the remote locations (stations, shafts, flood gates, etc.), the local systems in the remote locations continue functioning in a stand-alone mode.

All equipment components fully comply with the environmental, electrical and RFI/EMI requirements.

The CCTV system assures high availability of both live and recorded video streams from all cameras.

8 Conclusion

An overview of the solutions for the Passenger Security of Copenhagen Metro has been described, starting from the main question how to grant security, effective and perceived by passengers. The several observations have considered the specific society and the expected level of security expected for a mass transit system. A excursus on the general security requirements has been taken; requirements that have driven the development of the Security Management System, in respect of CCTV, Access Control and Intrusion detection System. The studio emphasizes how a security approach in all development process and operational phase must be taken in consideration. Architectural solution of the station and vehicle must properly developed in order to gain an intrinsically security feeling in the passenger.

At the moment of writing down this note, the Cityringen project it is in an advanced phase of design, many of the solution described are so in a “tuning phase”. Anyway, we are confident that the general architecture of the system will not have substantial change. This note has been written also bringing all the experiences related the first leg of the Metro, which is a more consolidate 10 years old running project, with many common points.