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

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