The New Challenges of Rail Security

Zakaryae Boudi, El Miloudi El Koursi, and Mohamed Ghazel
Univ. Lille Nord de France, F-59000 Lille, French Institute of Science and Technology for Transport, Development, and Networks IFSTTAR-COSYS-ESTAS, Villeneuve d'Ascq, France
Email:{zakaraye.boudi, el-miloudi.el-koursi, mohamed.ghazel}@ifsttar.fr

***Abstract*—Providing an efficient, safe and secure transportation service is a core factor for European growth, collaboration and employment. As such, this has been identified as a priority in the Europe 2020 strategy. Land transportation has two main challenges concerning security: avoiding interrupts of transport itself in order to assure the flow of freight and passengers and avoiding those transportation systems themselves become a mean for attacks. The European project CARONTE (Creating an Agenda for Research on Transportation security) intends to establish a future research agenda for security in land transport, which focuses on the relevant security gaps caused by emerging risks. Considering the current state of the art and existing research projects, CARONTE covers all threats, including cyber-crime, and security aspects for all land transportation modes, with respect to fundamental human rights and privacy. Accordingly, this paper provides an overview on existing and emerging risks, in terms of security, facing the rail mode as well as the potential measures, based on the risk assessment methodology adopted in the project. This work explains how, from the project point of view, the rising of new cyber-risks and the fast evolution of threats led by technological progress in the rail industry constitute the main challenges of the European rail security nowadays.**

***Index Terms*—railway security, land transportation, cyber security, emerging risks**

I. Introduction

Europe prosperity relies on effective transport systems. Any attacks and disturbances to land freight and passenger transport will have significant impacts on economic growth, territorial cohesion, social development and environment [1]. As is witnessed by historical data pertaining to the security of land transportation, there are unfortunately specific weaknesses in affecting this mode in terms of security.

Historically, several attacks have deliberately targeted the rail transportation, especially metro systems, within major European cities. These attacks have been specifically de-signed to cause maximum disruption and a high number of fatalities. Attacks on subways and local trains have shown that the rail network is an attractive target for attackers to spread fear and terror in the population. The terrorist attacks of the 2004 Madrid train bombings and the 2005 London bus bombings claimed the lives of 191 and 52 innocent civilians, respectively. Furthermore, criminals and terrorists have taken the transport sector to be an easy target. According to TAPA, the theft of high value and high risk products moving in supply chains costs business about € 8.2 billion a year in Europe.

Security issues related to land transport are diverse and complex. In the context of rail transportation and in order to effectively tackle the threats posed by terrorism and other forms of crime, it is important for the authorities and operators to investigate the past attacks perpetrated against railway systems and acknowledge preferred tactics, means and procedures, in order to provide pre-emptive answers to be adopted in case of attack. Moreover, it is crucial that end-users have a wide knowledge of security measures currently implemented by transportation entities that have suffered from attacks or which have confront with high levels of threat, in order to determine the most appropriate practices to face such critical circumstances.

However, the increasing evolution of railway systems, such as the new European signaling ERTMS system (European Rail Traffic Management System), leads up to new generation of threats and requires a continuous updating of the corporate practices to face these threats. Today, the growing risk of cyber-crime puts in fact the authorities and the railway stakeholders in front of new security challenges, where the main purpose is to minimize the risks from both existing and emerging threats, and provide better security solutions in order to avoid catastrophes.

With this respect, this paper will give at first, a brief presentation of the European project CARONTE, its scope and its objectives. Afterwards, the risk assessment methodology which is conducted in the project for threat identification and risk analysis will be detailed in order to introduce the rail mode risk model. Then, the core part of the paper is discussed, that is, an overview on the existing and emerging threats facing the rail sector and the co-existing security measures. The following sections will discuss some limitations of the existing risk assessment methodologies and raise the new challenges of security in the rail sector from the CARONTE project point of view. A final conclusion will summarize the work and recapitulate the future challenges we believe rail security in Europe will have to deal with.

II. The CARONTE Project

A. Project Summary

Continuous and coordinated efforts and investment are needed to address land transportation security issues.

Manuscript received January 1, 2015; revised August 24, 2015.

doi: 10.18178/jtle.4.1.56-60

CARONTE project (Creating an Agenda for Research On Transportation security) is one of the European projects within the 7th framework program that address land transport security at a national, European, and international level Fig. 1.

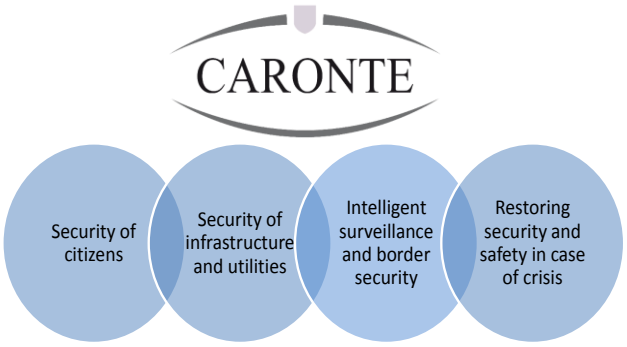


Figure 1. FP 7 Security missions and activities

The objective of the CARONTE project is to provide answers to the question of what type of security related projects should be planned in the future, which themes and topics should be investigated and who should be involved in the future research projects to respond to current and future threats facing land transport. CARONTE covers existing and emerging threats, including conventional and cyber threats and relevant work on security issues in all land transport modes (i.e., road, rail, air, maritime through ports and inland waterways). The project especially aims at increasing the know-how transfer between stakeholders and fostering the interoperability between member states for security management on issues related to land transport. Specifically, the following aspects are elaborated:

- Analyzing and describing the state of the play in transport modes, including infrastructure, vehicles, processes and stakeholders, covering passenger and freight transport;
- Identifying and assessing potential and future risks including cyber-attacks, ICT security and covering terrorism and crime among others;
- Identifying potential and future gaps in security vs. security measures taken, regulations existing and planned , current research and its foreseen results;
- Assessing the gaps identified and highlighting the needs for action;
- Analyzing social and ethical aspects of security measures (human rights, privacy vs. security);
- Reviewing and Analyzing past and current research projects, their results and impacts on future. Defining a risk assessment methodology for rail.

B. Security Terms

In this section, we introduce some common concepts that one has to handle when considering security issues.

- **Definition 1**. Security: Resistance to intentional, unauthorized act(s) designed to cause harm or damage to, or by, the supply chain.
- **Definition 2**. Vulnerability: Refers to a system, software, hardware, procedural, or human weakness that may provide an attacker the opportunity to enter a computer or network or the unauthorized access to resources. A vulnerability characterizes the absence or weakness of a safeguard that could be exploited.
- **Definition 3**. Threat: Any potential danger to information or systems. An attacker might identify a special vulnerability and use it against the organization or the individual, which constitutes a threat.
- **Definition 4**. Risk: The likelihood of an attacker taking advantage of vulnerability and the corresponding business impact.
- **Definition 5**. Exposure: An instance of being exposed to losses from an attacker. Vulnerabilities expose an organization to possible damages.

C. Risk Assessment Methodology

The CARONTE risk assessment methodology is based on best practices and standards such as those pointed out in ISO2700 [2], NIST Guide for Conducting Risk Assessments [3], [4] and other known risk assessment techniques originated and applied in the area of information security and safety engineering [5]. The risk assessment methodology includes a risk model, a risk assessment process, and assessment techniques.

Faults in a system can cause failures. Dangerous failures are able to cause hazards and hazards can cause harm. Depending on the severity of the harm and the probability that harm occurs, the risk can be calculated. If the risk is higher than the tolerable level, techniques for risk reduction need to be applied. The level of risk reduction which needs to be achieved is specified using the Safety Integrity Level (SIL) concept. The aim is to prevent from unacceptable risk. Hazards and the necessary risk reduction are determined in the hazard and risk assessment analysis. Potential hazards are identified and event sequences, which lead to such circumstances, are determined. Afterwards safety requirements and associated safety integrity levels are defined.

D. Risk Assessment Process for the Rail Mode

The steps of the risk assessment process for the rail mode start by collecting information on the railway system, including known common threats or attacks. With this basis, runs an identification of the targeted systems and subsystems followed by the enumeration of possible impacts (effects) related to these targets as a result of successful attacks. The generated impacts can be grouped into monetary loss, human life, and environment damage. Moreover, the induced consequences can be associated to an estimated severity levels specified in Table I.

TABLE I. DEFINITION OF SEVERITY CLASSES

Severity-Classes	Consequences to persons or environment	Functionality	Monetary losses

7	Very many people killed		
6	Death to several people		
5	Serious permanent injury to one or more persons; death to one person		
4	A failure mode which could potentially result in the failure of the system's primary functions and therefore causes serious damage to the system and its environment and/or personal injury or high monetary losses.	Lost, system destroyed	High losses
3	A failure mode which could potentially result in the failure of the system's primary functions and therefore causes considerable damage to the system and its environment or monetary losses, but which does not constitute a serious threat to life or injury.	Lost, system damaged	Considerable losses
2	A failure mode, which could potentially degrade system performance, function(s) without appreciable damage to system or threat to life or injury and only minor monetary losses.	Degraded, minor system damage	Minor losses
1	A failure mode which could potentially degrade the system's functions but will cause no damage to the system and does not constitute a threat to life or injury.	Temporally degraded	Minor losses

The next step consists in identifying potential threats which cause the impacts identified previously and assessing the likelihood of each threat and threat agent, while considering the resilience. Finally, the results are to be consolidated into a risk catalogue and the high priority risks need to be determined.

The risk assessment methodology must allow the understanding of different physical and cyber systems, technologies, and their developments in the rail mode. Accordingly, a classification of the different railway sub-systems (e.g., Supervisory control and data acquisition (SCADA), power, signalling, communication, and information systems etc.) is provided for the identification of related safety and security risk. However, it is required for CARONTE to carry out the work in a defined scope and a right level of abstraction.

TABLE II. ASSET CLASSIFICATION FOR THE RAIL MODE

Level 1:	Level 2	Level 3
Rail Mode	Connecting infrastructure	Tracks
		Tunnels
		Bridges/viaducts
		Switches/Rail junctions
	Mobile units	Locomotives
		Rolling stock
	Control systems	Central rail traffic management
		Local Rail traffic management
	Communication systems	Communication network
	Power supply	Catenaries
		Power supply national grid
		Diesel stations
	Staff	Driving personnel
		Handling personnel
		Maintenance personnel
		Information processing personnel
	Cargo	Non-dangerous
		Explosive
		Toxic
		Flammable
	Passenger	

III. RISK MODEL OF THE RAIL MODE

A. Asset Classification

The EU working document for regulation on enhancing supply chain security was used as a reference for the specification of land transport system and its components [6]. The classification adopted for the rail mode is shown in Table II.

B. Existing Risks

Regarding the classification of assets presented earlier, access, size, construction techniques, control command and communication systems are considered to be the most vulnerable elements of the railway transportation systems. Indeed, these central elements are easily exposed to malicious uses leading to serious threats. Previous research works revealed that among the tactics adopted to attack train and subway systems, bombing is largely the preferred and more common way to carry out attacks, followed by sabotage, armed attack and arson. Other cases seem to be numerically less relevant though.

Reducing the vulnerabilities of critical infrastructure and increasing their resilience to attacks is one of the major tasks in transport security. The economic impact of such attacks on rail transportation and the infrastructure and vehicle damage could rise to an uncontrollable level and compromise very large areas. Actually, an achieved criminal or terrorist attack may cause accidents and traffic congestion, impact on supply chains, destroy, disrupt, or delay movements of goods, and may produce environment impact, personal injury, fatalities psychological impact and common panic.

Nevertheless, authorities and rail industry have put in place a considerable number of measures and plans against the identified threats. For example, critical infrastructure and areas can be secured using access control systems, intruder alarms and detection, CCTV systems, intelligent video-analysis and other dedicated technologies. In addition, facilities continuous communication with staff and passengers in stations or trains is established by means of passenger information

and awareness raising and also by using train to station wireless communication technologies and security teams on the ground. On the other hand, issues caused by the size of the rail networks are addressed through monitoring and location systems, traffic control policies and security management systems. Furthermore, help points, security focused risk assessments, control centers; stored equipment for emergency cases, arrangements and cooperation with the relevant authorities can be set up for response and recovery from security incidents.

C. Emerging Risks

Over recent years, the rail systems have significantly evolved toward new technologies and communication-based systems, as it is the case in all land transport modes, especially for safety and security related domains. For this reason, we believe that the future research related to rail security should namely focus on the emergent cyber risks which could be more and more attractive for threat agents.

Actually, due to the advancing integration of ICT (Information and Communications Technology) technologies into land transport, mobile units and infrastructure alike, the number of potential cyber risks has steadily risen during the last decade. With the generalization of automation and computerization in the rail vehicles and signaling systems, we will most likely see attacks, motivated by financial gain, political or terroristic intends, or simply vandalism, using these techniques. This could become a high potential risk.

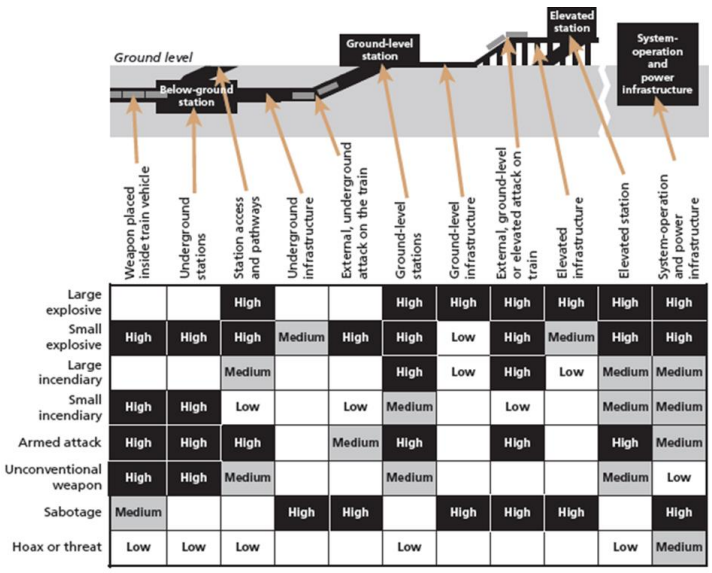
Additionally, the increasing use of wireless techniques as a basis for the communication infrastructure also poses additional risks. For example, in the ERTMS framework, GSM-R techniques are used for on-board/Track-side communication, where safety relevant information is exchanged [7]. Therefore, this new channel can be target of jamming or spoofing attacks. One of the research projects dealing with this emerging kind of risks is the European project SECRET (www.secret-project.eu) [8], [9], which aims to assess the risks and consequences of Electro-Magnetic attacks on the rail infrastructure, especially potential attacks on the GSM-R-Systems. The project came to the result that it is more likely to disturb the information exchanges between trains and control centers than to spoof the data, since the latter is much more complicated.

It is worthwhile to notice that the cyber threats increase as the train control systems are more and more relying on ICT systems and radio communication, even for automatic train control systems. As railway systems are designed according to the fail safe approach, interrupting of signals would lead to train stops, but the failure of communication operation makes the trouble caused much more complicated.

D. Discussion

Identifying land transport risks, and particularly rail transport risks is not such a trivial task. That is why the CARONTE consortium endeavors to reason about risks in a broader sense and looks forward to identifying common risk patterns that are applicable to similar or different components and systems in land transport.

With respect to the risk assessment methodology adopted in the project, it is important to mention that the likelihood is skipped, and only severity is considered to assess risks. The reason behind this choice is that likelihood is difficult to examine for emerging risks and also for existing risks with only limited information about vulnerabilities. In other terms, no sufficient data is available in order to carry out quantified analysis. Furthermore, security risks have the characteristic of undergoing constant evolving. It is therefore inappropriate to provide priorities according to the likelihood of a risk.



	Weapon placed inside train vehicle	Undergound stations	Station access and pathways	Undergound infrastructure	External, undergound attack on the train	Ground-level stations	Ground-level infrastructure	External, ground-level or elevated attack on train	Elevated infrastructure	Elevated station	System-operation and power infrastructure
Large explosive			High			High	High	High	High	High	High
Small explosive	High	High	High	Medium	High	High	Low	High	Medium	High	High
Large incendiary			Medium			High	Low	High	Low	Medium	Medium
Small incendiary	High	High	Low		Low	Medium		Low		Medium	Medium
Armed attack	High	High	High		Medium	High		High		High	Medium
Unconventional weapon	High	High	Medium			Medium				Medium	Low
Sabotage	Medium			High	High		High	High	High		High
Hoax or threat	Low	Low	Low			Low				Low	Medium

Figure 2. RAND corporation asset/tactic classification for rail risk levels

One of the main challenges for the CARONTE project in particular, and rail transport security in general is that some risk assessment methods for railways, for example, based on position of asset/threat [10] Fig. 2, only permit to study certain types of attacks. It is therefore very difficult and inadequate to codify different types using

such a classification. Indeed, such methods might be suitable for attacks by physical means, which is not the case for cyber-attacks.

From the CARONTE project point of view, another useful approach for risk identification and assessment is to consider the motivation of attackers. Attackers should be considered as rational people who optimize their attacks and use the easiest and cheapest way to reach a motivated goal. Therefore, although the existence of many tactics for attacking, whose embodiment is theoretically feasible, it is worth the effort to estimate the motivation in order to assess whether a risk is realistic. However, the fast evolution of threats and vulnerabilities makes it very challenging to assess emerging risks, which needs a continuous updating of the approach.

IV. Conclusion

This study done in the framework of the European project CARONTE (Creating an Agenda for Research On Transportation security), gives an overview on the existing and emerging risks in rail security, and therefore, introduced the new challenges for the rail sector in terms of security. The objective of the CARONTE project is to provide answers to the question of what type of security related projects should be planned in the future to respond to current and future threats facing land transport. As a main conclusion, the challenge today is to follow up the continuous evolution of threats and vulnerabilities, and to develop new approaches for risk assessment based on motivation of attackers and the severity of the expected impact, especially in relation with cyber-crime.

The results show that security risks in rail transport in particular and land transport in general are dynamic, complex, and inter-related. Railways have and will continue to process a large number of physical and cyber vulnerabilities, which can give rise to threats at different levels of sophistication. This presents a major challenge that the railway stakeholders need to face in the coming years.

Acknowledgment

The authors wish to thank all the CARONTE project consortium partners for their hard work. This project is funded by the European Commission.

References

[1] European Commission, "Commission staff working document on transport security," presented at SWD 143 Final, Brussels, May 31, 2012.

[2] Information Technology–Security Techniques-Information Security Management Systems–Requirements, ISO/IEC Standard 27001, 2013.

[3] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems-recommendations of the national institute of standards and technology," NIST, Special Publication 800-30, July 2002.

[4] National Institute of Standards and Technology, "Guide for conducting risk assessments," NIST Special Publication 800-30, Revision 1, September 2012.

[5] State Government Victoria, Security Risk Assessment for Transport Operators, A Practical Guide for Small to Medium-Sized Organizations, May 2012.

[6] Commission of the European Communities, "Proposal for a regulation of the European parliament and of the council on enhancing supply chain security," Commission Staff Working Document, COM (2006)79 Final, Brussels, 2006.

[7] European Commission, Directorate-General for Mobility and Transport, Directorate-General for Energy, "ERTMS—delivering flexible and reliable rail traffic. A major industrial project for Europe," Office for Official Publications of the European Communities, 2006.

[8] V. Deniau, "Overview of the european project security of railways in Europe against electromagnetic attacks (SECRET)," *IEEE Electromagnetic Compatibility Magazine*, vol. 3, no. 4, pp. 80–85, 2014.

[9] M. Heddebaut, S. Mili, D. Sodoyer, E. Jacob, M. Aguado, C. P. Zamalloa, *et al*., "Towards a resilient railway communication network against electromagnetic attacks," presented at Transport Research Arena, Paris, France, September 5, 2014.

[10] J. M. Wilson, B. A. Jackson, M. Eisman, P. S. Steinberg, and K. Jack Riley, *Securing America's Passenger-Rail Systems*, RAND Corporation, 2007.

Zakaryae Boudi received his engineering degree in Automation and Computer Science from the Ecole Mohamadia d'Ingénieurs (EMI), Rabat, Morocco. Since then, he has been a researcher and an engineer at the French Institute of Science and Technology for Transport, Development and Networks, France. His work is mainly focused on railway safety and security, especially in the new generation of signaling systems (CBTC, ERTMS, computerized interlocking…). His research interests include risk assessment techniques in rail security and the industrial use of formal methods for safety critical systems.

El Miloudi El Koursi is a Research Director at IFSTTAR. He has 25 years of experience in performing assessment and certification of safety related rail and associated systems. In recent years, he has been involved in various European projects. He was the leader of European FP5, SAMNET "Safety Management and interoperability thematic network) thematic network and the leader of pole 6 "Safety and security" within FP6 EURNEX "European Rail Research Network of excellence" European network of excellence.

Mohamed Ghazel is a senior researcher at IFSTTAR. He mainly works on system safety and security and develops methods of behavioral modelling, model checking while using formal (Petri-nets) and semi-formal (UML) notations. He has been involved in several national and European research projects dealing with security and safety of guided transport and critical infrastructures.