Available online at www.sciencedirect.com

ScienceDirect

Transportation Research Procedia 3 (2014) 740 – 749

Transportation Research Procedia

www.elsevier.com/locate/procedia

17th Meeting of the EURO Working Group on Transportation, EWGT2014, 2-4 July 2014, Sevilla, Spain

# A quantitative approach to risk management in Critical Infrastructures

Sapori E. [a], Sciutto M. [b], Sciutto G. [c, d,] *

[a] *Italian Center of Excellence on Integrated Logistics (C.I.E.L.I.), Via Bensa 1, Genoa - 16124, Italy*
[b] *SI-Consulting s.r.l., Via Gavotti 5, Genoa - 16121, Italy*
[c] *University of Genoa (DITEN), Via dell'Opera Pia 11A, Genoa - 16145, Italy*
[d] *National Interuniversity Consortium for Transport and Logistics (NITEL), Piazza dell'Esquilino 29, Rome - 00185, Italy*

## Abstract

In the last ten years, an efficient Security Management System (SEMS) has acquired an important role for organizations working in transportation sector. In many cases, Critical Infrastructure legislation plans specific and mandatory quality requirements for the implementation of a security management system. The organizations are encouraged by the legislative requirements and the competitiveness to certify the SEMS in accordance with the current international standards (e.g. ISO 27001 and ISO 28000). As well known, certification can be either a mandatory or a voluntary process but it is usually voluntary and qualitative. In the SEMS, as in other management systems, current certification uses a qualitative approach deriving from the ISO 9000. Normally in certification, quantitative assessment characterizes only some technological systems while every other application including human factor or procedures uses qualitative assessment. The development of security management system certification should bring to introducing risk-based and quantitative assessment methods. Benefits arising from the residual risk quantification of the SEMS can set certification a tool enabling to bargain with insurances, a warranty for the investments undertaken when facing stakeholders and shareholders, a proof to justify decisions during a legal action and last but not least a good publicity for company's image and hence company's competitiveness. This paper proposes the implementation of risk-based methodologies in use by process engineering to achieve a quantitative assessment of security management systems. The methodology is exposed and applied to a railway case study. The first steps show how to analyze the system (study of macro operability functions, identification of subsystems, etc.) and how to integrate technological, human and procedural aspects by flow charts. The later steps describe how to manage threats, vulnerability and criticality of Critical Infrastructure subsystems and how to identify "primary causes" and "Top Event consequences" drawing fault trees and event trees, and finally how to calculate the residual risk for security management system. In conclusion, the methodology is applied on a case study of one railway subsystem and the results of the quantitative risk analysis are exposed.

Selection and peer-review under responsibility of the Scientific Committee of EWGT2014

* Corresponding author. Tel.: +39-06-488-0635
*E-mail address:* sciutto@nitel.it

Selection and peer-review under responsibility of the Scientific Committee of EWGT2014
doi:10.1016/j.trpro.2014.10.053

*Keywords:* Risk Management; Risk Assessment; Critical Infrastructure; Railway System

## 1. Introduction

The risk management of Critical Infrastructure is taking an increasingly important role. Whether at first, the demand of risk management turned to provide safe services against technological failure (safety), in the last ten years, security and natural disasters have significantly expanded its purpose. The international authorities, at different levels, decided to address the problem through a standardization of procedures for risk analysis and assessment. The latest decisions of the Europe Union (2008) and the Europe Commission (2012) and the introduction of specific international standards of risk management underline this common policy (ISO/IEC 27001, 2013; ISO 28000, 2007; ISO 31000, 2009).

The risk measurement refers to the well-known expression:

$$\text{Risk} = \text{Treat} \times \text{Vulnerability} \times \text{Consequence} \tag{1}$$

where the risk R is the product of the probability of occurrence of the threat T, the vulnerability V (i.e. the probability of fulfillment the threat) and the damage caused C. In case of natural and intentional threats, the probability of occurrence T is a variable difficult to evaluate because strongly dependent by external factors not always predictable. The hazardous weather events have very complex dynamic and it is difficult to obtain a long-term forecasting reliable enough. Similarly, the intentional threat, being a deliberate action, depends on time changing socio-political context and opponent utility therefore, also in this case, are difficult to predict (Bier et al., 2005; McGill et al., 2007). In risk assessment, apart from technological failures, the threat is often an element of great uncertainty requiring hypothesis assumption and/or different scenarios to study.

In risk analysis and in risk assessment, there are international standards indicating qualitative, semi-quantitative and quantitative approaches, but in practice, the most used methods are qualitative or semi-quantitative. This aptitude is greater when the Critical Infrastructure analysis regards a large number of factors such as technological systems, human factor and procedures. In this case, the most used approach is the semi-quantitative using ad-hoc evaluation tables to rate threat, vulnerability and consequence by brainstorming activity. This method does not allow an effective risk management because it is difficult to detect and measure assessment errors.

The European Union demanding to introduce methods for quantitative assessment of the safety level emphasized this problem in the context of rail traffic. Complying with this request, Cesario et al. (2008) presented an analytical method for the quantitative assessment of the safety level in railway transportation. This paper deals the general problem of risk management in Critical Infrastructure. Section 2 presents a methodological approach for risk management: the first part introduces the techniques used to model the Critical Infrastructure and carry out the risk analysis while the second part describes the Alarm & Intervention Management System (AIMS) analysis and the vulnerability assessment. In section 3 the key steps of methodology are applied on a railway case study and finally the results of the quantitative risk assessment are presented.

## 2. Quantitative Evaluation Methodology for Risk Management

This section presents the main features of the methodological approach aimed at a quantitative risk assessment: the process and functional analysis of Critical Infrastructure and the evaluation of risk management system. Figure 1 shows the quantitative assessment scheme in the risk management process, which is briefly described from step 1 to step 6 in section 2.1.

The aim of the methodology is to quantify the risk in all processes and operations that compose the core business of the system under analysis. Among the given techniques for quantitative risk assessment of ISO 31010 (2009), Process Flow Diagram (PFD) and Enhanced Functional Flow Block Diagram (EFFBD) are used to model the