Matsika E, O'Neill C, Battista U, Khosravi M, Laportec AS, Munoz E. Development of Risk Assessment Specifications for Analysing Terrorist Attacks Vulnerability on Metro and Light Rail Systems. *In: Transport Research Arena TRA2016*. 2016, Warsaw, Poland: Elsevier.

Copyright:

© 2016 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license.

DOI link to article:

http://dx.doi.org/10.1016/j.trpro.2016.05.207

Date deposited:

28/06/2016

This work is licensed under a
Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International licence

Newcastle University ePrints - eprint.ncl.ac.uk

Available online at www.sciencedirect.com

ScienceDirect

Transportation Research Procedia 14 (2016) 1345 – 1354

Transportation Research Procedia

www.elsevier.com/locate/procedia

6th Transport Research Arena April 18-21, 2016

Development of risk assessment specifications for analysing terrorist attacks vulnerability on metro and light rail systems

Emmanuel Matsika [a, *], Conor O'Neill [a], Umberto Battista [b], Mony Khosravi [b], Antonio de Santiago Laporte [c], Eduardo Munoz [c]

[a]*NewRail, Newcastle University, Newcastle upon Tyne, NE1 7RU, UK*
[b]*Stam S.r.l., Piazza della Vittoria, 14/11 - 16121 Genova, Italy*
[c]*Metro de Madrid, Calle Cavanilles número 58, 28017,Madrid, Spain*

Abstract

With terrorist security of critical assets becoming a vital aspect of railway systems, this paper reviews the existing international policy frameworks and also risk assessment methodologies. This information fed into development of a risk assessment methodology (RAMPART Methodology) specifically addressing metro and light rail systems (mass transit). The uniqueness lies in differentiating itself using the following nine factors and parameters: qualitative vs quantitative approach; detail (depth of data/information levels disaggregation); scope (e.g. what threats/assets/sector covered?); what is target user group (legislators, management, technocrats, etc); definition of asset criticality; degree of subjectivity in whole RA process; is resilience (countermeasures) included?; are interdependences included; and common taxonomy/terminology.

© 2016 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).
Peer-review under responsibility of Road and Bridge Research Institute (IBDiM)

Keywords: Risk assessment; critical infrastructure (CI); terrorist attack; mass transit; countermeasures

* Corresponding author. Tel.: +44-191-208-8648; fax: +44-191-208-8600.
E-mail address: emmanuel.matsika@newcastle.ac.uk

2352-1465 © 2016 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).
Peer-review under responsibility of Road and Bridge Research Institute (IBDiM)
doi:10.1016/j.trpro.2016.05.207

1. Introduction

1.1. Background

Security is of growing concern in the EU. The cost of security could be high. That is why security investments need to be correlated to a set of identified risks, which can be defined as the product of the likelihood and the impact of specific threats. Installation of security technologies, more security staff and accompanying personal training that must be done in order to protect the passengers, staff and assets. A comprehensive risk assessment provides a good potential to strike the desired balance between costs and effectiveness. The term "threats" in security applies to a wide array of unlawful activities, from low and medium crimes such as graffiti, aggression or theft to major attacks such as bombings or arson.

Inevitably, there exist many risk assessment methodologies (RAMs) across the world for different applications. These are usually tested and validated for the purpose - for a sector, organisation, asset or threat or indeed a particular audience (policy makers, decision makers or operators). The RAMPART methodology focusses on the threat of terrorist attacks on assets related to metro and light rail. The following approach is applied within this research work to develop risk assessment specifications that address metro and light rail applications:

- Review of European and international critical assets protection policy frameworks
- Literature review of risk assessment methodologies relevant to metro/ light rail transportation.
- Development of RAMPART tool risk assessment specifications
- Development of an asset inventory and determination of critical assets

1.2. Research Objectives and Scope

Threat and risk assessments are considered as an analytical approach needed for the prioritisation of resources in the security sector, with the final goal of reducing/mitigating terrorist risks. There is currently an increasing interest in the use of risk management techniques for assessing vulnerability of CIs to a terrorist hazard. As such, the various uncertainties and risks associated with terrorism must be quantified and then used as the basis for assessing the viability and relative benefits of different mitigation measures. To date many different risk assessment methodologies have been developed to be implemented for specific applications and scenarios, from infrastructure to information technology to business management.

As far as blast-related threats are concerned, most of state-of-the-art risk management methodologies are focused only on the structural resistance of the assets, rather than on a complete assessment approach (Ingleton and O'Neill, 2011). A probabilistic approach is sometimes applied to predict risks of damage arising from blast damage to built-infrastructure, keeping into account the properties of the materials involved. The same applies to software tools used against blast threats. There is therefore the need for a risk management methodology and tool to mitigate blast terrorist threats, based on a global and holistic approach, since nowadays none of these are available on the market for the involved stakeholders. This was the motivation for developing the RAMPART risk assessment methodology. The objectives of this research are as follows:

- Appraisal and evaluation of the methodologies and processes in developing risk assessment strategies.
- Identification of strengths and weaknesses of relevant state-of-the-art risk assessment methodologies.
- Development of specifications for RAM for terrorist attacks on metro and light rail systems.

2. Risk Management

2.1. Fundamentals

The risk assessment helps identify the security gaps, supports the security operation planning and management and helps draw up the adequate preventive actions and countermeasures. In the overall context of risk management, the objective of performing risk assessments is to identify and estimate levels of exposure to the likelihood of loss, so that managers can make informed decisions on how to manage those risks of loss – either by accepting each risk, or by mitigating it – through investing in appropriate internal protective measures judged sufficient to lower the potential loss to an acceptable level, or by investing in external indemnity (The Open Group, 2009). Risk assessment takes account of the probability of a threat happening – this is the main difference with a general impact assessment.

The risk management process shown in Fig. 1 is made up of five main pillars (Soehchen and Barcanescu, 2014):

- Establishing the context and defining levels of details for the risk assessment

- Identification of Risks
- Analysis of Risks
- Evaluation of Risks
- Treatment of Risks

The three middle pillars constitute risk assessment. The main rationale behind performing and applying a risk assessment is to spot the relevant security gaps, in order to decide what measures may be appropriate in order to improve the overall security level.

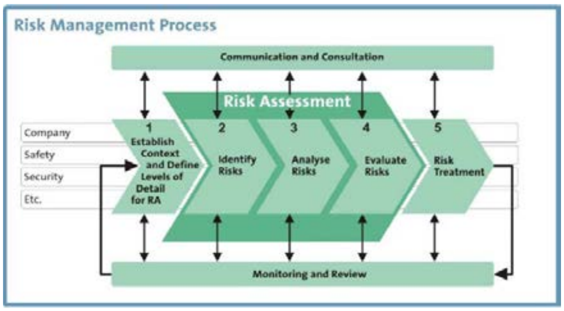

Fig. 1. Risk Management Process (Soehchen and Barcanescu, 2014).

According to (Soehchen and Barcanescu, 2014) the three risk assessment stages involve the following:

- **Risk Identification:** Precisely identify the potential threats and their connected risk scenarios that can have an impact on the metro system.
- **Risk Analysis:** It is the moment when experts from different backgrounds – operations, security department, technical departments and others, but also external stakeholders, especially police and law enforcement agencies – will analyse and assess the risks and risk scenarios.
- **Risk evaluation:** risk analysis results are obtained and analysed. Based on the findings, the risk assessment team can thus define the threats and/or the risk scenarios which need to be assessed in more detail usually applying the ALARP (As Low As Reasonably Practicable/Possible) principle.
- **Risk mitigation:** The final step of the risk assessment procedure is the risk mitigation.

Any risk assessment should undergo a review and monitoring process. Generally however, most RAMs follow a linear approach of as shown in Figure 2.

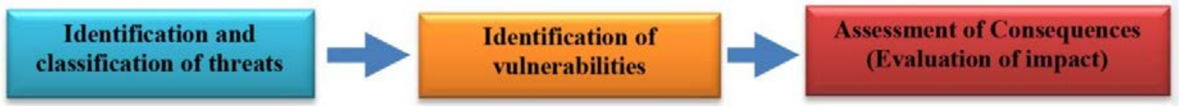
Identification and classification of threats
Identification of vulnerabilities
Assessment of Consequences (Evaluation of impact)

Fig. 2. Sequence of risk assessment.

The second important parameter that enters the stage for the risk assessment methodologies of networked infrastructures is the element of interdependencies. According to the work of Rinaldi et al (2001) four types of interdependencies are identified for critical infrastructures:

- **Physical**: The operation of one infrastructure depends on the material output of the other.
- **Cyber**: Dependency on information transmitted through the information infrastructure.
- **Geographic**: Dependency on local environmental effects that affects simultaneously several infrastructures.
- **Logical**: Any kind of dependency not characterised as Physical, Cyber or Geographic.

Critical Infrastructure Protection (CIP) risk assessment methodologies can be divided in two major categories:

- Sectoral methodologies, when each sector is treated separately with its own risks
- Ranking and systems approach that assess the critical infrastructures as an interconnected network.

Methodologies that have been initially conceptualised to fit in the second category are rather limited. The vast majority of the existing work has been sectoral and mostly at asset level (Giannopoulos et al, 2012). The majority of this approaches resort to the theory of resilience (Hollnagel et al, 2006; Sterbenz et al, 2010) and the emerging behaviour (Woltjer, 2010).

2.2. Risk Taxonomy

The Open Group (2009) observes that one of the major problems with risk management is that a variety of definitions do exist, but the risk management community has not yet adopted a consistent definition for even the most fundamental terms in its vocabulary; e.g., threat, vulnerability, even risk itself. To deal with this, they developed a standard that provides a single logical and rational taxonomical framework for anyone who needs to understand and/or analyse information security risk. This, however, was in the context of software threats. Coherent Risk Taxonomy is an essential step towards enabling all stakeholders in risk management to use key risk management terms – with precise meanings so that there is a bridge for the language gap between risk assessors, security wings, business managers, lawyers, politicians, and other professionals, in all sectors of industry and commerce and the critical infrastructure, whose responsibilities depend on managing risk.

3. Policy Frameworks

Terrorism mainly targets ‘western countries’. Therefore explained below are CIPs for the EU, USA and Canada which provide a good representation of western countries. At a high national level, policy drives risk management that is applied at sector or company levels.

3.1. European Union (EU)

The European Programme for Critical Infrastructure Protection (EPCIP) is a multi-annual programme that encompasses several instruments for the protection of critical infrastructures in Europe. The legislative instrument is the Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (EC, 2008). Due to the interrelationship between sectors and infrastructure, a systems approach was recommended for critical infrastructure under the EPCIP Directive (Giannopoulos et al, 2012).

3.2. *USA*

The Homeland Security Presidential Directive (HSPD-7) established U.S. policy for enhancing critical infrastructure protection by establishing a framework for the Department’s partners to identify, prioritise, and protect the critical infrastructure in their communities from terrorist attacks (US Government, 2014). The directive identified 17 critical infrastructure sectors and, for each sector, designated a federal Sector-Specific Agency (SSA) to lead protection and resilience-building programmes and activities. HSPD-7 allows for the Department of Homeland Security (DHS) to identify gaps in existing critical infrastructure sectors and establish new sectors to fill these gaps.

3.3. *Canada*

The National Strategy for Critical Infrastructure Protection (Canadian Government, 2014) sets the framework for strengthening the resilience of critical infrastructure in Canada. It gives emphasis to the resilience aspect of critical infrastructures as the ultimate goal to be achieved. A sectoral approach is used. However, interdependencies are taken into account. Resilience is not directly tackled at this level but it is part of the national strategy for CIP.

4. Past EU Projects

Six past EU projects have been identified as being relevant to the objectives of the RAMAPRT project. They listed in Table 1:

Table 1. Past EU Projects Relevant to Risk Assessment s for Terrorist Attacks.

EU Project	Duration	Objectives	Was RAM developed?	Does the RAM resolve Metro and Light Rail	Was software tool developed?	Was resilience included	Website
SECUR-ED	Apr 2011 - Sept 2014 (3.5yrs)	Demonstration project provide a set of counter-measure tools to improve urban transport security	Yes	No (only partly, countermeasures)	No (only a framework)	Yes (demonstration of counter measures)	http://www.secur-ed.eu/?page_id=10
SECURE-STATION	Jun 2011 - May 2014 (3yrs)	Development of a design guidance to address the risk of terrorist attacks in railway stations	Yes	No (party, only buildings)	Yes	Yes (Secure by Design)	http://www.securestation.eu/
SECURE-METRO	Jan 2010 - Dec 2012 (3 yrs)	Develop validated materials selection & structural design strategies for building metro vehicles with resilience to explosive & firebomb attacks.	No (applied adaptation of existing FAIR tool)	N/A (Developed KPIs specific to metro vehicles)	No	Yes	http://securemetro.inrets.fr/
EURACOM	Jul 2009 – Mar 2011 (2yrs)	Identify, together with European Critical Energy Infrastructures operators, a common and holistic approach (end-to-end energy supply chain) for risk assessment and risk management solutions.	Yes	No (wide and applied at high CI and country level)	No	No (covers energy supply chain)	http://www.eos-eu.com/?Page=euracom
RACAM	Feb 2009 – Jan 2011 (2yrs)	Develop a risk assessment framework & counter-measure auditing methodology to assess & mitigate vulnerabilities of metro systems against potential terrorist attacks.	Yes (a framework)	No	No	Yes (counter measure auditing methodology, not counter measures)	http://ec.europa.eu/dgs/home-affairs/financing/fundings/projects/stories/racam_en.htm
COUNTER-ACT	Jun 2006 – Oct 2009 (3yrs)	Development of a risk methodology for transport and energy sectors against terrorist threats	Yes	No	No	Yes (best practice countermeasures considered)	http://www.transport-research.info/web/projects/project_details.cfm?id=36152

5. Risk Assessment Methodologies (RAMs)

5.1. Review of EU and International Risk Assessment Methodologies

As a starting point, a review of EU and international RA methodologies was conducted, most of which were reviewed by the European Commission Joint Research Centre (Giannopoulos et al, 2012). See Table 2.

5.2. Commonalities and Differences between Risk Assessment Methodologies

Review of the risk methodologies presented indicates that there are more differences than commonalities. The main commonality is that most apply a linear approach to risk assessment where threats to assets (or targets) are identified following by evaluation of how much the asset is vulnerable to the threat. Finally, the consequence (or impact) of a successful attack is determined (seeFigure 2).

Although some methodologies were similar in some aspects, overall, they do not all agree on the following:

- Qualitative vs quantitative approach
- Detail (depth of data/information levels disaggregation)
- Scope (e.g. what threats/assets/sector covered?)
- What is target user group (legislators, management, technocrats, etc)
- Definition of asset criticality (physical assets, economical, operations, lives, etc).

- Degree of (human) subjectivity in whole RA process
- Is resilience included? (are countermeasures integrated)
- Are interdependences included (system or sectoral)?
- Common taxonomy/terminology

The differences do not necessarily represent a fundamental disagreement between the methodologies. However, they mostly indicate their specificities of areas of applications. For the RAMPART Project, these differences, also present an opportunity for differentiating itself for application in metro and light rail applications, with flexibility to cover other rail segments.

Table 2. Risk Assessment Methodologies.

Country/Region	Risk Assessment Methodologies
USA	• Better Infrastructure Risk and Resilience (BIRR) – USA • Protection of Critical Infrastructures - Baseline Protection Concept (BMI) – USA • CARVER2 – USA • Critical Infrastructure Modelling Simulation (CIMS) – USA • Critical Infrastructure Protection Decision Support System (CIPDSS) – USA • CommAspen – USA • Fast Analysis Infrastructure Tool (FAIT) – US • Multilayer Infrastructure Network (MIN) – US • Modular Dynamic Model – US • Agent-Based Laboratory for Economics (N-ABLE) – US • Net-Centric Effects-based operations MOdel (NEMO) - US • Network Security Risk Assessment modelling (NSRAM) – US • RAMCAP-Plus - US • Sandia Risk Assessment Methodology – US • RAND Corporation – US • Factor Analysis of and Information Risk (FAIR) – US (Not in JRC)
Australia	• Critical Infrastructure Protection modelling and Analysis (CIPMA)
European Union	• European Risk Assessment and Contingency Planning Methodologies for Interconnected Energy Networks (EURACOM) – EU • Cluster Of User Networks in Transport and Energy Relating to Anti-terrorist ACTivities (COUNTERACT) –EU • SECUR-ED Risk Management Methodology – EU
Norway	• DECRIS – Norway
Denmark	• Risk and Vulnerability analysis (RVA) - Denmark

5.3. Characteristics of a Complete Risk Assessment Methodology

Recognising that risk assessment is made up of three main components: Threats, Vulnerability and Impact, an effective RAM should be able to quantify and/or qualify all these. In order to be consistently effective in making these decisions, there is need to be able to compare the issues themselves, as well as the options and solutions that are available. In order to compare, there is need to measure, and measurement is predicated upon a solid definition of the things to be measured. All risk assessment approaches should include (The Open Group, 2009):

- An effort to clearly identify and characterise the assets, threats, controls, and impact/loss elements at play within the risk scenario being assessed.
- An understanding of the organisational context for the analysis (what is at stake?).
- Measurement and/or estimation of the various risk factors.
- Calculation of risk.
- Communication of the risk results to decision-makers in a form that is meaningful and useful.

Where a computer too is developed for a risk assessment methodology, the following aspects need to be considered: Complexity of the Model; Availability of Data; Iterative Risk Analyses; and Perspective.

6. Development of RAMPART Risk Assessment Specifications

6.1. Risk Assessment Requirements - Approach

The main output of RAMPART is a risk assessment methodology specific to metro and light rail undertakings, which are at risk of terrorist attacks. Recognising that there exist many RA methodologies, an analysis of current methodologies relevant to CIPs was conducted. Beneficial aspects of these were incorporated in the RAMPART Risk Assessment

Methodology (see Figure 3). Inevitably there may be deficiencies between the project requirements and those of existing methodologies. RAMPART will find solutions to these deficiencies to become inputs to the new methodology.

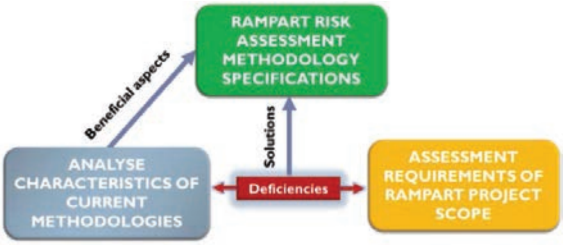
RAMPART RISK ASSESSMENT METHODOLOGY SPECIFICATIONS
Beneficial aspects
Solutions
ANALYSE CHARACTERISTICS OF CURRENT METHODOLOGIES
Deficiencies
ASSESSMENT REQUIREMENTS OF RAMPART PROJECT SCOPE

Fig. 3. Flow chart for developing the RAMPART RA methodology.

6.2. Selected RAMs for Detailed Review

As part of this research, over twenty risk assessment methodologies shown in Section 0 were considered (Matsika and O'Neill, 2015a). During an expert project meeting six methodologies were selected for detailed analysis. Selection was done based on the following: Scope; Sector; Treatment of qualitative vs quantitative approach; Taxonomy applied; and Relevance to metro and light rail applications. They were analysed to identify their strengths and weaknesses (see Table 3).

- **SEST-RAM:** Developed through the EC SECURESTATION project (Soehchen and Barcanescu, 2014).
- **RAMCAP Plus:** An all **hazards**/all infrastructures resilience oriented RAM, focusing on decreasing vulnerability by realisation of critical threats and scenarios, and increasing system's resilience (ASME-ITI, 2009).
- **NSRAM:** The focus of the Network Security Risk Assessment modelling (NSRAM) methodology is to determine the interconnected system response to different types of incidents and accidents (IIIA, 2015).
- **FAIR:** Factor Analysis of IT & Information Risk (FAIR) is a framework for creating and maintaining a threat-modelled **information** risk framework (Optical Risk, 2014).
- **FAIT:** This **tool** was developed in the US by the National Infrastructure Simulation and Analysis Centre to support DHS by determining the significance and the interdependencies of US critical infrastructures (Kelic et al, 2008).
- **RAND Methodology:** Scenario based qualitative RA cost effective evaluation. The scope of the work is railway sector and **terrorist** threats. The main strength of this methodology is the level of detail (88 different attack scenarios) that the model analyses (Ortiz et al, 2008).

Beneficial Aspects drawn from these RAs were:

1. Optimises the scope by avoiding unnecessary details and focusing on the most critical assets of a system (RAMCAP Plus)
2. Interdependencies – covering interconnected infrastructures with the objective is to determine how the systems respond and interact to various kinds of accidents and attacks (NSRAM, FAIT)
3. Probabilistic risk assessment (NSRAM, FAIR)
4. Quantification, less qualification (FAIR, RAMCAP Plus)
5. Asset Characterisation (identification) (FAIR, RAMCAP Plus)
6. Cost Benefit Analysis of countermeasures (NSRAM, RAND)
7. Cost based on asset valuation – monetary value (FAIR)
8. Targeted at CI operators and decision makers (RAMCAP Plus, NSRAM)
9. High visualisation capability (FAIT)
10. Scenario based (RAND)
11. Design for resilience (SEST-RAM)
12. Integrates evacuation (SEST-RAM)

RAMPART (additional or enhanced characteristics):

1. Combined effects that include loss of property and life.
2. Incorporates countermeasures/resilience
3. Highly abstracted
4. Cost benefit analysis
5. Detailed inventory of metro and light rail key assets

6. Threats: explosives IED/VBIED, CBRN, sabotage, cyber-attacks, Armmed attack , unarmed attack
7. Customised to metro and light rail applications
8. Is highly parametrised and leans more towards quantitative analysis as opposed to qualitative
9. Flexibility: Minimises subjectivity
10. Impact: casualties, injuries, out of hour service, physical damage

Table 3. Risk Assessment Methodologies Beneficial Aspects RAMPART Specifications.

RAM Tool	Developer	Objectives	Scope	Level of Abstraction	Target Group	Is resilience (counter-measures) incorporated?	Remarks
SEST-RAM	EC Project SECURESTATION	measures risk in relative rather than absolute terms	Design of rail stations for terrorist attack resilience	Medium	Technocrats and decision makers	Yes (with cost benefit)	Includes rapid evacuation
RAMCAP-Plus	American Society of Mechanical Engineers (ASME) (USA)	all hazards risk and resilience assessment methodology	all hazards/all infrastructures	Low (high-level approach)	CI operators and decision makers	Yes	
Fast Analysis Infrastructure Tool (FAIT)	National Infrastructure Simulation and Analysis Centre (USA)	determining the significance and inter-dependencies of US critical infrastructures	All infrastructure	high	Policy makers and decision makers	No	Impact assessment tool, not RA tool
Network Security Risk Assessment modelling (NSRAM)	Institute for Infrastructure and Information Assurance at James Madison University (USA	determine the interconnected system response to different types of incidents and accidents	flow-based analysis	Medium	Decision makers	Yes (with Cost benefit analysis)	
Factor Analysis of Information Risk (FAIR)	Risk Management Insight LLC, USA	creating and maintaining a threat-modelled information risk framework	IT/software	High	IT practitioners and Decision makers	Yes	
RAND Methodology	RAND Corporation	Scenario based qualitative RA cost effective evaluation	Railway sector and terrorist threats	High	Decision makers	Yes	Does not consider the additional scenarios

6.3. RAMPART Risk Assessment Methodology Specifications

As mentioned before, the RAMPART project has specific requirements or specifications aimed at addressing unique goals identified to address risk of terrorist attacks on metros and light rail. Key issues to consider include: Effectiveness of the methodology and any interdependencies among sectors or systems to be considered. Resilience is usually not included in the risk assessments review, although some RAs implicitly incorporate it.

7. RAMPART Risk Assessment Methodology

By applying the approach depicted in (see Figure 3), key factors that constitute a robust RAM were identified. This led to development of RAMPART specifications as described below:

7.1. Qualitative vs Quantitative Approach

According to the outcomes of the SECUR-ED project, a risk assessment in the public transport security should be done in a qualitative way. A quantitative assessment based on mathematical formulas and calculations is not possible due to a lack of statistics (especially concerning terrorist incidents) (Soehchen and Barcanescu, 2014). However, with projects such as SECUREMETRO, SECURESTATION, COUNTERACT and SECUR-ED completed, the amount of information gathered should allow for good quality semi-quantitative analysis. Further through the application of the FAIR methodology, the project SECUREMETRO demonstrated that risk can be quantified in economic terms. The decision to use qualitative or quantitative values should be driven by the needs and desires of those who will receive or base their decisions on the analysis results. The presence of the cost benefit analysis requires fully quantitative risk assessment approach.

7.2. *Detail (depth of data/information levels disaggregation)*

The RAMPART methodology is designed to cover risk down to asset and passenger levels. Even if asset value is taken into account, overall risk accounts for impact on lives. As such it captures data such as passenger numbers for a station on an hourly level.

7.3. *Scope (e.g. what threats/assets/Impact Category/sector covered?)*

Considering research carried out under EC projects, particularly the SECUREMETRO Project, four types of terrorist attacks are included. They represent the majority (over 90%) of potential threats to which metro and light rail systems are exposed. The threats considered include explosives, CBRN, sabotage and cyber-attacks (Armed attack and Unarmed attack).

7.4. *What is target user group (legislators, management, technocrats, etc.)*

RAMPART is best suited for application at company level, providing high level of detail. The targeted user groups include security department, rail operations mangers and management (decision makers).

7.5. *Definition of asset criticality (physical assets, economical, operations, lives, etc.)*

Determining the level of asset criticality plays a pivotal role in prioritising efforts for countermeasures and budget allocation. Through the project, a study was conducted to develop an inventory of vulnerable assets in the event of a terrorist attack (Matsika and O’Neill, 2015b). Further, the most critical assets were determined. From the literature, past terrorist attacks, semi-structured interviews with operators and observational studies, the following clusters of assets were identified as being exposed, and therefore vulnerable to terrorist attacks.

- **Moveable assets** (Metro Vehicles and Light Rail vehicles)
- **Fixed (non-moveable) assets** (Stations, Rail track, Systems and Peripheral infrastructure around)

The criticality of an asset can be determined in terms of one or combination of the following:

- Immediate direct economic value of asset?
- Spiral indirect effect on other activities (e.g. train operations, other linked business activities, etc.)
- Safety (injuries and loss of life)

In this project, a combination approach was applied. From the moveable assets, the ones considered to be most critical are: Railway vehicle interior; Electrical installations and Driver. Critical non-moveable assets were identified as Passenger waiting areas; Boarding platform; Operations/security control centre; Concrete sub layer; Tunnel structure; Signaling and Switches and Electrical supply.

7.6. *Degree of (human) subjectivity in whole RA process*

Although it applies a combination of quantitative and qualitative analysis, the model leans heavily towards quantitative analysis. Inevitably, however, the senior management should determine their levels of tolerance for each of the identified assets. Overall, the model minimises human subjectivity, thereby increasing the accuracy and repeatability of the model outcomes.

7.7. *Inclusion of Resilience (Integration of countermeasures)*

A risk assessment tool has enhanced usefulness if it integrates the ability to quickly bounce back after a successful attack, and also provide measures that make it harder for a successful attack. In the event that the attack is successful, the measures should result it minimal impact.

7.8. *Interdependences included (system and/or sectoral)*

With the application of the RAMPAT methodology being specific to metros and light rail, interdependencies incorporated mainly cover rail transport network ones. This means links to other transport systems (heavy rail and road) are taken into account. With the advent of increasing designs of interchanges, such interdependencies are critical. Today's interchanges mainly integrate heavy rail, metro, light rail and road (bus stations). In Europe, it is also becoming common for the interchange to be an integral part of a shopping mall.

7.9. *Common taxonomy/terminology*

Taxonomy adopted in this methodology applies that from the FAIR and RAND methodologies, with addition to cover the uniqueness of the RAMPART methodology.

8. Conclusion

A review of existing national and regional policy frameworks for Canada, EU and USA, together with associated national and sectoral risk assessment methodologies has been conducted. Specific to metro and light rail applications, RAMPART Project risk assessment specifications have been developed. They constitute nine factors and parameters: qualitative vs quantitative approach; detail (depth of data/information levels disaggregation); scope (e.g. what threats/assets/sector covered?); what is target user group (legislators, management, technocrats, etc); definition of asset criticality; degree of (human) subjectivity in whole RA process; is resilience included? (are countermeasures integrated); are interdependences included (system or sectoral?); and common taxonomy/terminology.

Acknowledgements

The authors would like to thank their respective institutions for the support rendered. They would also like to thank the European Commission for funding the research through Grant no.: HOME/2013/CIPS/AG/4000005116.

References

ASME-ITI, 2009. All-Hazards Risk and Resilience. Prioritizing Critical Infrastructures Using the RAMCAP Plus SM Approach. ASME Innovative Technologies Institute, LLC. ISBN: 978-0-7918-0287-8. Available on http://files.asme.org/ASMEITI/RAMCAP/17978.pdf

Canadian Government, 2014. http://www.publicsafety.gc.ca/prg/ns/ci/ntnl-eng.aspx, last accessed 02/09/2014.

EC, 2008. Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union, L345/75.

Giannopoulos G., Filippini R., Schimmer M., 2012. Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art. European Commission Joint Research Centre. Institute for the Protection and Security of the Citizen.

Herrera I.A., Woltjer R. 2010. Comparing a multi linear (STEP) and systemic (FRAM) method for accident analysis, Reliability Engineering and System Safety 95 (2010) 1269-1275.

Hollnagel E., Woods D. D., Leveson N. 2006. Resilience engineering: Concepts and precepts / [ed] UK: Ashgate Publishing Limited , 2006. ISBN: 0-7546-4641-6.

IIIA, 2015. NSRAM Infrastructure Modeling Tool. Institute for Infrastructure and Information Assurance (IIIA). http://www.jmu.edu/iiia/wm_library/Network_Security_Risk_Assessment_Modeling_(NSRAM)2.pdf

Ingleton, S., O'Neill, C., 2011. Deliverable D1.03 Definition of Attack Cases (Confidential). Work package 1 (Scenario Definition) under the EC Project Inherently Secure Blast Resistant and Fire Safe Metro Vehicles (SECUREMETRO) FP7 Grant Agreement no.: 234148.

Kelic A, Warren D. E., Phillips L. R., 2008. Cyber and Physical Infrastructure Interdependencies. SANDIA REPORT

Matsika E., O'Neill C., 2015a. Deliverable D1.1: Benchmarking Risk Assessment Methodologies. WP1 – Risk Assessment Formulations and Methodology. EC RAMPART Project Grant no.: HOME/2013/CIPS/AG/4000005116.

Matsika E., O'Neill C., 2015b. Deliverable D2.1: Key Assets Inventory. WP1 – Risk Assessment and Cost/Benefit Methodology Definition. EC RAMPART Project Grant no.: HOME/2013/CIPS/AG/4000005116.

Optical Risk (2014): Factor Analysis of Information Risk Methodology Brochure. Available at http://www.optimalrisk.com/Cyber-Security/FAIR-Methodology.

Ortiz D.S., Weatherford B.A., Greenberg M.D., Ecola L., 2008. Improving the Safety and Security of Freight and Passenger Rail in Pennsylvania. RAND Corporation.

Rinaldi S. M., Peerenboom J. P., Kelly T. K., 2001.Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies, IEEE Control Systems Magazine, December 2001, pp. 11-25.

SAND2008-6192. Unlimited Release.

Sterbenz J. P. G., Hutchison D., Çetinkaya E. K., Jabbar A., Rohrer J. P., Schöller M., Smith P. 2009. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. Computer Networks 54 (2010) 1245–1265.

The Open Group, 2009. Technical Standard. Risk Taxonomy. ISBN: 1-931624-77-1. Document Number: C081

US Government, 2014. http://www.dhs.gov/xlibrary/assets/NIPP RiskMgmt.pdf, last accessed 02/09/2014.