

# COUNTERACT

Cluster Of User Networks in Transport and Energy Relating to Anti-terrorist Activities

**EC Contract Number SSP4/2005/TREN/05/FP6/S07.48891**

**Coordination Action funded by the European Commission under the Sixth Framework Programme for Research and Development (2002-2006)**



**Project start date: June 2006**

**Project duration: 34 months**

**Date of delivery: October 2009**

**Deliverable 3**

**PT4: GENERIC GUIDELINES FOR CONDUCTING RISK ASSESSMENT IN PUBLIC TRANSPORT NETWORKS**

**FINAL REPORT 4**



TABLE OF CONTENTS

Executive Summary..... 4

Foreword..... 6

1 Introduction ..... 8

    1.1 What is a Risk Assessment?..... 8

    1.2 Why Risk Assessment?..... 9

    1.3 How to use these guidelines ..... 11

    1.4 Some notes on the methodology..... 13

2 Preconditions ..... 14

3 Guidelines for systematic structuring of operational diagram ..... 16

4 Definitions..... 20

    4.1 Threats..... 20

    4.2 Organisation specific Definitions ..... 21

        4.2.1 Definition of Probability of Occurrence ..... 21

        4.2.2 Definition of Impact/Severity ..... 22

        4.2.3 Definition of Risk-Categories ..... 24

5 Overview and Assessment of existing Safeguards ..... 25

6 How to assess Risks..... 27

7 Vulnerability Assessment ..... 31

8 Regular updates of Risk Assessments ..... 37

9 Glossary ..... 38

10 Further Reading ..... 41

11 Appendix 1: LIST of Potential Threats..... 43

    11.1 *General considerations* ..... 43

    11.2 *Tables of threats*..... 44

12 Appendix 2: Description of Potential Threats ..... 48

    12.1 Explosives attacks..... 48

        12.1.1 Improvised explosive devices ..... 48

        12.1.2 Timed Devices ..... 49

        12.1.3 Armed attack..... 49

        12.1.4 Suicide Bombing..... 50

    12.2 Hijacking..... 51

    12.3 Sabotage..... 52

    12.4 Arson Attack ..... 52

    12.5 Dispersion of chemical, biological or radiological agents. .... 53

    12.6 Using a vehicle as a weapon ..... 54

PT4	Generic Guidelines for Risk Assessment		2
-----	--	--	---

12.7	Intrusion in the information system (cybercrime) .....	54
12.8	Attack using dangerous cargo .....	55
13	Appendix 3: Concrete Example of a public transport operator conducting risk assessment.....	56
13.1	Introduction .....	56
13.2	Kick-off Meeting.....	57
13.3	Definitions.....	58
13.3.1	Threats .....	58
13.3.2	Definition of Probability of Occurrence .....	59
13.3.3	Definition of Impact/Severity .....	59
13.3.4	Definition of Risk Categories.....	60
13.4	Systematic structuring of the Public Transport System.....	61
13.5	Conducting the Risk Assessment .....	69
13.6	Final steps.....	74
13.6.1	Ranking of Results .....	74
13.6.2	Vulnerability Assessment.....	74
13.6.3	Evaluation of additional safeguards, Conclusion Report and Action Plan.....	74
14	Appendix 4: Testing the Guidelines .....	75
14.1	Involvement of the police .....	75
14.2	Trial and error .....	76
14.3	Adapting the guidelines .....	76
15	Appendix 5: Memorandum of Understanding .....	77
16	Appendix 6: Questionnaire for Public Transport Operators on Risk Assessment .....	78
17	Acknowledgements .....	82

## EXECUTIVE SUMMARY

Security is a relatively new concept in the context of public transport. Since the beginning, the core business of a public transport operator has been to transport passengers from one point to another in an economically beneficial way. Eventually, public safety became an important focus and the sector is now governed by a series of laws and guidelines with an aim to make public transport as safe as possible. In recent years, the issue of **security** has been added to the list of priorities: many public transport operators in Europe have witnessed an increase in criminality on their networks (vandalism, assault against drivers and passengers...), more recently terrorism has struck several networks in recent years with devastating effects.

Making a network free from crime and terrorism is impossible. Indeed, the intrinsic open and accessible nature of public transport, and the volumes of anonymous passengers present in the systems, makes it impossible to completely eradicate all security problems. This is further complicated by the fact that many operators are relatively inexperienced on how to combat effectively such issues.

It is in this context that the COUNTERACT project, funded under the 6<sup>th</sup> Framework Programme of the European Commission, was set up, to bring together knowledge on how to protect networks from security threats.

Experienced operators agree that there are many measures which can be taken to improve security. Some of them have been the object of studies in the COUNTERACT project. However, they agree that conducting a **security risk assessment** is a vital first step.

Many operators put security measures in place in an ad-hoc manner as and when particular security problems arise. For example, to combat vandalism and graffiti, many networks installed CCTV surveillance systems.

Whilst this is a natural way to proceed, it is neither structured nor methodical. Resources tend to be very limited for public transport operators. It is therefore advisable to find a structured and methodical approach to the allocation of resources for security purposes.



**Conducting a security risk assessment is the one and only method to assess needs in a systematic and analytically clear way.**

### What is a security risk assessment?

Through a series of workshops with key members of the organisation and external partners, each asset of the network is analysed by considering the **probability** of a threat occurring together with the **impact** that such a threat would have: this is the risk analysis. This is followed by a **vulnerability assessment** which assesses potential safeguards against the risks diagnosed.

Risk analysis + Vulnerability assessment = Risk assessment



**There are no agreed common definitions of *risk assessment, risk analysis, risk management, threat assessment, vulnerability analysis* and so on. Read very carefully the COUNTERACT definitions given in the glossary to understand fully the scope of these guidelines.**

### Benefits of Risk Assessment

Conducting a security risk assessment gives the operator a “picture” of the security risks to the network at the time the assessment was conducted. This “picture” helps the management team to decide where to invest resources. Apart from this basic usage, there are other benefits:

- justify where to invest resources, and where not to invest resources
- reveal where investment up until now may have been ineffective
- give management confidence in its decision-making
- revealing the risks can demonstrate to the authorities the need for further financial support

## Getting started

For those who already have an experience or an understanding of risk assessment, the methodology proposed in these guidelines will be relatively easy to follow.



For those who are discovering the risk assessment process for the first time, it is highly recommended to read this document in its entirety **twice**.

Another helpful tip for beginners is to take contact with a colleague who is experienced in risk assessment. Although these guidelines have been designed so that anyone, experienced or not, can use them independently, it is logical that support from an experienced colleague can be valuable.

## The steps involved

The actual steps involved in this process can be summarised as follows:

- read and understand the guidelines
- verify that you have full support from the following
  - management
  - external partners, e.g. law enforcement, authorities etc
  - relevant internal staff
- Workshop 1 – “Kick-off” – all relevant parties must attend, including those mentioned above, to decide scope of the study, distribution of tasks, agree definitions to be used, appoint workshop moderator, adoption of work-plan etc
- gather all necessary background information and arrange into an operational diagram
- Workshop 2 – “Risk Assessment”
- Ranking of results
- Vulnerability assessment
- A conclusions report to be submitted to management

## Estimated workload

The workload will depend on the size of the network, the resources allocated to carry out the process and how quickly support can be ensured from management and external partners, such as the police.

When the process was tested by an operator in Belgium (see appendix 4 – did not include the vulnerability assessment), the “Kick-off” workshop was held over one day. Three weeks later, the “Risk Assessment” workshop was held over two days. More time would have been helpful were it not for the constraints of the project deadlines.

The first time the process is carried out will be time-consuming. Once the process is integrated into the yearly operations of the network, repeat assessments will take much less time.

## Link to other security steps

As mentioned above, risk assessment is the first step in a coherent security policy of a public transport network. It is not a security measure in itself, but a tool to prioritise resources and which will help decide where and how measures need to be implemented. More information on security measures, planning and procedures can be found in the COUNTERACT study PT5<sup>1</sup>.

---

<sup>1</sup> COUNTERACT PT5 Public Transport Security Planning – Organisation, Countermeasures & Operations Guidance (see [www.colpofer.org](http://www.colpofer.org)) and UITP ([www.uitp.org/knowledge/projects.cfm](http://www.uitp.org/knowledge/projects.cfm))

## FOREWORD

From the beginning of the COUNTERACT project, developing guidelines for conducting risk assessment in public transport networks was considered a priority within the consortium and among the members of the Passenger Public Transport Thematic User Group (TUG).

As indicated in the *State of the Art Report* (Deliverable 1), security risk assessment is practiced in many of the large and experienced public transport (PT) organisations across Europe. However, the practice was clearly neither universal nor harmonized, especially among small and medium-sized operators. This was for a variety of reasons:

- A feeling that the terrorist threat does not apply to all;
- A perception of the daunting scale of the task;
- Lack of funding;
- Lack of understanding of the concept of a security risk assessment;
- No easily applicable methodology suited to public transport networks.

Therefore, one of the first and largest Targeted Studies undertaken by the Passenger Public Transport Cluster was to develop generic guidelines for conducting risk assessment in public transport networks.

The first step of the study team, led by UITP, involved carrying out extensive bibliographical research, with the support of subcontractor Mohamed Mezghani, on available risk assessment methodologies and practices. Various site visits were undertaken (for example to Lisbon Metro, RATP, London Underground and TMB) to gain a better understanding of the state of the art of public transport security risk assessment and how this fits into the overall security strategy of a public transport undertaking. This part of the study benefited from the close collaboration of some key TUG members who attended study meetings.

The second major step was issuing a questionnaire to public transport networks (see Appendix 6). The questionnaire was developed by the study team with the continuing support of subcontractor Hamburg Consult. The aim was to gather experience and material used by experienced public transport operators, but also to identify problems and weaknesses encountered by experienced and inexperienced operators.

The questionnaire was sent to the TUG as well as to a wide range of public transport operators throughout EU27.

Several phone interviews and site visits were carried out as a follow-up exercise to gain more insight into the responses gained through the questionnaire.

The next step was drafting the guidelines. Weekly conference calls of the PT Cluster with the relevant subcontractors ensured that each point was agreed upon and that the appropriate linkage was made with the other Targeted Studies under development, especially Targeted Study PT5: *Public Transport Security Planning – Organisation, Countermeasures & Operations Guidance*. Indeed, it is intended that these studies be read together. Risk Assessment is the first step to be undertaken (PT4) which will indicate to the operator what security planning needs to be done (PT5).

PT4	Generic Guidelines for Risk Assessment		6
-----	--	--	---

A further step in the development of the risk assessment guidelines was the Targeted Study PT2: *Exchange of Security Policy Experience of Public Transport Operators*. This study resulted in two exchange events being held in which table-top risk assessment exercises were carried out by the participants using the draft risk assessment guidelines and based on a fictive European city and public transport network. This was a chance to check that the guidelines were comprehensible and useable.

Secondly, an actual live test of the draft guidelines was carried out by a real public transport operator in Belgium (see appendix 4). This exercise was vital to ensuring the practical usability of the guidelines as well as their being able to produce a useful result. Happily, the test was a success and the operator in question was very satisfied with the results of the exercise.



**The following guidelines have been developed for any public transport organisation of any level of experience to conduct a security risk assessment.**

## 1 INTRODUCTION

### 1.1 What is a Risk Assessment?

A risk assessment is a step in the “risk management cycle”. In the security context, it is a procedure to assess the security risks to a public transport network by looking at the *probability* of a threat occurring on the network and the *impact* that such a threat would have. This is followed by a *vulnerability analysis* which assesses existing and potential safety and security provisions against the risks diagnosed. Once a risk assessment has been carried out, it can be used as a base for a structured, analytically clear and proportionate approach to security planning for a public transport network.



This document provides guidelines for carrying out a *qualitative risk assessment* of a public transport network. It should be read together with the COUNTERACT Targeted Study PT5: *Public Transport Security Planning – Organisation, Countermeasures & Operations Guidance* which provides the next step in the *risk management cycle*.



**Safety:** Risks refer to unintentional threats to technical or operational matters including severe weather conditions, accidents, etc. It covers problems that arise as result of an accidental danger. In this purpose, traffic-related safety includes accidents arising from **non-malicious** interactions among passengers, vehicles and pedestrians.

**Security:** Risks refer to intentional threats and include among others severe crime and terrorism.

## 1.2 Why Risk Assessment?

9/11 has changed the world: ever since, terrorist threats have to be acknowledged as a threat to open and democratic societies.

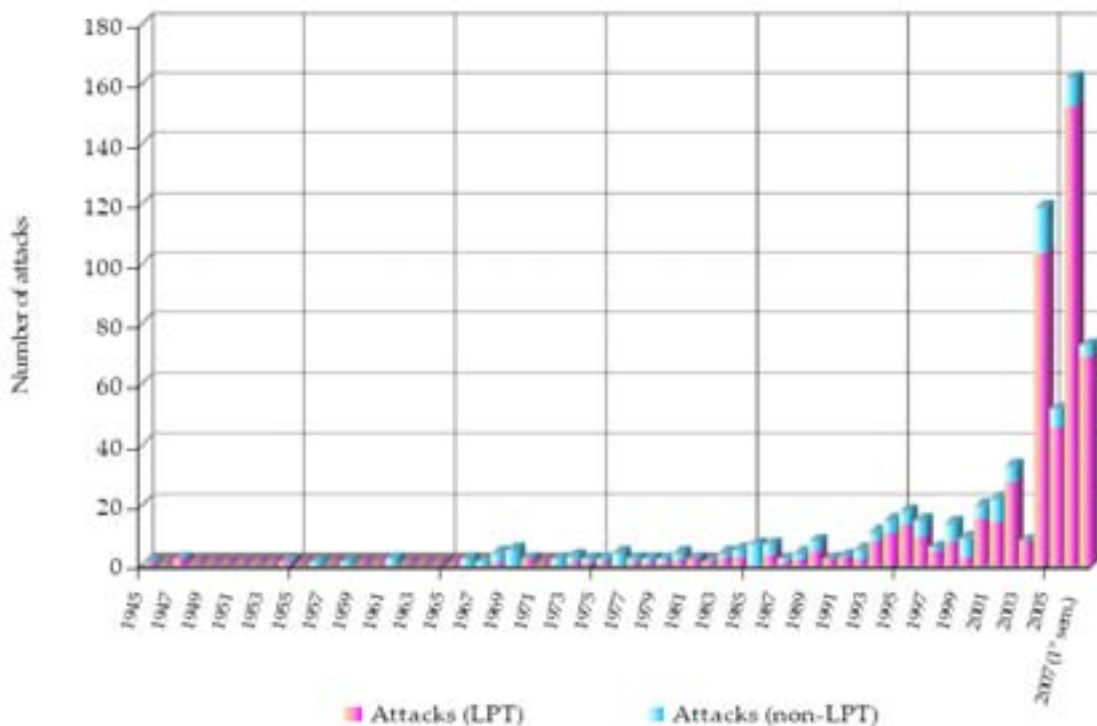
In Europe, any illusion of being a safe haven from terrorism was destroyed when bombs exploded in commuter trains in Madrid in 2004. Terrorism against public transport (PT) systems has struck in Moscow, London and other places. Fortunately, other attacks have been prevented or have failed for technical reasons, for example in regional trains in Germany.

The COUNTERACT project was designed to provide tools for public transport organisations to help them prepare for the terrorist threat. Providing guidelines for conducting risk assessment was identified as a key priority. Due to the scope of the project, the guidelines focus on terrorist threats; however, it can be easily adapted to other crimes (e.g. assaults against drivers or passengers) or even threats provided by natural events.

Public transport systems are soft targets for terrorism and serious crimes, because

- their open systems facilitate easy access and quick egress;
- the anonymity supports unnoticed preparation and impedes its discovery; and especially
- the high number of people gathering in closed and restricted environments makes them particularly vulnerable and provides maximum potential for casualties.

The frequency of all kinds of attacks against all transport systems world-wide has significantly increased over recent decades:



LPT = local public transport, comprising 'Railways' (trains, stations and rail lines), 'Subways', 'Buses' and 'Bus stops/Terminals'.

Non-LPT = non local public transport, comprising 'Aircraft', 'Airport', 'Convoy', 'Maritime' and 'Cargo Transport'.

Source: *Terrorism and Public Transport – An Analysis with a Focus on 1945-2007*, Alessia Nicotera, ASS.TRA. Associazione Trasporti and Luca Nicotera, A.T.A.C. SpA, 2009

Terrorists target people. They aim at mass killings in crowded spaces in order to attract maximum publicity for their cause. In general, urban transport systems are soft and therefore preferred targets for this perfidious aim; the PT locations are less protected by law enforcement due to the multitude of embarking/disembarking points and because of their vast extent. However, this is no excuse for doing nothing. Actually, soft targets can be hardened effectively! In order to prevent and mitigate attacks in the most effective as well as cost-efficient way, the logical first step must be carrying out a risk assessment of the transport operation. This is the content of these guidelines.

#### Good reasons for conducting a risk assessment:

- **A sound methodology:** Risk assessment is the one and only method to assess needs in a systematic and analytically clear way – instead of arbitrary – action;
- **A full picture:** Risk assessment creates an overview on a scalable base, so that it is possible to compare individual threats, risks and vulnerabilities. This is the precondition that the organisation can justly focus on these factors that can impact the organisation most severely. This approach establishes a solid and reasonable foundation for effective and cost efficient measures, or, on the other hand, substantiates why action has not been taken in a certain area;
- **Definition of priorities:** Risk assessment is a precondition for defining priorities in risk reducing measures. At the same time, risk assessment is a base to reveal unnecessary measures or identify better alternatives;
- **Basis for management's decision making:** Risk assessment produces risk rankings which may serve the management of an organisation in its decision making. A regular update of the risk assessment may also contribute to integration of safety and security matters in the operation's regular planning activities;
- **Communication and convincing stakeholders:** The management of the organisation may use the results of the risk assessment to communicate needs and back up claims, for example for funding of security activities by public authorities;
- **Legal and fiduciary obligation:** It goes without saying that it is obligatory for all public transport operations to live up to the highest standards in order to protect passengers, staff, and their core-business from any safety and security threats.



**While the main focus of this document is clearly on terrorism threats, conducting a risk assessment is never exclusively limited to one threat alone and may well help to discover weak points regarding all sorts of risks, including safety hazards and organisational procedures.**

The practical tools to carry out a risk and vulnerability analysis, i.e. risk assessment, are the contents of these guidelines.

### 1.3 How to use these guidelines

These guidelines are a tool for public transport operations to carry out risk assessments regarding security threats, i.e. terrorism and other serious crimes. They will support those persons within the operations in charge of security: in raising awareness as well as kick-starting, organising and carrying out the procedure. Finally, with the results of the risk assessment at hand, and with the COUNTERACT study PT5, effective countermeasures can be developed, justified and implemented.



**The guidelines can be used by any size of operator operating any and all modes.**

The approach to risk assessment presented in these guidelines is similar for large and smaller public transport systems, for those that are composed of several integrated systems, like bus, tram, metro and heavy rail, or systems that exclusively run one mode, for example buses. In principle, it does not matter whether the system serves an urban, a rural or a mixed area.

The successive steps are described as precisely as possible. However, every PT network has its specific circumstances, which cannot always be given due recognition to in these guidelines.

It goes without saying, that thorough preparation is indispensable for a smooth and successful risk assessment. The time requirement depends first of all on the depth of analysis and the availability of resources (mainly manpower).

Before starting the preparation of risk assessment, support from top-management from the start of the project, as well as the continuous supervision and guidance of the management, should be ensured.



**Support from top management is vital.**

One way of achieving continuous management involvement could be the creation of a dedicated Steering Committee.

The approach for risk assessment followed in these guidelines foresees team based analysis work, where a number of workshops are affected. The participants in the workshop (who assess the Probability of Occurrence and Impact/Severity of diverse threats), are the main guarantors of credible results. Therefore, the selection of the members in the workshop is of utmost importance.



**The selection of workshop members is crucial.**

The members must be highly experienced and responsible in their respective technical, operational or other field (e.g. Operational Control Centre, Security, High voltage, Building management, Financial, HR...), so that the joint assessments and working results of the workshop are not easily challenged. The number of the participants in the workshop depends – among others – on the resources available. It is recommended to appoint a working group with wide-ranging competencies from different backgrounds. In addition to internal experts, external experts should be included, especially law-enforcement agencies (including the police!), and others, for example for methodological support in handling the vast amount of data. However, the more participants are involved, the more complex the analysis might become as further aspects and perspectives will be added.

Possibly, the public transport operator and external experts, e.g. the police force, may formalise their cooperation by signing a Memorandum of Understanding, detailing the procedure, the input from all sides and the expected output of the undertaking (see appendix 5).

The workshop should start with agreeing on a work plan (see appendix 3), and precisely defining the terminology (based on the terminology suggested in these guidelines).

Obviously, risk assessment is focussing on highly sensitive matters. The confidentiality of the contents of work, especially the results and their documentation, must be ensured at all times. Adequate provisions must be made from the very beginning by, for example, issuing a confidentiality clause which must be signed by all workshop participants.

The table below details a step-by-step approach:

<b>Rough outline for an Activity Plan for Risk Assessment</b> <small>compare: RVA-model: The Danish Emergency Management Agency (DEMA) model for risk and vulnerability analysis</small>	<b>Date</b>
Consider and define the desired depth of analysis, delimitations and success criteria (e.g. “we will pay attention only to the metro network, during peak hours considering the threat of suicide attacks”).	
Develop a preliminary working-plan and calculate the required resources for carrying out a risk assessment	
Lobby for and ensure strong and continuous support and involvement of management (possibly creation of a dedicated steering committee)	
Kick-start and maintain mutual understanding and strong working relations with law enforcement agencies including the police	
Preparation of a workshop for the assessment of Probability of Occurrence and Impact/Severity of diverse Threats, including selection of internal/external members/participants	
Gathering of (background) information from internal and external sources; processing of data; structuring of PT network (in general) in an operational diagram; assessment of safeguards already existing and potentially available	
Preliminary meeting of workshop-members for agreeing on methodology, schedule, and definitions (range of Threats to be included/excluded, Probability of Occurrence, Impact/Severity, Risk-Categories, etc.)	
Detailed structuring of PT System in an operational diagram	
Final Preparations for Workshop	
Asset Study / Assessment of existing safeguards	
Carrying out Workshop for Risk Analysis	
Assessment of the results of the Risk Analysis	
Vulnerability Assessment; general overview of potential measures and safeguards including their costs, effectiveness, time for implementation, additional benefits, etc.	
Ranking of Risks, evaluation of highest risks and re-assessment with potentially added further safeguards	
Preparation of list with priority measures, i.e. those measures that are most effective, cost efficient, and realistic to implement	

<b>Rough outline for an Activity Plan for Risk Assessment</b> <small>compare: RVA-model: The Danish Emergency Management Agency (DEMA) model for risk and vulnerability analysis</small>	Date
Conclusions report, based on the risk assessment and identification of list of potential measures. At the same time, identification and documentation of any uncertainty in the analysis, as well as documentation of work process for quality assurance. Discussion of “tolerance criteria” for acceptable risks and vulnerabilities as well as cost estimates and implementation times for recommended measures.	
Preparation of executive summary and decision making outline for management, possibly supplemented with draft action plan containing precise tasks, responsible units/personnel, timelines, budgets, etc.	
Definition of frequency of risk assessment updates, both on a regular basis and to meet changed circumstances or new intelligence	

### 1.4 Some notes on the methodology

It must be clearly pointed out that there are many different ways to carry out risk assessments. A wide range of literature on this topic does exist and may be beneficial to consult. But the literature focuses on all different kinds of businesses and “critical infrastructures”, and is confusing at times. Unfortunately, neither the approaches (i.e. methodologies) are consistently and uniformly applied in the literature (and in practice), nor is the use of terminology coherent.

In order to conduct a security risk assessment for public transport systems, there are – in general – many different methodologies applicable. The methodology chosen and recommended in these guidelines is certainly not the only one that can be applied for this purpose. Others, for example more scenario-based approaches, might well be selected if considered more suitable by individual public transport operators.



**The approach presented here, has repeatedly and successfully been used by public transport operations of different sizes for this purpose and has proven to be feasible.**

For practical reasons, the methodology suggested in these guidelines is primarily based on the use of qualitative rather than quantitative data. Consequently, the assessment is not a purely objective process, but normative considerations impact on the results. The assessment is carried out using an index method, i.e. a level of Probability of Occurrence and Impact/Severity is determined. The methodology has many advantages:

- It can be applied to most types of organisations;
- It does not require that the users have prior knowledge of risk assessment;
- It facilitates and supports collective brainstorming and evaluation processes by experts from various backgrounds;
- It allows the inclusion of all different kinds of threats;
- It allows the inclusion of all phases of risk-management, i.e. prevention, mitigation and rehabilitation.

If you are interested in other methodologies, you may consult – for example – the following recommended publications, in which alternative approaches are described:

- Danish Emergency Management Agency, *DEMA's Approach to Risk and Vulnerability Analysis for Civil Contingency Planning, The RVAmodeI*, 2006
- Joint Technical Committee OB-007, *Australian/New Zealand Standard: Risk Management, AS/NZS 4360:2004*, Sydney, 2004<sup>3</sup>
- Bundesministerium des Inneren, *Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement. Leitfaden für Unternehmen und Behörden*. Berlin 2007 (please note: this publication is available in German language only)

## 2 PRECONDITIONS

### Ensuring Support from Top Management

What might sound like commonplace often turns out to be the most decisive factor: the top-management of the operation must acknowledge the potential threat of terrorism and other serious crimes, and put its active support behind reducing this risk. This requires allocating adequate resources, i.e. time, manpower, and money.

It might be reasoned by the management that countering terrorism and other serious crimes is the sole responsibility of law enforcement agencies, or that nobody can prevent terrorism anyway, and therefore PT operations should not engage in this issue. As a matter of course, security competes with other important matters, but these are not good reasons for ignoring this threat and the operation's responsibility to proactively mitigate this danger in a systematic way.

Set out below are some examples of scepticism for conducting risk assessment together with counter-arguments:

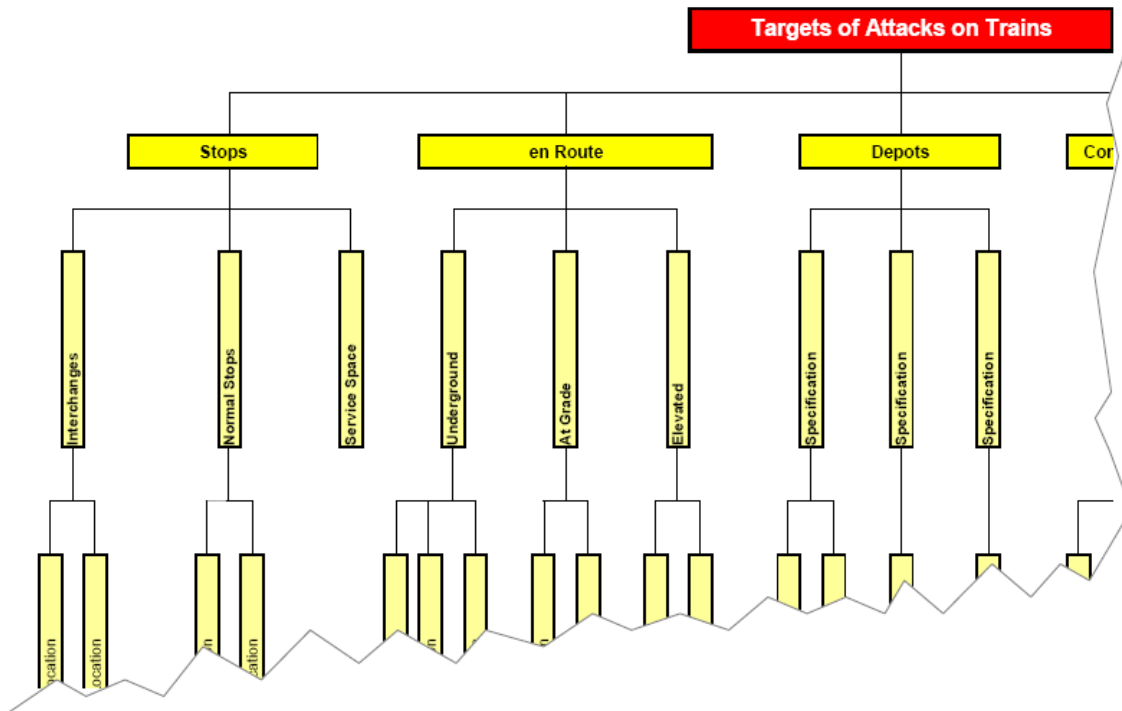
Scepticism	Beyond doubt
Anti-terrorism activities are the responsibility of law enforcement agencies!	True, but not exclusively: PT operations have the duty to provide their passengers and staff with highest levels of safety and security and protect their core business! They must assess risks and proactively take preventive or mitigating action.
Nobody can do anything against terrorism anyway!	Not true! Even though terrorism cannot be fully eliminated, soft targets can be hardened effectively <ul style="list-style-type: none"> <li>• Preventive measures can be implemented that <b>decrease the Probability of Occurrence</b> and</li> <li>• Mitigating measures can be implemented that <b>lessen the destructive Impact</b> in case an incident has occurred</li> <li>• <b>Incident management and contingency planning</b> must start proactively, and risk assessment is a precondition to get priorities right!</li> </ul>
We lack money and manpower to conduct a Risk Assessment!	Get the priorities right, and realise that Risk Assessment is part of the core business of a public transport operator!
We lack money and manpower to conduct a Risk Assessment!	Starting the process is an investment for the future. It is a way to insure effective transfer of knowledge when the security manager retires or leaves as the approach to security is systematic and the decision-making transparent and easy to trace.

<b>Scepticism</b>	<b>Beyond doubt</b>
<p>We lack money and manpower to implement countermeasures!</p>	<p>This is exactly why we need to carry out a risk assessment in order to spend our limited resources where they are most needed! Risk assessment allows us to identify the most urgent needs and set priorities accordingly!</p>
<p>We are not the capital city and we are not important enough to be a potential target for terrorists.</p>	<p>Terrorists target people and not cities. The fact that a PT-operation is not located in a capital city is a weak argument. On the contrary, this often means that the respective city and PT operation might be less covered by police forces. However, the PT network still does offer the same concentration of passengers on limited surfaces, making it a “suitable” potential target.</p> <p>There are examples of terrorist attempts in non-capital cities, for example the attempted bombings of regional trains in Germany in 2007 which did not take place in the capital but in far smaller cities.</p>
<p>There is little European legislation concerning passenger transport security. Risk and vulnerability assessments are rarely required by regulators; therefore we are not obligated to conduct a risk assessment.</p>	<p>A systematic risk assessment process may heighten the “security culture” within passenger transport networks, in order to make staff and managers aware of the threats they could face. If the risk assessment is conducted regularly, it may also contribute to integrating safety and security issues into routine activities and business functions.</p>

### 3 GUIDELINES FOR SYSTEMATIC STRUCTURING OF OPERATIONAL DIAGRAM

In order to identify possible targets for attacks it is necessary to structure the whole PT system in an operational diagram.

It might be useful to start with a brainstorming session to collect the first input from internal and external experts. This input should be incorporated in a visualised structure that depicts the whole system. The following graph is a cut out from an example rail system. A similar drawing should be made for all sub-systems, i.e. heavy rail, metro, light rail/tram, bus, and other, for example ferry.



This visualisation may support the discussion and assessment in the later workshops for the qualitative risk-assessment. In any case, the comprehensive structure must finally be listed in a matrix, as shown below and explained in the chapter on Risk Assessment (when each part of the system is assessed regarding Probability of Occurrence and Impact/Severity of each potential threat).

	<p><b>The challenge is to get the right degree of specification, i.e. neither too general (risk of overlooking crucial aspects), nor too detailed (risk of getting drowned in data)</b></p>
--	---

Matrix for qualitative Assessment (Metro)				Threat														
				Atomic Bomb	Dirty Bomb	Biological Weapon	Chemical Weapon	Person Attack	Bomb Threat	ED	Car Bomb	Rocket-Propelled Grenade	Suicide Attack					
Station	Target																	
	Location A	Specification	Specification															
	Location B	Specification	Specification															
	Location C	Specification	Specification															
	Location D	Specification	Specification															
	Location E	Specification	Specification															
	Location F	Specification	Specification															
	Location G	Specification	Specification															
	Location H	Specification	Specification															
		Specification	Specification															

Back to structuring the system: As a first step, it is recommended to discuss general aspects in a brainstorming session with internal and external (law enforcement/police) experts from various fields:

- How severe are the threats for their own network?
- How attractive is the city/region for terrorists compared to others?
- How attractive is the PT-system for terrorists compared to other potential targets in the city/region?
- Which system elements are most attractive for terrorists?
- Which parts of the network are most critical to the operation?

**Relevant aspects to investigate, which may increase the “attractiveness” of parts of the system as a target for attacks:**

- Number of passengers in interchanges/stations/stops, vehicles (at peak times)
- Nodes and intersections / Role and Importance for network
- Geographical and geological distinct features that could facilitate attacks or impede response efforts and therefore increase the potential impact, e.g.
  - Low lying location (e.g. where vehicles can be spotted and attacked easily from higher ground)
  - Locations with deep /steep sided cuttings
  - Deep tunnels
  - Elevated
  - Underneath major structures
  - Remote locations where the response would be difficult
- Symbolic importance
  - of part of the system or
  - of adjacent buildings
  - Postcard-view of station/infrastructure that could produce “strong” images in media coverage after an attack
- Special/Large events organised nearby (adjacent or where PT carries the visitors) that could temporarily raise the risk level
- Special dates (anniversaries)

- Temporary building works
- Institutions/Organisations nearby that generate a group of passengers, which is at special risk (e.g. political or religious groups)
- Cash handling
- Is there a history of attacks? Have there been attacks in the past?
- Areas with easy access of vehicles to sensitive areas at close range, e.g. stations and critical assets

**Key aspects to structure the whole PT system in an operational systematic:**

- What are the different parts of the system?
  - Heavy Rail
  - Metro
  - Light Rail/Tram
  - Bus
  - Other, e.g. Ferry
- What Supporting Infrastructure and People are in the system?

These are examples therefore this is not a complete list.

Operational Infrastructure with public access	
	Interchanges <ul style="list-style-type: none"> <li>▪ Elevated</li> <li>▪ At-grade</li> <li>▪ Underground</li> </ul>
	Stations <ul style="list-style-type: none"> <li>▪ Elevated</li> <li>▪ At-grade</li> <li>▪ Underground</li> </ul>
	Tracks/Routes <ul style="list-style-type: none"> <li>▪ Elevated</li> <li>▪ At-grade</li> <li>▪ Low lying location</li> <li>▪ Underground</li> </ul>
Operational Infrastructure and Equipment with restricted access	
	Air-conditioning and ventilation of <ul style="list-style-type: none"> <li>▪ Stations</li> <li>▪ Vehicles</li> </ul>
	Head office Cash centres

	Main Operations Control Centre (OCC)
	Security Control Centre (if different from OCC)
	Fall-back Operations Control Centre
	Regional Control Centre / Sub-Operations Control Centre
	Operational and technical rooms in the system
	Empty and unused rooms in the system
	Data processing centre
	Power supply / traction current
	Electricity network
	Control and communication system / network
	Depots
	Workshop
	Stabling yard/Parking including rolling stock or bus fleet
<b>Staff</b>	
	Operation Security Administration

- How to categorise the different parts of the transport system in a comprehensive and analytically clear way?



**It is crucial to develop a structure for the whole system that is comprehensive (no omissions or a wrong Risk analysis might be formulated!) and has no overlaps!**

## 4 DEFINITIONS

Well thought out definitions are indispensable for the qualitative risk assessment to produce reliable and coherent results.

The range of potential threats is almost unlimited. Before 9/11 hardly anyone had perceived civilian aircrafts as potential rockets in the hands of terrorists. For practical reasons, the number of threats and potential scenarios that shall be assessed by the PT operations must be limited and agreed upon first.

Then, definitions for “Probability of Occurrence”, “Impact/Severity” as well as for the different “Risk-Categories” must be found.

The definitions presented in these guidelines shall serve as a starting point.



**Since each PT operation has its specific environment and needs, the proposed definitions must be checked regarding their applicability in the given circumstances, and more than likely they must be modified.**

After starting to fill out the matrix, it may become apparent that the chosen definitions are not entirely suitable and need to be modified accordingly.

The different categories can also be *named* differently to the categories suggested here. However, these definitions have been chosen specifically to differ from the vocabulary usually associated with *safety* aspects, or conducting *safety risk assessment in order to avoid confusion*. For example, UITP's *Manual for the Development of Bus Transport System Safety Management*, the 'safety threats' are referred to as 'hazards' and are categorised from unacceptable, undesirable, acceptable (with review) and acceptable.

### 4.1 Threats

#### Coordination with Law Enforcement Agencies / Collaboration

Public transport operations cannot and need not take over responsibilities from law enforcement agencies. However, it is essential that PT operations establish and maintain a regular dialogue with law enforcement agencies – especially with the police – to allow exchange of current intelligence and receipt of threat information.

Individual Member States and maybe even regions and single cities within a given Member State assess the threats differently.



**PT operations should seek the participation of law enforcement agencies (police forces) for the preparation and execution of risk assessment.**

#### Definition of Threats and Scenarios

A Threat is defined as an event that may cause an incident in the organisation, producing material damage or non physical losses (e.g. fear of using transportation mode) in its assets. (For safety issues, “threats” are referred to as “hazards”.)

An incomplete list of potential threats is given below and briefly described in Appendix 1. It should be taken into consideration that some threats are a “living matter”, i.e. always changing.



**The cumulative effects of incidents need to be given due consideration when the impact/consequence of the threats is evaluated.**

- Improvised Explosive Devices (IED) using materials such as military or commercial explosives, e.g. landmines or improvised explosives;
- Assault Weapons, Standoff Weapons and use of Standard Explosives (Hand grenades, Rocket Propelled Grenades, Shooting);
- Suicide bomb;
- Vehicle borne IED (VBIED) – ‘car/vehicle’ bombs;
- Arson and Improvised Incendiary Device - IID (e.g. “Molotov cocktails”);
- Hijacking;
- Sabotage;
- Weapons of Mass Destruction: Chemical/Biological/Radiological/Nuclear (CBRN-E).

## 4.2 Organisation specific Definitions

The qualitative assessments of risks require analytically clear definitions. The starting point for the definitions presented below was the Euro Norm EN 50126, which treats safety and security in a wider sense. The Euro Norm has been modified and further developed so that it meets the practical requirements of sensible risk assessment in the context of public transportation

Two factors determine the risk of an attack:

- Probability of Occurrence;
- Impact/Severity of Occurrence.

Combining the two components Probability of Occurrence and Impact/Severity results in a portfolio, which allows the user to identify risks easily and to display these risks with utmost clarity. Why and how risks have been assessed then becomes transparent and traceable. This provides a solid base for any further action.

The risks may be grouped in categories. While there are general indicators for the definition of Probability of Occurrence, Impact/Severity and Risk Categories (presented below), all the definitions must be carefully checked regarding their applicability in the specific circumstances of every single PT operation, and modified accordingly. For example, the damage (impact) caused by a certain threat – say, the loss of 20 buses – may be merely painful for a large operation, but potentially critical for the survival of a smaller operator.

### 4.2.1 Definition of Probability of Occurrence

The Probability of Occurrence is the possibility of a threat being executed, which is measured in escalating categories (that need to be defined).

Here, the Probability of Occurrence is divided into five escalating steps (although the number of steps can be slightly adapted), starting with “Very unlikely” up to “Very high”. The criteria for the differentiation between the different steps focus – among others – mainly on the frequency the threat has been executed in their own or in other PT operations.

Probability of Occurrence	Definition Criteria <small>(derived from Euro Norm 50126)</small>
<b>Very high</b>	The threat can be executed at any time and/or has been executed within the organisation repeatedly
<b>High</b>	It has to be reckoned with the threat being executed repeatedly. The threat has been executed within the own organisation once.
<b>Possible</b>	An execution of the threat has to be reckoned with. The threat has been executed repeatedly within other PT operations world-wide, or at least once within a PT operation in the own/neighbouring country
<b>Low</b>	The threat is executed rarely, but has been executed in isolated cases in other organisations (world-wide)
<b>Very unlikely</b>	An execution of the threat is extremely unlikely, and the threat has never been executed in other PT operations before

*NB the definitions above are examples and should serve as a starting point for discussions: in fact, everything can be discussed ! In order to tailor the risk assessment to your specific operation, it is highly recommended to discuss, amend and agree on all the definitions as appropriate.*

#### 4.2.2 Definition of Impact/Severity

Impact/Severity stands for the damage to an asset arising from the execution of a threat, which is measured in escalating categories (that need to be defined).

Impact/Severity of threats are ordered in four escalating categories (although the number of categories can be slightly adapted) starting with "Uncritical", "Marginal", "Critical" and finally "Disastrous". The definition mainly takes into account the consequences of the various threats for persons and property or the environment on the one hand, and for the PT Operator and the service provision on the other hand.

As previously mentioned, "disastrous" can mean different things depending on the size and scope of the operation in question. It is strongly recommended to properly distinguish several categories, i.e. to experiment with and test the definitions in order to ensure, that the assessment generates results in different risk-categories.



**If the "disastrous" category is too global, then most squares of the matrix will be categorized as "intolerable" (red) and the benefit of the exercise will be lost.**

Impact/Severity	Definition Criteria	
	(derived from Euro Norm 50126)	
	Consequences for <b>Persons</b> and/or <b>Property/Environment</b>	Consequences for <b>PT Operator</b> and <b>Services</b>
<b>Disastrous</b>	Several (to be defined by Operator) deaths and/or numerous severe injuries and/or most severe damage to property and/or environment	Loss of vital functions and/or operation over a long (to be defined by Operator) period of time
<b>Critical</b>	Low (to be defined by Operator) number of deaths and/or severely injured and/or severe (to be defined by Operator) damage to property and/or environment	Loss of vital functions and/or operation over a short period of time
<b>Marginal</b>	Light casualties and/or notable damage to property and/or environment	Minor impact on functions and/or operation
<b>Uncritical</b>	Possibility of few light casualties and/or small damage to property and/or environment	No impact on functions and/or operation

*NB the definitions above are examples and should serve as a starting point for discussions: in fact, everything can be discussed. In order to tailor the risk assessment to your specific operation, it is highly recommended to discuss, amend and agree the definitions as appropriate.*

#### 4.2.3 Definition of Risk-Categories

The combination of Probability of Occurrence and Impact/Severity results in the “Risk” categories. In order to differentiate the risk more precisely within the four risk categories, the five categories for “Probability of Occurrence” as well as the four categories for “Impact/Severity” may be attributed with escalating numbers (starting with one). Then, the numbers for “Probability of Occurrence” and “Impact” may be multiplied. The resulting figures allow for a more precise ranking of the different risks even within the said categories.

The “Risk” categories may also be illustrated by colours. This makes the final result very visually clear:

Probability of Occurrence	Risk Categories			
Very high (5)	Tolerable (5)	Precarious (10)	Intolerable (15)	Intolerable (20)
High (4)	Tolerable (4)	Precarious (8)	Precarious (12)	Intolerable (16)
Possible (3)	Negligible (3)	Tolerable (6)	Precarious (9)	Precarious (12)
Low (2)	Negligible (2)	Tolerable (4)	Tolerable (6)	Precarious (8)
Very unlikely (1)	Negligible (1)	Negligible (2)	Negligible (3)	Tolerable (4)
	Uncritical (1)	Marginal(2)	Critical (3)	Disastrous (4)
	Impact / Severity			

The risk-categories are linked with the countermeasures, as shown in the following table:

Risk-Category	Score	Action Required
Intolerable	15-20	Must be avoided or Impact must be mitigated as far as possible
Precarious	8-12	Shall only be accepted if the efforts for prevention and/or mitigation of impact is unreasonable high
Tolerable	4-6	Shall be accepted, but threat needs to be assessed regularly
Negligible	1-3	Shall be accepted

It is important that the group and the management team feel comfortable with the choice of wording for the risk categories. The notion of a “tolerable” or “intolerable” risk is clearly subjective. Sometimes a risk is tolerable because there is nothing which can be done to change it. Other times management can choose to label a risk tolerable for other reasons.

The risk-categories can be named in another way, for example “inconsequential”, “perceptible”, “precarious” and “significant” for the purposes of the exercise, and a further step would be for the Management to evaluate which are tolerable and which are intolerable.

## 5 OVERVIEW AND ASSESSMENT OF EXISTING SAFEGUARDS

Many safeguards are already in place in the PT operation. Most safeguards for safety-aspects are applicable to security-threats, for example regarding fire, evacuation procedures and crisis communication. Therefore most aspects are not mentioned twice in the following tables on Safety and Security Safeguards.

However, in some cases, second thoughts might be given to security particularities, for example to secondary devices threatening rescue efforts and assembly/evacuation points, or the psychological impact on rescue-teams due to rumours of radiological contamination after an explosion of a (dirty) bomb.

Safeguards are relevant in all phases, before, during and after a potential threat may be executed, i.e.

- **Preparedness** before a potential threat may be executed including preventive/detection measures;
- Capacities for **response**, relief and mitigation, during an incident;
- Capacities for **recovery** after an incident has occurred.

Safety Safeguards
Design Principles <ul style="list-style-type: none"> <li>○ Transparency (i.e. clear sightlines)</li> <li>○ Clearing out (e.g. by removing unnecessary furniture, vending machines, etc.)</li> <li>○ Improvement of lighting levels</li> <li>○ Etc.</li> </ul>
Equipment
Fire protection (including direct fire protection, ventilation, etc.)
Operational standards/Instructions/Guidelines
Collaboration agreements
Line of communication <ul style="list-style-type: none"> <li>○ Internal</li> <li>○ External</li> </ul>
Crisis communication
Overall preparedness plan as well as Contingency planning with detail
Crisis management group/structures
Evacuation <ul style="list-style-type: none"> <li>○ Rules &amp; procedures</li> <li>○ Training &amp; exercises</li> </ul>
Training/Education of operational staff
Exercises (tabletop / real)

Security Safeguards
CCTV
Emergency buttons/SOS telephones
Guards/patrols/intervention teams with vehicles/Patrols with canines
Dialogue and joint (tabletop/real) exercises with law enforcement agencies (especially with police)
Perimeter control and intrusion detection/anti-intrusion systems
Access regulation and control/organisation of keys
Identification procedures
Design principles - construction
CBRN-E detection
Staff vetting
Back-up systems
Security screening and inspection procedures

## 6 HOW TO ASSESS RISKS

You are now ready to conduct the risk analysis.

The PT system has been structured in a systematic way in the operational diagram and this must now be organised into the matrix templates for each sub-system (i.e. heavy rail, metro, light rail, bus, etc.)

The columns on the left show the different locations of the system (according to the graph on structuring the system as shown before).

The rows on the right indicate all threats deemed possible.

It has proven most effective to draft this table as an Excel-Sheet and print it out in large format (e.g. in ISO A0 format). Alternatively, you can use a projector, so that all participants in the workshop can see and visualise the table. This table should be filled in during a workshop, in which experts from various backgrounds discuss and assess the Probability of Occurrence and Impact/Severity of all the threats for all the locations in all the sub-systems. This is a laborious task that might require two days or more of intensive work (depending on the size of the system). The internal and possibly external experts should cover all relevant aspects for the qualitative assessment of threats according to the agreed definitions



**Make sure that the group stays coherent over the entire workshop, and that fluctuation of workshop-members is minimal.**

For a coherent assessment, well thought out definitions are necessary. However, the definitions should act as a starting point for the discussion of each case and the overall impression of the group should also be taken into account.



**Do not be “fundamentalist”, i.e. do not stick to the definitions to the letter, but always put logic and reason first! If necessary, modify or change the definitions as you go (trial and error), so that the results you produce are coherent and logical!**

In case definitions are changed, you **MUST** go back to the start and re-define all assessments with the new definitions!



**Assign someone to document from the very beginning the reasons behind the individual assessments, so you can always recapitulate how the assessment derived.**

From this point on, the whole analysis becomes more complex. A solid structure and possibly methodological support by experienced people are necessary in order not to get drowned in the flood of data.



**Assign someone to permanently crosscheck the assessments regarding logic and coherence to earlier decisions.**

The participation of representatives from law enforcement agencies, for example the police, is extremely beneficial, provided they are willing to participate. Refer to appendix 3 in which the benefits of involving the police is highlighted.

The experts participating in the assessment must be experienced and must have a recognised knowledge about the system, so that they can add their weight to the results of the analysis. Otherwise the outcome of the risk-assessment could be challenged – especially if results are not flattering.

Remember:



**Always remember: due to the nature of the subject you often have to make assessments based on incomplete information.**



**Make sure that the group stays coherent over the entire workshop, and that fluctuation of workshop-members is minimal.**



**Do not be “fundamentalist”, i.e. do not stick to the definitions to the letter, but always put logic and reason first! If necessary, modify or change the definitions as you go (trial and error), so that the results you produce are coherent and logical!**



**Assign someone to document from the very beginning the reasons behind the individual assessments, so you can always recapitulate how the assessment derived.**



**Assign someone to permanently crosscheck the assessments regarding logic and coherence to earlier decisions.**



**Always remember: due to the nature of the subject you often have to make assessments based on incomplete information.**

Matrix for qualitative Assessment (Metro)				Threat													
				Atomic Bomb	Dirty Bomb	Biological Weapon	Chemical Weapon	Arson Attack	Bomb Threat	ED	Car Bomb	Rocket-Propelled Grenade	Sniper Attack				
Station	Target		Specification														
		Location A	Specification	Specification													
	Location B	Specification	Specification														
	Location C	Specification	Specification														
	Location D	Specification	Specification														
	Location E	Specification	Specification														
	Location F	Specification	Specification														
			Specification														
	Location G	Specification	Specification														
	Location H	Specification	Specification														
			Specification														
			Specification														

It is recommended that the results of the verbal assessment regarding Probability of Occurrence and Impact/Severity be marked by colours according to the risk categories. Such colours clearly indicate and visualise, where the greatest risks are to be found, and it shows, where preventive or mitigating action is needed:

Matrix indicating Risks (Metro)			Type of Attack														
			Type of Attack A	Type of Attack B	Type of Attack C	Type of Attack D	Type of Attack E	Type of Attack F	Type of Attack G	Type of Attack H	Type of Attack I	Type of Attack K	Type of Attack L	Type of Attack M	Type of Attack N		
Station	Target		Specification														
		Location A	Specification		Yellow	Orange	Grey				Yellow	Green	Green	Green	Green	Green	Green
	Location B	Specification		Yellow	Yellow	Red	Red	Red	Red	Yellow	Green	Green	Green	Green	Green	Green	Green
	Location C	Specification		Yellow	Yellow	Red	Red	Red	Red	Yellow	Green	Green	Green	Green	Green	Green	Green
	Location D	Specification		Yellow	Yellow	Red	Red	Red	Red	Yellow	Green	Green	Green	Green	Green	Green	Green
	Location E	Specification		Yellow	Yellow	Red	Red	Red	Red	Yellow	Green	Green	Green	Green	Green	Green	Green
	Location F	Specification		Yellow	Yellow	Red	Red	Red	Red	Yellow	Green	Green	Green	Green	Green	Green	Green
			Specification														
	Location G	Specification		Yellow	Orange	Red	Red	Red	Red	Yellow	Green	Green	Green	Green	Green	Green	Green
	Location H	Specification		Yellow	Yellow	Red	Red	Red	Red	Yellow	Green	Green	Green	Green	Green	Green	Green

The results of the analysis can be used to “experiment” with: they can be ranked according to different considerations, e.g. according to locations, as demonstrated in the graph below.

Risks ranked according to Locations							
No	Target					Type of Attack	Risk Category
1	Location / Specification		Location	Specification		Type of Attack A	Red
			Location	Specification		Type of Attack A	
2 to 7	Location / Specification	Specification	Location	Specification		Type of Attack B	Red
			Location	Specification		Type of Attack B	
			Location	Specification		Type of Attack B	
			Location	Specification		Type of Attack B	
			Location	Specification		Type of Attack B	
8 to 26	Location / Specification	Specification	Location	Specification	Specification	Type of Attack C	Orange
						Type of Attack D	
			Location	Specification	Specification	Type of Attack B	
			Location	Specification	Specification	Type of Attack B	
			Location	Specification	Specification	Type of Attack C	

Alternatively, the results of the analysis can be ranked according to threats and types of attack, as illustrated in the graph below.

This is an excellent way to demonstrate the need for specific action, for example to decision makers with little time.

Risks ranked according to Type of Attack						
Type of Attack	Target					Risk Category
1. Type of Attack A	Specification		Location	Location		Red
			Location	Location		
			Location	Location		
	Specification	Specification				Yellow
	Specification	Specification				Yellow
	Specification	Specification				Green
2. Type of Attack B	Specification	Specification	Location	Location	Location	Red
			Location	Location	Location	
	Specification		Location	Location		Red
			Location	Location		
	Specification	Specification	Location	Location	Location	Orange
	Specification					

## 7 VULNERABILITY ASSESSMENT

Now that the matrix is complete, it clearly indicates where the greatest risks are to be found, and it shows where preventive or mitigating action is needed. Therefore, this analysis should be the solid base for any action, because:

- It prevents ineffective action;
- It enables decision makers to make the most efficient use of scarce resources by optimally targeting their investments in safety and security.

The logical next step is the Vulnerability Assessment.



**The Vulnerability Assessment is applied to detect gaps and weak points in the prevention and mitigation of threats and incidents as well as diagnosing potential for optimising the safeguards of the PT system.**

Basically, the Vulnerability Assessment is analysing potential additional safety and security provisions against the risks diagnosed in the previous step (see Safety and Security Safeguards in Section 5 on page 15), i.e. do – and to what extent – the existing and planned safeguards match the diagnosed risks?

With this approach the most urgent action is identified. Based on the identification of weak-points, suitable measures for prevention and mitigation can be developed.

The assessment of potential measures and safeguard could include – and are most likely:

- Costs;
- Effectiveness;
- Time for implementation;
- Additional benefits regarding safety-aspects (increasing the lighting level for the use of CCTV cameras will facilitate evacuation) or service/comfort of passengers, improving the security perception of passengers /staff, reduction of vandalism, etc.
- Insurance impact

Target within PT-System	Threat		Risk-Category & Ranking BEFORE	Risk-Category & Ranking AFTER	Current Approach with its difficulties & deficiencies	Possible new Approach for Prevention & Mitigation	Costs	Remarks
	Type of Threat	Specification						
Target in PT-System	Type of Threat	Specification	20	16	ABC...	DEF...	...€	...
Target in PT-System	Type of Threat	Specification	20	15	GHI...	JKL...	...€	...
Target in PT-System	Type of Threat	Specification	15	12	MNO...	PQR...	...€	...
Target in PT-System	Type of Threat	Specification	12	8	STU...	VWX...	...€	...
Target in PT-System	Type of Threat	Specification	9	6	YZA...	BCD...	...€	...
Target in PT-System	Type of Threat	Specification	8	4	EFG...	HIJ...	...€	...
Target in PT-System	Type of Threat	Specification	6	4	KLM...	NOP...	...€	...
Target in PT-System	Type of Threat	Specification	3	1	QRS...	TUV...	...€	...
Target in PT-System	Type of Threat	Specification	2	1	WXY...	ZAB...	...€	...

The development and implementation of preventive and mitigating measures is the contents of COUNTERACT study PT5: *Public Transport Security Planning – Organisation, Countermeasures & Operations Guidance*, and therefore not detailed here.

The table above allows for experimentation. The risk categories and the ranking (according to the assessed product of Probability of Occurrence and impact/severity) before and after certain preventive/mitigating measures will have been implemented, are an ideal preparatory work and basis for decision making by the management.

The broad list of potential measures and safeguards has been refined in the described process, and a list with clear priorities has been developed. Priorities are taking into account the level of risk, the effectiveness and cost-efficiency as well as the time frame for implementation of potential safeguards.

Finally, the priority list of safeguards recommended for implementation is elaborated in a report. The report should clearly identify and comment on uncertainties, limitations and simplifications in the risk assessment and may also require more detailed investigations into certain aspects, if necessary.

The final report should be prepared in a standard format, so that it can be used for quality assurance and referred to in future analyses.

An executive summary with a brief overview of the crucial findings of the risk assessment, as well as the recommendations should be prepared for senior management decision making. The management may ensure the adequate integration of the findings and recommendations in the continuous preparedness planning. Senior management may ask for an action plan to be drafted that outlines:

- Which measures shall be implemented, when and where;
- The rationale behind the measures;
- The organisation and/or personnel in charge of implementation;
- The resources required for implementation.



**Elaborate findings in a report.**



**Prepare an executive summary of report.**



**Repeat the risk assessment study regularly.**

Let's take an example:

Imagine that we have a metro station called Central Station with a very large main entrance.



A lot of vehicles can park just in front of this entrance which brought us to the conclusion during the Risk Assessment study that the Risk level for the car bomb threat at this location has to be considered as "Intolerable" (level 16 based on Risk analysis where occurrence factor is "high" and impact / severity factor is "disastrous"):

Matrix <b>METRO</b> (Qualitative Assessment)				Dirty Bomb	Chemical Weapon	Biological Weapon	IED	Arson Attack	Car bomb	Rocket-Propelled Grenade	Suicide Attack	Hijacking	Sabotage	Bomb Threat	Hold-up (cash)	Unspecified Threat
				VLO	VLO	VLO	POS	POS	HIG	POS	POS	POS	POS	VHG	LOW	
<b>Target</b>																
Stations particularly exposed	Central Station	Centre	Leo, Railway, busses	DIS	DIS	CRI	DIS	DIS	DIS	CRI	DIS	CRI	MAR	MAR	MAR	

Going on site, we came to the conclusion that the best way to mitigate the risk was to place bollards in front of the entrance preventing vehicles parking there or worse, partially entering the station.

We looked for information, found potential providers and asked for offers.

This best offer has been submitted to the management with a report summarizing the situation (pictures of the site, results of the Risk analysis, way to reduce the risk):

Target within PT-System	Threat		Risk-Category & Ranking BEFORE	Risk-Category & Ranking AFTER	Current Approach with its difficulties & deficiencies	Possible new Approach for Prevention & Mitigation	Costs	Remarks
Central Station	Car bomb	Explosion	<b>16</b>	<b>N.A.</b>	Open space, no limitation of parking	Place bollards	8848.00€	To be done ASAP

The proposal was approved by the management (small budget needed) and the bollards ordered.

Order placed by:		National Metro Company		ORDER FORM			
Object:		Delivery and putting in of security bollards at the "Central Station"		LOCATION: CENTRAL STATION			
Reference:		2009-NMC-4525J		v.01			
Art. Nr		DESCRIPTION OF THE ORDER / DESCRIPTION OF THE WORKS TO BE PERFORMED	Unit	Qty	Unit Price in Eur (€)	Total price in Eur (€)	
		<i>Outside Location</i>					
		01 Parking area in front of main entrance					
		<b>1. PHYSICAL SECURITY</b>					
1	B01	Delivery of bollards (precise localisation to be confirmed)	Pcs	8	995	7960	
2	B02	Accessories for bollards (Mounting plates, bolts, nuts...)	Pcs	8	45	360	
3	S03	Putting in	Hrs	24	22	528	
		<b>Total</b>				<b>8.848,00</b>	

And placed.



Finally, we reconsidered the situation of Central Station regarding the car bomb threat after the improvement.

First factor: Occurrence

The only possible conclusion is the “not applicable” category: it is no longer possible to let a car explode directly in front of or inside the main entrance of Central Station.

Second factor: impact / severity

If a car explodes beyond the zone protected by the bollards, any damage will be negligible and will have no impact on the metro traffic.

Remark

We also realised that the bollards implementation also has an impact on the mitigation of other risks not specifically linked to terrorism



Conclusion

We have to conclude that the risk of a car bomb explosion in front of the main entrance of the Central Station no longer exists, thus we have to update the Risk analysis matrix, turning from “red” (intolerable) to “grey” (not applicable).

Matrix METRO (Qualitative Assessment)			Dirty Bomb	Chemical Weapon	Biological Weapon	IED	Arson Attack	Car bomb	Rocket-Propelled Grenade	Suicide Attack	Hijacking	Sabotage	Bomb Threat	Hold-up (cash)	Unspecified Threat
			Stations particularly exposed	Central Station	Centre	VLO	VLO	VLO	POS	POS	POS	POS	POS	POS	POS
			DIS	DIS	CRH	DIS	DIS	DIS	CRH	DIS	CRH	MAR	MAR	MAR	

## 8 REGULAR UPDATES OF RISK ASSESSMENTS

Threats and risks are not static but subject to change. Therefore, they should be assessed at regular intervals, for example yearly. In case of actual incidents, organisational changes/restructuring, acquisition of more assets, a one-off large event or even a change in the national threat level, an earlier reassessment (than the planned regular interval) may be necessary.



**The responsibility for updating the risk assessment should be anchored in one organisational unit.**

The updating should be facilitated so that it does not interrupt daily routines, but takes place as a natural element in the organisation's preparedness planning. It is clear that conducting risk assessment is an iterative process: risks are interdependent with the safeguards in place, i.e. adding and improving safeguards will impact on the assessment of risks.



As mentioned above, this sound methodology is putting threats and risks in a wider picture. Its systematic and analytical clarity allows a sound definition of priorities, and therewith creates a solid base for decision making. Decisions can be reasoned and communicated using the results of the risk assessment, and scarce resources are used in a most effective and cost efficient way in order to satisfy legal and fiduciary obligations.

Following this way of thinking peer reviews could be conducted after completion of the initial assessments to review the results. This may result in clarification of certain aspects of the assessments, confirmation that the results are in line with their own assessments and to recommend changes if they differ. This could be seen as a safeguard against the danger of intense "group dynamic" negatively impacting the assessment. It may also provide reassurance to top management of the credibility of the results.

Peer reviews could be conducted by other internal or external stakeholders, by colleagues from other public transport operators or authorities, or by experienced consultants.

## 9 GLOSSARY

<b>Asset</b>	Any person, part or feature of a system that has a value. Assets can be classified into physical assets, human assets, software assets, information assets, etc.
<b>Attack</b>	Any deliberate action designed to harm a system
<b>Biological agents</b>	Living organisms or the materials derived from them that cause disease in or harm to humans, animals, or plants or cause deterioration of material. Biological agents may be used as liquid droplets, aerosols, or dry powders.
<b>Bomb-Threat</b>	Handling of Bomb Threats (e.g. by mail or phone), which are experienced by many public transport operators, should be included in the standard operating procedures of the operation. Therefore, they are not described in this guideline. Such issues are addressed in the COUNTERACT study PT5.
<b>Chemical agent</b>	A chemical substance that is intended to kill, seriously injure, or incapacitate people through physiological effects. Generally separated by severity of effect (e.g. lethal, blister, and incapacitating).
<b>Control</b>	Safeguard
<b>Countermeasure</b>	Safeguard
<b>Crime</b>	<p>An act or commission of an act that is forbidden or the omission of a duty that is commanded by a public law and that makes the offender liable to punishment by that law. Crime can be divided into four main categories:</p> <ul style="list-style-type: none"> <li>- Reported</li> <li>- Unreported</li> <li>- Unacknowledged</li> <li>- Undetected</li> </ul> <p>The majority of crime is represented by the last three categories.</p>
<b>Cyber attack</b>	Damage to, unauthorized use of, or exploitation of, and, destruction of electronic information contained therein to ensure confidentiality, integrity, and availability of information networks and wireline, wireless, satellite, public safety answering points, communications and control systems.
<b>Degradation</b>	The loss of value of an asset as a result of the execution of a threat, e.g. the amount of damage done to an asset
<b>Dimension</b>	An aspect that allows the value of an asset to be measured in the sense of the damage that would be caused by its loss of value.
<b>Dirty bomb</b>	A device designed to spread radioactive material by conventional explosives when the bomb explodes. A dirty bomb kills or injures people through the initial blast of the conventional explosive and spreads radioactive contamination over possibly a large area—hence the term “dirty.” Such bombs could be miniature devices or large truck bombs. A dirty bomb is much simpler to make than a true nuclear weapon. See also <i>radiological dispersal device</i>

<b>Hyper-terrorism</b>	Terrorism with intent to maximize casualties, no warnings or negotiation possible. Often used to describe large scale terrorism since 9/11.
<b>Impact</b>	The damage to an asset arising from the execution of a threat, measured in escalating categories (to be defined)
<b>Incident</b>	Organisations in Member States use various terms, such as 'attack' and 'incident', to describe the wide range of circumstances that can involve, or potentially involve, security issues. For the purpose of this document, the term 'incident' covers: <ul style="list-style-type: none"> <li>▪ The term 'emergency' and the range of circumstances from minor to very serious incidents.</li> <li>▪ Deliberate security acts intended to kill and injure, damage equipment and infrastructure, disrupt operations and achieve publicity for the perpetrator, such as a threat, suspicious object, actual attack or hijack.</li> </ul>
<b>Nuclear detonation device</b>	An explosion resulting from fission and/or fusion reactions in nuclear material, such as that from a nuclear weapon.
<b>Probability of occurrence</b>	The possibility of a threat being executed, measured in escalating categories (to be defined).
<b>Radiological dispersal device</b>	A device that disperses radioactive material by conventional explosive or other mechanical means, such as a spray. See also <i>dirty bomb</i> .
<b>Residual impact</b>	The impact of a threat remaining after the implementation of the safeguards described in the security plan.
<b>Residual probability of occurrence</b>	The probability of an execution of a threat remaining after the implementation of the safeguards described in the security plan.
<b>Residual risk</b>	The risk of a threat remaining after the implementation of the safeguards described in the security plan.
<b>Risk</b>	The degree of exposure to a threat. The risk increases with the impact and the probability of a threat being executed. Risk is measured in escalating categories.
<b>(Security) Risk analysis</b>	A tool for to analyse potential threats to a system in a systematic way. This includes the identification of assets and a classification according to their criticality. The analysis of a range of potential threats regarding their probability of execution, and their potential impact is also part of a risk assessment
<b>(Security) Risk assessment</b>	. (Security) Risk analysis plus vulnerability assessment
<b>Risk management</b>	The process of identifying security actions (selection and implementation of safeguards) that are suitable to know, prevent, reduce or control the risks identified through a risk assessment.
<b>Safeguards</b>	Any action, device, procedure, technique, or other measure that mitigates risk by reducing the vulnerability of a system, the impact from a threat being executed, or the probability of a threat being executed.
<b>Safety Risks</b>	Unintentional hazards to technical or operational matters including severe weather

	conditions, accidents, etc.
<b>Security Risks</b>	Intentional threats including among others severe crime and terrorism.
<b>Terrorism 1</b>	An intentional act of violence that is intended to inflict significant damage to property, produce panic and fear and most of all inflict casualties.
<b>Terrorism 2</b>	The unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.
<b>Threat</b>	An event that may cause an incident in the organisation, producing material damage or non physical losses (e.g. fear of using transportation mode) in its assets.
<b>Tiger-kidnapping</b>	To abduct someone, or to hold someone hostage, in order to persuade someone else to assist in a crime, e.g. a person of importance to the victim is held hostage as collateral until the victim has met the criminal's demands. It is called <i>tiger</i> kidnapping because of the predatory stalking that precedes it.
<b>Vulnerability</b>	The gap between safeguards of a system and the identified risks, i.e. where safeguards are not sufficiently meeting the security requirements/containing the risks.
<b>Weakness</b>	A part of a system that can be exploited by a threat.

## 10 FURTHER READING

- Anon., *International Ship and Port Facility Security ISPS code*, International Maritime Organization, London, UK, 2004.
- ASIS International, "*General Security Risk Assessment Guideline*", 2003
- Bundesministerium des Inneren, *Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement. Leitfaden für Unternehmen und Behörden*. Berlin 2007
- Danish Emergency Management Agency, *DEMA's Approach to Risk and Vulnerability Analysis for Civil Contingency Planning, The RVAmode*, 2006
- European Commission, COUNTERACT project, "PT1: *Impact Assessment on Rail and urban passenger transport security at the European Level regarding terrorist threats in railways and urban passenger transport*", Final report, Nov. 2006
- European Commission, COUNTERACT project, "PT5 *Public Transport Security Planning Guidance*", March 2009
- European Standard EN 50126 Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS). English Version. European Committee for Electrotechnical Standardization. ISBN 0 580 35694 9
- FEMA 452, Risk Management Series: Risk Assessment. A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings. U.S. Department of Homeland Security, 2005
- Joint Technical Committee OB-007, *Australian/New Zealand Standard: Risk Management, AS/NZS 4360:2004*, Sydney, 2004<sup>3</sup>
- *Manual for the development of bus transport system safety management*, UITP, 2007
- R.V. Matalucci, *Risk Assessment Methodology for Dams (RAM-D<sup>SM</sup>)*, Proceedings of the 6<sup>th</sup> International Conference on Probabilistic Safety Assessment and Management, 2002. Pages: 169-176.
- M. Mueth, "*Risk assessment for public transport systems*", EU/UITP Anti-Terrorism International Conference, London 2005
- NICOTERA, Luca & NICOTERA Alessia, *Terrorism and Public Transport – An Analysis with a Focus on 1945-2007*, A.T.A.C. SpA & ASS.TRA. Associazione Trasporti, January 2009
- North American Electric Reliability Council's, Critical Infrastructure Protection Committee, "*Risk-Assessment Methodologies for Use in the Electric Utility Industry*", Sept. 2005
- SAIC, "*An introduction to chemical, biological, and radiological threat agents*", September 2005
- *Security in ports, ILO and IMO code of practice*, International Labour Office, Geneva/ International Maritime Organization, London, UK, 2004.
- *Security vulnerability assessment methodology for the petroleum and petrochemical industries*, American Petroleum Institute (API) and National Petrochemical & Refiners Association (NPRA), 2003.
- L.J.P Speijker, C.J.M. de Jong, M.K.H. Giesberts, O. Laviv, D. Shumer, D. Gaultier, "*Risk assessment of newly proposed concepts to improve in-flight security*", 25<sup>th</sup> International congress of the aeronautical sciences, Sept. 2006
- Transit Security Design Considerations, FTA. Cambridge, MA, 2004
- United States Government Accountability Office, "*Passenger rail security: Enhanced Federal Leadership Needed to Prioritize and Guide Security*", Report to Congressional Requesters, Sept. 2005

PT4	Generic Guidelines for Risk Assessment		41
-----	--	--	----

- United States Government Accountability Office, "*Risk management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*", Report to Congressional Requesters, Dec. 2005
- *Vulnerability assessment methodology–electric power infrastructure*, US Department of Energy – Office of Energy Assurance, 2002. [http://www.esisac.com/publicdocs/assessment\\_methods/VA.pdf](http://www.esisac.com/publicdocs/assessment_methods/VA.pdf)

## 11 APPENDIX 1: LIST OF POTENTIAL THREATS

### Preliminary Remark

Although the COUNTERACT project ended in March 2009 and on the request of the EC, the present work has been updated with an extended list of possible threats. The reader will thus be able to select the threats to be taken into consideration.

The list of threats provided here below comes from the draft of the deliverable 9.1 from MODSafe (Modular Urban Transport Safety and Security Analysis) part of the European Commission Seventh framework programme.

### 11.1 General considerations

#### Threats

A distinction is generally made between conventional and unconventional threats. The rationale stems from the clear distinction between two very different classes of weapons:

Weapons of mass destruction (WMD) on one hand,  
Traditional or conventional weapons on the other.

This fundamental distinction is based on obvious major differences between the two:

WMD are controlled by heads of state, delivered on order by strategic forces, subject to sophisticated handling and delivery procedures and meant to cause mass casualties and extreme prejudice;

Traditional weapons in contrast are available to the general public, otherwise can be improvised or home-made (see IED), are extensively used by various perpetrators and cause far less casualties and collateral damage to property.

From these two clearly identified levels of threat stem the following two categories of threat:

- **Unconventional threats:** This category chiefly includes hyper terrorism or Chemical, Biological, Radiological and Nuclear (CBRN) threats and state-sponsored large scale cyber attacks targeting another state or the operations of an international group.

- **Conventional threats:** This second category includes all other threats than those mentioned in the first category of threats. Their modes of operation are not necessarily inclusive of any kind of weapon (e.g. verbal assault, theft, property vandalism, etc.). Within the scope of conventional threats, there is a further need to distinguish between external and internal threats to transport security:

o **External threats** are exogenous to a given system. They are due to the outer environment of a given transport operator,

o **Internal threats** are endogenous to a given system. They are due to the inner environment of a given operator and are generally management-related issues (e.g. lack of understanding of the threat, of vision, of response; of preparedness; Under qualified staff, etc.).

## 11.2 Tables of threats

**Table 1 – Unconventional threats**

<b>11. Offence against humanity (persons &amp; property)</b>	
Mass destruction (CBRN-related)	Chemical agent
	Biological agent
	Radioactive <sup>2</sup> dispersal device (e.g. radioactive material, dirty bomb)
	Nuclear detonation device
State-sponsored large-scale cyber attacks	Massive strategic strike on a State, an international business group

**Table 2 – Conventional threats (internal, from 21 to 25 and external, see 26)**

<b>21. Offences against persons &amp; property</b>	
Terrorist attacks <sup>3</sup> (domestic and/or international)	Arson (large scale e.g. forest fires, buildings)
	Bombing(s) (single, multiple)
	Mass shooting(s)
	Use of a standoff weapon (e.g. rocket propelled grenade)
	Use of a VBIED (vehicle borne improvised explosive device, e.g. car, truck, airplane)
Violence from groups	Gang fights, confrontation (e.g. in stations)
	Riots, mass demonstration
<b>22. Offences against persons</b>	
Arson	Small scale fire (e.g. carriage, dust bin)
Assault with non lethal weapons	Acoustic and optical systems
	Chemical agent in gas form (e.g. tear gas, pepper spray etc.)
	Chemical agent in liquid form (e.g. acid throwing)
	High voltage system (e.g. <i>Taser</i> )
	Millimetre radio waves
	Rubber bullets

<sup>2</sup> It should be noted that radiological materials are not always Weapons of Mass Destruction (WMDs)

<sup>3</sup> Listing by alphabetical order

	Torching (criminal use of inflammable liquids and setting fire to victim)
Assault with physical violence and theft	Robbery
	Robbery with threat
Assault with physical violence only	Attempted rape and/or fondle and/or frotteurism
	High jacking
	Hostage taking
	Kidnapping / Tiger-kidnapping
	Rape
	Spittle
	Stabbing (knife or sharp object)

<b>22. Offences against persons (continued)</b>	
Assault with theft only	Robbery
Assault with neither physical violence nor theft	Aggressive behaviour
	Peeping
	Use of abusive language
	Up skirt photography
Deliberate crash with fatalities (cf. sabotage)	Collision between 2 trains
	Collision with an obstacle on the railway
	Derailment
	<i>Idiosyncratic</i> projectile (e.g. airplane)
Deliberate collapse of infrastructure on persons	Bridge collapse
	Flooding in a sub-aqua tunnel
	Tunnel collapse
Murder	Including premeditated murder
Shootings	Sniper shooting (e.g. random or targeted)
Theft without assault (Theft from person)	Picking pockets
<b>23. Crime against property (material &amp; immaterial)</b>	
Property damage, degradation, destruction (Criminal damage)	Engraving
	Projectile throwing (e.g. stoning)
	Shooting against rolling stock
	Small scale arson
	Tag, graffiti
Other threats	Hoax

Property theft	Theft (robbery, burglary, swindle, stealing information)
Sabotage	Bombing to disrupt traffic
	Causing collision
	Causing derailment
	Cutting energy supply (e.g. traction power, station)
	Cyber attack (small scale by other than State)
	Destruction of electronics by electromagnetic pulse (EMP)
	Misuse of a security system
<b>23. Crime against property (material &amp; immaterial) Continued</b>	
Sabotage (continued)	Interfering with signalling or power equipment
	Neutralization of door system
	Paralysis of train movement by non-lethal weapons (e.g. use of super adhesives and bindings to immobilise vehicles; catenary's sabotage)
	Puncture of tyre
<b>24. Other offences related to traffics and behaviour</b>	
Behavioural offence Public Disorder offences	Abusive use of personal audio devices
	Begging
	Drunkenness
	Exhibitionism
	Hawking
	Non compliance with animals rules
	Non compliance with smoking rules
	Soliciting (prostitution)
Vagabonds (homeless, squatters, etc.)	
Other illegal activities	Consuming illegal products
	Illegal sales (tickets, other item)
	Production and sale of counterfeit tickets
Traffic violations	Trafficking (drugs, weapons, etc.)
	Misuse of safety devices (alarm button, hammers)
	Obstruction to traffic (e.g. occupation of the tracks, obstruction of station entrance)
	Suicide on the tracks

Trespassing	Access to restricted areas Illegal access on track
	Crossing of railway tracks by a vehicle
	Crossing of ticket barrier (fare evasion)
	Illegal use of reserved lanes by a vehicle
<b>25. Other external or exogenous threats</b>	
Overcrowding (safety hazard that can have an impact on the feeling of insecurity if not managed)	
<b>26. Internal or endogenous threats</b>	
Corporate / Operator weaknesses	Managerial dysfunction, under qualified staff, lack of preparedness, unclear command chain, etc.
Vengeful employee or former employee	Sabotage

## 12 APPENDIX 2: DESCRIPTION OF POTENTIAL THREATS

### 12.1 Explosives attacks

Explosives are efficient weapons for terrorist attacks because of the large number of casualties and the physical damage they can cause with relatively low cost and easy-to-obtain means. In most cases, so-called Improvised Explosive Devices (IEDs) are used. These are explosive device created by terrorists using available materials e.g. timing devices, means of detonation, explosives (commercially available or 'home-made') and other articles, such as nails or ball bearings, for additional impact. IEDs may use components of military explosive articles. An IED may also contain incendiary materials.

There are various ways to carry out an explosive attack:

- Improvised explosive devices (IED): the device is planted by the attacker and is detonated either remotely by the attacker or automatically by some external force (e.g. like land mines);
- Timed devices: containing an arrangement enabling the period before detonation to be preset;
- Armed attack/launched explosives: the attacker is at the scene at the time of the attack, but the time of detonation is delayed allowing the attacker to launch the device at the target without himself being injured or killed (e.g. hand grenades); and
- Suicide bombing: the attacker blows himself up with the explosion.

#### 12.1.1 Improvised explosive devices

***Such IED's can be either remotely detonated by the attacker, or the attacker can leave the detonation to be triggered by some external force, e.g. the target running over the device.***

The advantage of remotely or automatically triggering an explosives attack is the possibility for the attackers to escape and continue the terrorist campaign elsewhere. The main disadvantage for the attacker of automatically triggering the detonation is that he can exert no control on the moment of detonation, and thereby can never be 100% sure that the target is really affected.

Attackers detonating an IED remotely have to, depending on the target, plant the device in advance, or hide the device, possibly amongst other items. In terms of detonation, the terrorist will either favour a delayed timer device, detonate from line of sight or electronically. The disadvantage of the latter possibility is that the attacker has no means to control the time of explosion, thereby risking a much smaller impact than planned. There has to be careful planning and preparation to avoid detection.

Two broad sizes of explosive device can be considered:

- small explosive, e.g. portable explosives that can be carried into a passenger transport system;
- large explosive, e.g. VBIED (Vehicle Borne Improvised Explosive Device), which is an IED carried in a vehicle enabling a large IED to be delivered.

The consequences of such potential attacks depend on the different station types within public transport networks. The risk to produce greater casualties is higher in underground stations (confined spaces) than ground level or elevated stations (open air spaces).

The remote character of the attack makes it possible to detect the device before detonation, leaving a larger chance of countering the attack.

**The case of Madrid, March 2004**

The 2004 Madrid bombings caused significant disruption to the capital's transport network. The explosion resulted in the tragic loss of 190 lives, with about 1400 passengers injured. Though different sources claim that the bombings are likely to have played a role in the results of the political election that took place in Spain just after the attacks, the economic impact was rather marginal. The fast recovery proves that a city can swiftly bounce back from attacks and that the economic cost can be relatively short-term, even in the terrorism sensitive tourism sector. Just after the events, 90% of customers had been lost and both passengers and RENFE staff suffered from psychological problems. However, the city reacted quickly responding with success to the need for communication campaigns to regain customers' confidence and for increased security in the transport system, upgrading the equipment of stations and through extensive staff training.

**The case of Michgaon, April 2007**

On the evening of April 27<sup>th</sup>, 2007, five security personnel were killed in a landmine blast triggered by Maoist rebels in Michgaon village of Kanker district, about 175 km south of Raipur (India). As many as 18 security men were also injured in the blast. Their condition was stated to be serious. 'The blast destroyed the front portion of a bus the policemen were travelling in', a senior police officer said. The police team was returning from Pakhanjore in the bus when the landmine exploded at a village near Durgukondal on the Bhanupratappur-Pakhanjore-Bande road.

*12.1.2 Timed Devices*

These contain a timer or some chemical means which can be preset or arranged to give a predetermined period before detonation occurs. They can be used with both IEDs and VBIEDs. Devices of this type were often used in the bombing campaigns targeting transport in Great Britain in the 1970-1990s as a result of IRA campaigns. Many of the considerations previously identified for remotely detonated devices also apply to timed devices.

**The case of Assam, June 2004**

Six people were killed when an explosion ripped through a passenger bus in the north-eastern Indian state of Assam. The attack occurred early on June 24<sup>th</sup>, 2004, in Sivasagar, 360km east of state capital, Guwahati.

At least 17 other passengers were injured as the bus caught fire following the blast. The police said the outlawed United Liberation Front of Assam (Ulfa) was responsible for the incident. The group is fighting for a separate homeland. The incident happened when a time bomb exploded in a passenger bus near the village of Mathurapur.

*12.1.3 Armed attack*

Another way to carry out an explosives attack is to use a device with a small time delay between triggering and explosion.

Attackers carry the device and trigger the delayed detonation near the scene of the attack. The launching could either be manual (hand grenades, Molotov cocktails) or demand more advanced machinery (rocket propelled grenades, missile launching). The way of launching also determines the impact of the attack. Manually launched explosives will have a limited size and thereby cause limited damage, unless they trigger a second explosion. Automatically launched devices are often larger and cause greater damage. In the case of manually launched explosives, the attacker could simply carry the device with him/her near the targeted area, without being detected. In the case of automatically launched devices the attacker will probably be at a distance of the scene, limiting the chance of being caught.

Use of standard firearms and other infantry weapons have been prominent in past terrorist and criminal action on and against subway and rail systems. Such weapons could be used in operations ranging from small-scale attacks (e.g. individual shootings to inspire fear) to higher-impact assaults (e.g. multiple-shooter attacks on crowded train cars).

#### **The case of Haifa, July 2006**

In July 2006 Haifa was the target of missile attacks of the Palestinian Hezbollah. The biggest missile hit a busy railway maintenance building, destroying the roof, killing 8, wounding more than 20 and leaving congealing pools of blood on the platform. The missile, which Israel said was a Syrian-produced model of a Iranian Fajr-3, has a range of about 30 miles and carries a warhead with some 100 pounds of high explosive and shrapnel, a significant change from the smaller Katyushas that Hezbollah has mostly been using.

#### **The case of Seattle, November 1998**

On November 27, 1998, the driver of a southbound Route 359 express bus was shot twice as the bus began crossing the Aurora Bridge, which crosses the Lake Washington Ship Canal in Seattle. After shooting the driver, the shooter turned his .380 automatic handgun on himself. The bus dropped 50 feet into the Fremont neighbourhood, killing one passenger and injuring 32 others.

The bus crossed two lanes of oncoming traffic and plunged 50 feet, landing first on the roof of an apartment building before tumbling to the ground. Had the bus travelled a few hundred yards farther it would have dropped more than 160 feet into the ship canal.

No clear motive for the shooting could be determined, although there were signs that the perpetrator had been experiencing emotional problems and had become severely withdrawn.

#### *12.1.4 Suicide Bombing*

A notable feature of the current terrorist phenomenon is the rise in attacks being carried out by suicide bombers. The attraction to the terrorist of such an act is that within a crowded and busy transport network, it is exceedingly difficult to detect the bomber amongst millions of travelling public.

For the time being, the weapon of choice will remain the conventional explosive mix. Access to the precursors, although not straightforward, is difficult to prevent and when packed with common nuts, bolts, nails or other sharp metal objects, will inflict horrendous injuries and death to the travelling public. Such a weapon, carried by a suicide bomber is almost unstoppable.

Despite the liberal positioning of security cameras and CCTV, it would still seem that identification of a suicide bomber once he or she enters the transport network is virtually impossible and, without reliable intelligence, their assault is immune from disruption or response. It is believed, however, that even a determined suicide bomber could have their operation disrupted if there is sufficient security and surveillance, including detection systems or foot patrols, especially with sniffer dogs. It might not be enough to prevent the terrorist detonating a concealed weapon but it might prevent them from hitting the target of choice. Indeed, if the target of choice is fixed, the presence of security could at least forestall the event.

#### **The case of London, July 2005**

In the London bombings of July 7<sup>th</sup> 2005, 52 people were murdered and more than 700 injured. The vital importance of the London transport system to London's economy makes it particularly vulnerable as a terrorist target. Every day more than 6 million passengers use the buses, over 3 million use the tube and nearly 1.5 million use the train within the capital. The resilience of Londoners to the 7/7 attacks is well documented and the physical disruption and impact in terms of business output was not as devastating as many had predicted.

Besides the recovery of the transport network and service, an intense activity to support victims, rebuild customer and staff confidence and renovate security plans and procedure was put in place since the very moment that the tragic events took place. By 4 August 2005 the whole transport system was restored and

the number of passengers was back in number by September.

As for businesses, according to the London Chamber of Commerce and Industry (LCCI), their response to the July attacks was robust and they managed to resume normal operation within two working days at most. However, the 7/7 attacks had a major impact upon business confidence in the capital and in the wider UK economy, in the short-term at least. Although previous falls in confidence, recorded after 9/11 and during the Iraq war, have been more pronounced, this is the longest phase of pessimism as far as the LCCI monitoring period is concerned (Source: LCCI London Monitor Quarterly Economic Survey: 2000-2006).

## 12.2 Hijacking

Transportation vehicles are especially vulnerable to hijacking because of easy public access and multitude of passengers on board. Attackers may use a wide variety of weapons, such as small arms, assault rifles, knives or other bladed weapons, and small explosive devices.

There are several scenarios of this type of attack occurring on buses, train, tram or underground, either when the vehicle is stationary or in service. Perpetrators may attempt to attack passengers or the operator, while the vehicle is in service. This type of situation could develop into a more serious incident involving the taking of hostages.

Public transport road vehicles are viewed not only as targets, but as weapons as well. Attackers might attempt to hijack an operational vehicle in order to redirect it into a building or bridge, or place explosive devices in the vehicle with the intention of detonating it at a later time. Attacks might be directed at the vehicle itself, at the transport system, or at the surrounding environment.

A hijack creates an atmosphere of panic amongst the travelling public and disrupts normal transportation service. The impact of the attack may largely vary, depending on the reason of the attack and the demands of the hijackers, as well as on the efficiency of the rescue operation. If the attackers use the hijacked vehicle as a missile, the number of casualties is likely to be very large.

As potential hijackers are likely to carry weapons with them, security measures to find such weapons might lead to an identification of the hijackers before they carry out the attack. However, the easy public access of transportation vehicles makes them vulnerable for such attacks.

### **The case of De Punt (The Netherlands), May-June 1977**

On May 2, 1977 a train hijack takes place close to the village of De Punt in the Drenthe province, northeast of the Netherlands. Nine armed Moluccans pulled the emergency brake around 9 AM and took about 50 people as hostages. The hijackers were part of the RMS (Republik Maluku Selatan) movement, fighting for the recognition of their own independent state. The hijacking lasted for 482 hours (20 days); two hostages and six hijackers were killed.

On June 11 1977, almost three weeks after the start of the hijacking, six Starfighter jet planes flew low over the train at 5:00 AM with the purpose of disorienting the hijackers and also making the hostages duck down to the floor of the train where they would be relatively safe. Then the marines started shooting; an estimated 15.000 bullets were shot at the train. The marines aimed at the first class and in-between compartments with the doors because they knew that there were the areas the hijackers were hiding. One of the hostages who had been permitted in such a compartment was also killed. Six hijackers were killed.

This was the second train hijack in the Netherlands and, like the train hijack in 1975 in Wijster, again by Moluccans.

### **The case of Berlin, April 2003.**

A 27-year-old Lebanese man who hijacked a Berlin bus, holding nine people hostage for 45 minutes, demanded that Israel withdraw from the West Bank and Gaza. The hostages were released unharmed after the police persuaded the man to surrender. It was the third time bus passengers in Germany had been taken hostage in two weeks.

### 12.3 Sabotage

Sabotage refers to the damaging of rail systems without the use of a weapon (e.g. removal of rails, manual damaging of equipment) with the intent of derailing trains, causing disruption or producing accidents resulting in casualties. The impact of sabotage will be particularly high if the derailed train contains dangerous cargo like liquefied petroleum gas. Such operations have the advantage of not requiring any weapons, although the saboteurs do require some technical and system operations knowledge.

Shorting a signalling system could cause the signal for that block to show red. At a minimum this would be an inconvenience, but this would also leave the stationary train vulnerable to attack. A coordinated effort could also use shorting to stop several trains simultaneously; transit staff could interpret this as a serious malfunction of network or control centre equipment, triggering a wider shutdown while the problem is diagnosed. A more sophisticated and serious sabotage method is modifying the circuitry so a signal shows green to an approaching train, even when a preceding train is in the block. This has the potential for causing a collision between trains.

Tamper-resistant housings for signalling equipment and telemetric systems to remotely monitor the conditions of track and switch signals are the best defence against deliberate attack. Where possible, signalling equipment can be located in a high visibility area (near a well-travelled intersection or adjacent to a transit station, for example) to increase the probability that tampering attempts will be seen and reported. Railways should be as much as possible secured against open access.

#### The case of Japan, May 1998

Unidentified saboteurs struck high-speed bullet train tracks. Saboteurs removed 25 bolts from train tracks which, if undiscovered, would have resulted in a derailment with heavy casualties. Rail employees discovered the sabotage before the morning trains began their routes. On the same day, stationmasters across the country received letters threatening derailments that would kill as many as 10,000 people. Police suspected members of Kakumaruha, a leftist group active in the 1960s.

### 12.4 Arson Attack

The deliberate starting of a fire or fires in an underground system could result in both mass casualties and the destruction of infrastructure. Even the attempts to extinguish the fire would result in both serious flooding and damage to rolling stock, infrastructure and key electrical systems.

The attractiveness of arson is that it is cheap, can be replicated throughout the system, can be added to through the use of certain liquids and substances and avoidance of detection is possible. Even with the limited exploitation of arson and the alarms which inevitably come with it, an arson attack would lead to severe disruption of services which would undoubtedly lead to costly loss of business for transport providers, users and secondary reliant economic entities.

Arson attacks are often carried out using an IID (Improvised Incendiary Device). This is a device, with a primary arson objective, created by terrorists using available flammable materials. An IID may be initiated manually on site, such as a Molotov Cocktail, by a timing device or remotely. An IID may be combined with an IED.

#### The case of Daegu, February 2003

On February 18, 2003, an arsonist set fire to a train stopped at the Jungangno Station of the Daegu Metropolitan Subway in Daegu, South Korea. The fire then spread to a second train which had entered the station from the opposite direction.

By most accounts, he boarded a train carrying a duffel bag which contained two green milk cartons filled with a flammable liquid, possibly paint thinner or gasoline. As the train left Daegu Station around 9:53 a.m., the attacker began fumbling with the cartons and a cigarette lighter, alarming other passengers who tried to stop him. In the struggle, one of the cartons spilled and its liquid contents caught fire as the train pulled into Jungangno Station in downtown Daegu. The attacker managed to escape along with many passengers on

the train, but within two minutes the fire had spread to all six cars. The fire spread quickly in the insulation between the layers of aluminium that form the shell of the cars, the vinyl and plastic materials in seat cushions and strap handles, and heavy plastic matting on the floors, producing thick smoke as it burned. The Daegu subway fire killed at least 198 people and injured at least 147.

The operator of the train, Choi Jeong-hwan, failed to notify subway officials immediately of the fire.

The arsonist was a 56 year-old unemployed former taxi driver who had suffered a stroke that left him partly paralyzed. He was dissatisfied with his medical treatment and had expressed sentiments of violence and depression; he later told police he wanted to kill himself, but to do so in a crowded place rather than alone.

## 12.5 Dispersion of chemical, biological or radiological agents.

Weapons of mass destruction (WMD) typically refer to chemical, biological, radiological and nuclear weapons capable of inflicting mass casualties, cause panic and adverse social and economic consequences. WMD can also refer to other contaminants intended to harm quickly large numbers of people, such as any powders, liquids, gases, and dirty bombs. These attacks could be very effective against passenger public transport networks due to their ease of spread, and can cause disease by inhalation, ingestion or skin contact.

There are differences between biological, radiological, and chemical agents. The effects of chemical agents may be evident quite quickly with people collapsing. The effects of radiological agents are typically recognized within hours after a release, while it may be anywhere from a couple of days to a week before the effects of a biological attack are seen as symptoms. After a biological attack is recognized, it may take several additional days to confirm the type of biological agent.

In addition, recovery from a chemical or biochemical attack can be difficult. Certain types of materials may slow down the decontamination process or reduce the lingering effects of the agent used in the attack. For example, materials that are porous, such as vehicle carpeting or mesh-screened walls in stations, are more difficult to sanitize and can trap chemical agents within the material. This may prolong the decontamination process or force removal of the material altogether.

### The case of Tokyo, March 1995

More than a decade ago, on March 20, 1995, the nerve agent sarin was used in a terror attack in Tokyo by members of the Japanese "Uhm-Shinrikiu" cult. Sarin, a potent inhibitor of the enzyme acetylcholinesterase, causes a prompt flux of the neurotransmitter acetylcholine, resulting in a variety of peripheral and central neurological symptoms. The attack took place during the morning rush hour, in several subway stations simultaneously. More than 5,500 civilians, including members of the rescue teams, were injured. Most of them (4,073) suffered only mild symptoms (mainly ocular) and were dismissed from hospital after a few hours; 984 victims suffered moderate injuries, without the need for mechanical ventilation, 50 victims had severe injuries and needed mechanical ventilation and resuscitation, and 12 people died as a result of the attack. Despite an earlier chemical attack in Japan (by the same group) and obvious signs of something awkward going on, the chemical attack against the Metro in Tokyo was not recognised quickly – further increasing the number of victims.

The sarin gas attack was the most serious terrorist attack in Japan's modern history. It caused massive disruption and widespread fear in a society that had previously been perceived as virtually free of crime.

Shortly after the attack, Aum Shinrikyo (former name of a controversial group now known as Aleph) lost its status as a religious organisation and many of its assets were seized.

## 12.6 Using a vehicle as a weapon

A vehicle can be used as a missile by attackers by crashing into a target. The vehicle can either be a vehicle owned by the attackers, or a passenger transport vehicle. In the latter case, the vehicle first has to be hijacked (unless the attacker is the driver of the PT vehicle). The impact of the attack depends on the target and the size of the vehicle used to carry out the attack. A vehicle that does not attract the attention is likely to be used, making the attack relatively easy to carry out without being detected.

### The case of Azor, February 2005

In February 2005, eight people were killed and 23 people wounded when a Palestinian bus driver ploughed into a crowded bus stop at the Azor junction near Holon.

The driver, Khalil Mohammed Abu Ulbah, 36, a part-time Egged driver from Gaza, fled the area at high speed with police in pursuit. He was finally stopped at the Gan Yavne intersection on Route 4 when he crashed into a truck stopped at a traffic light, after having been shot by a policeman.

## 12.7 Intrusion in the information system (cybercrime)

Information systems have long been at some risk from malicious actions. In recent years, systems have become more susceptible to these threats because computers have become more interconnected and, thus, more interdependent and accessible to a larger number of individuals. In addition, the number of individuals with computer skills is increasing, and intrusion, or “hacking,” techniques are becoming more widely known via the Internet and other media, so sabotage or terrorism via cyberspace may become a more serious threat, e.g. terrorist threats made via electronic communication could cause panic amongst the passengers of public transport.

Controlled Information related to automated operations, documents and internet-based material about schedules, routes, security measures, emergency responses and other sensitive information might be adequately protected to avoid the use of this information by terrorists groups and individuals to organize and execute attacks against public transport networks.

A basic management control objective for passenger transport networks is to protect data supporting its critical operations from unauthorized access, which could lead to improper modification, disclosure or deletion of the data. Access controls, which are intended to prevent, limit, and detect unauthorized access to computing resources, programmes, information, and facilities, can be both electronic and physical. Electronic access controls include use of passwords, access privileges, encryption and audit logs. Physical security controls are important for protecting computer facilities

### The case of Poland, January 2008

A good example of the vulnerabilities of these information systems was the incident caused by a teenager in Poland. The fourteen year old allegedly turned the tram system in the city of Lodz into his own personal train set, triggering chaos and derailing four trams in the process. Twelve people were injured in one of the incidents. The young boy modified a TV remote control so that it could be used to change track points. Local police said the youngster trespassed in tram depots to gather information needed to build the device. The teenager told police that he modified track setting for a prank.

## 12.8 Attack using dangerous cargo

This is an example of the effect that dangerous goods could have, however the case in question was an accident and not an intentional act.

Passenger transport systems often use the same infrastructure as cargo transport systems (whether it be railway tracks, road or air space). Dangerous cargo therefore present an opportunity for terrorists to carry out attacks using material that is already on the scene of the attack.

Dangerous cargo can either be used as an explosive (like liquefied petroleum gas), or as a chemical agent (e.g. chlorine). The dangerous material can be released from its containing vehicle either through derailment (sabotage), through an explosive attack, or by using another vehicle to crash into vehicle containing the dangerous cargo.

### **The case of Graniteville, 2006.**

In October 2006, nine people were killed when a freight train slammed into a parked train on a side track in the town of Graniteville, South Carolina. Fourteen cars on the moving train derailed, including three chlorine tank cars, one of which leaked a cloud of the deadly gas. Besides the nine fatalities, at least 234 people were hospitalized, most with respiratory illness from inhaling chlorine gas. More than 5,000 people within a one-mile radius of the accident were evacuated from their homes.

## 13 APPENDIX 3: CONCRETE EXAMPLE OF A PUBLIC TRANSPORT OPERATOR CONDUCTING RISK ASSESSMENT



The example provided below is pure theory; it concerns a fictive operator and is not based on the real experience of testing the guidelines in a public transport network as described in appendix 3.

### 13.1 Introduction

The purpose of presenting this example is to demonstrate how conducting risk assessment within a public transport operation might look in practice. This example is merely for illustration and can not serve as a blueprint! In particular the definition of risk categories and the assessment of risks for certain parts of the transport system can not be copied, but must be specifically developed for every individual transport system!

For this example a fictitious transport operator within a fictitious city are created:

#### City size:

- 600,000 inhabitants
- The city is the base of renowned multinational enterprises and serves supra-regional political as well as religious functions with symbolic places

**Transport Operator** with 2,200 staff, transporting 200 million passengers annually:

- **Metro:**
  - 150 km lines
  - 100 stations
    - 25 underground
    - 75 above ground
  - 4 depots and workshops
  - 350 trains
  - 1 Operations Control Centre (OCC) for metro and bus
- **Bus**
  - 50 routes of 550 km length
  - 700 stops
  - 150 buses
  - 2 depots with workshops
  - OCC shared with metro (see above)

## 13.2 Kick-off Meeting

*See Guidelines point 1.3, page 8*

The management of the operator understands the need for and the benefits of conducting a risk assessment with a sound methodology, to draw a full picture of potential security risks, and to define priorities in a profound way, in order to make the best use of scarce resources.

The Kick-off Meeting comprises the participation of the chief operating officers for metro and bus operations, the head of the security-department, their dedicated managers, representatives from law enforcement (including police) and external consultants, who are experienced in conducting risk assessments.

The Kick-off Meeting serves to organise and decide the procedures, contents and the assignment of tasks (to organisational units and personnel) for conducting the risk assessment:

Creation of workgroup and steering committee for the project;

Appointment of workshop moderator (it is important to have one person to direct the proceedings);

Selection of the precise methodology for Risk Assessment (analogous to these guidelines);

Decision on the depth of analysis;

Adoption on a work-plan and adequate resources for conducting the Risk Assessment;

Composition of a list of potential threats analysed within the Risk Assessment;

Structuring the public transport system for

- Metro
- Bus
- Administration;

Collection of data on the transport system regarding

- Ridership numbers/peak-hour loads at main lines and stations
- Particular aspects and points within the system regarding
  - Structural aspects
  - Geological aspects
  - Traffic aspects
  - Operational aspects
  - Symbolic aspects;

Collection of relevant data on the history of crimes within the transport operation (including large scale graffiti and vandalism);

Composition of an inventory of existing (safety and security) safeguards within the organisation;

Harnessing security related data, advice and personnel support from law-enforcement agencies: Police, Home Office, etc.;

Definition of the appropriate terminology for

- Probability of Occurrence
- Impact of Threats
- Risk-Categories;

Implementation of adequate safeguards to ensure confidentiality of the data in this project.

### 13.3 Definitions

*See Guidelines part 4, page 17*

#### 13.3.1 Threats

Having consulted with local law enforcement agencies (police) the PT operator decides to assess the following range of potential threats to the system:

Handling of unspecified threats, e.g. blackmail;

Hijacking;

Sabotage;

Suicide Attack;

Rocket Propelled Grenade;

Car bomb/VBIED;

IED with either remote or time-mechanism;

Bomb Threat;

Arson Attack;

Chemical Weapon;

Biological Weapon;

Dirty Bomb;

Atomic Bomb.

### 13.3.2 Definition of Probability of Occurrence

The group defines the Probability of Occurrence in five escalating steps:

Probability of Occurrence	Definition Criteria  (derived from Euro Norm 50126)
<b>Very high</b>	The threat can be executed at any time and/or has been executed within the organisation repeatedly
<b>High</b>	It has to be reckoned with the threat being executed repeatedly. The threat has been executed within the own organisation once.
<b>Possible</b>	It has to be reckoned with the threat being executed. The threat has been executed repeatedly within other PT operations world-wide, or at least once within a PT operation in their own/neighbouring country
<b>Low</b>	The threat is rarely executed, but has been executed in isolated cases in other organisations (world-wide)
<b>Very unlikely</b>	An execution of the threat is extremely unlikely, and the threat has never been executed in other PT operations

### 13.3.3 Definition of Impact/Severity

The group defines the Impact/Severity in four escalating steps:

Impact / Severity	Definition Criteria  (derived from Euro Norm 50126)	
	Consequences for <b>Persons</b> and/or <b>Property/Environment</b>	Consequences for <b>PT Operator</b> and <b>Services</b>
<b>Disastrous</b>	Many (over three) deaths, and/or numerous severe injuries and/or most severe damage to property and/or environment	Loss of vital functions and/or operation over a longer (12 months) period of time
<b>Critical</b>	Low number of deaths (up to three), and/or severely injured (up to 20) and/or severe damage to property and/or environment	Loss of vital functions and/or operation over a period of time up to three months
<b>Marginal</b>	Light casualties and/or notable damage to property and/or environment	Minor impact on functions and/or operation

Impact / Severity	Definition Criteria	
	(derived from Euro Norm 50126)	
	Consequences for <b>Persons</b> and/or <b>Property/Environment</b>	Consequences for <b>PT Operator</b> and <b>Services</b>
<b>Uncritical</b>	Possibility of few light casualties and/or small damage to property and/or environment	No impact on functions and/or operation

### 13.3.4 Definition of Risk Categories

The group defines the Risk categories as follows:

Probability of Occurrence	Risk Categories			
	Very high (5)	Tolerable (5)	Precarious (10)	Intolerable (15)
High (4)	Tolerable (4)	Precarious (8)	Precarious (12)	Intolerable (16)
Possible (3)	Negligible (3)	Tolerable (6)	Precarious (9)	Precarious (12)
Low (2)	Negligible (2)	Tolerable (4)	Tolerable (6)	Precarious (8)
Very unlikely (1)	Negligible (1)	Negligible (2)	Negligible (3)	Tolerable (4)
	Uncritical (1)	Marginal (2)	Critical (3)	Disastrous (4)
	Impact / Severity			

The group links the risk-categories with countermeasures, as shown in the following table:

Risk-Category	Score	Action Required
<b>Intolerable</b>	<b>15-20</b>	Must be avoided or Impact must be mitigated as far as possible
<b>Precarious</b>	<b>8-12</b>	Shall only be accepted if the efforts for prevention and/or mitigation of impact is unreasonable high
<b>Tolerable</b>	<b>4-6</b>	Shall be accepted, but threat needs to be assessed regularly
<b>Negligible</b>	<b>1-3</b>	Shall be accepted

### 13.4 Systematic structuring of the Public Transport System

*See Guidelines Part 3, page 13*

In order to identify possible targets for attacks the PT Operator structures the whole metro and bus system in an operational diagram.

The operator starts with a brainstorming session to collect the first input from internal and external experts.

Number of passengers in interchanges/stations/stops, vehicles (at peak times);

Nodes and intersections/Role and Importance for network;

Geographical and geological distinct features that could facilitate attacks or impede response efforts, e.g.

- Low lying location
- Deep tunnels
- Elevated
- Underneath major structure;

Symbolic importance

- of parts of the system or
- of adjacent buildings/institutions/events;

Postcard-view of station/infrastructure that could produce "strong" images in media-coverage after an attack;

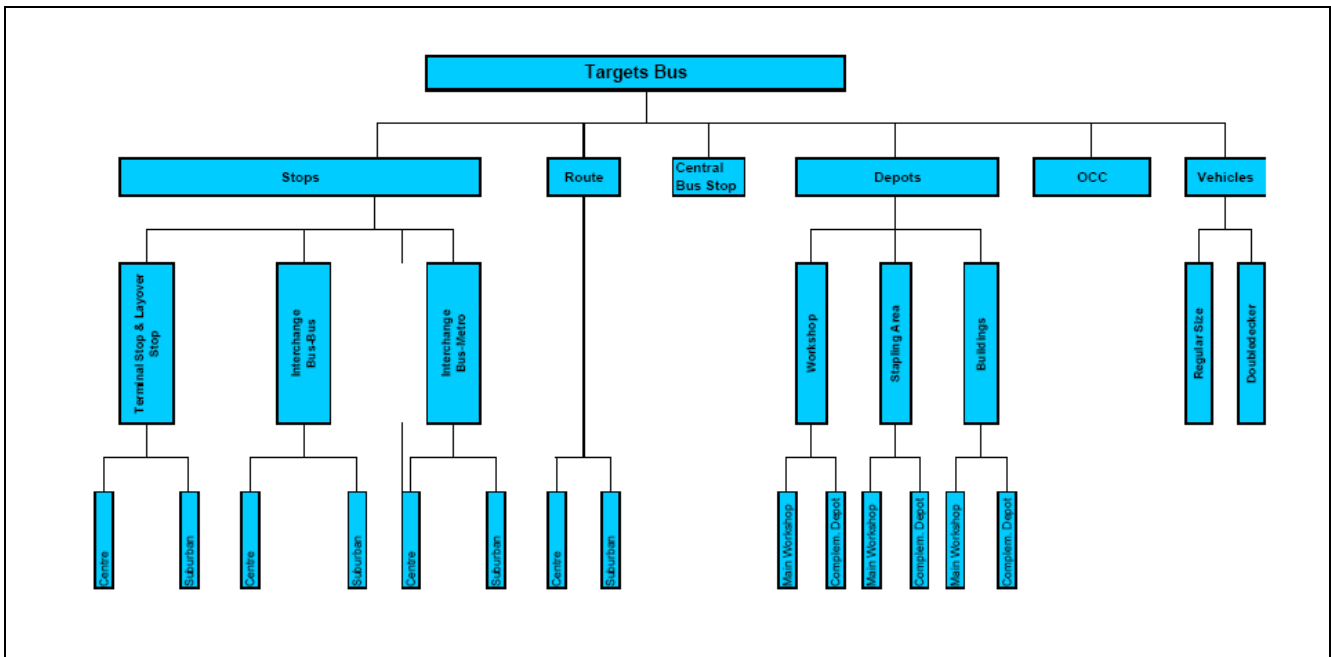
Special/Large events organised nearby (adjacent or where PT carries the visitors) that could temporarily raise the risk level;

Institutions/Organisations nearby that generate a group of riders, which is at special risk (e.g. political or religious groups);

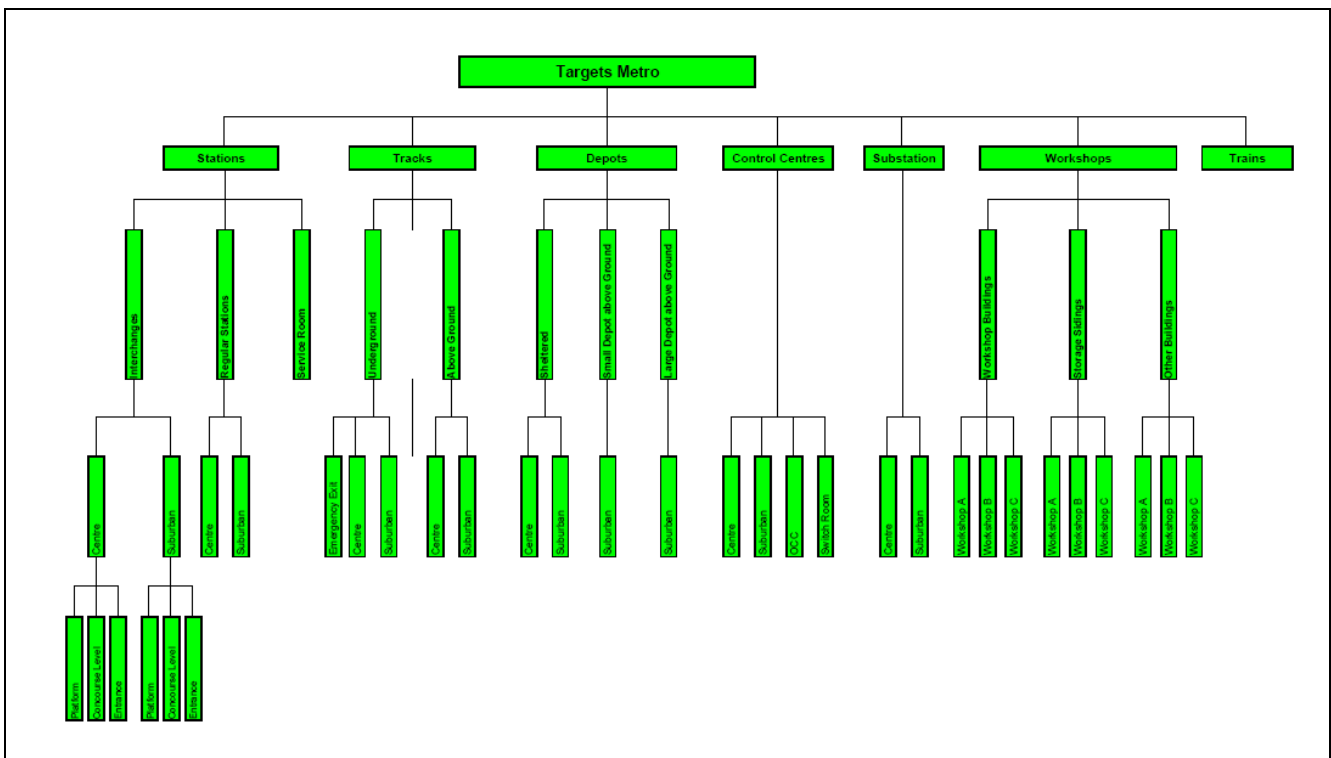
Is there a history of events? Have there been attacks in the past?

Areas with easy access of cars/vans to sensitive areas at close range.

A visualised structure is drawn that depicts the whole bus system.



Also, a visualised structure is drawn that depicts the whole metro system.



These graphics are translated into matrices (one for bus, one for metro) for the assessment of Probability of Occurrence and Impact/Severity of each potential threat in the Risk Assessment Workshops:

The **Bus System** is described in four tables:

Matrix BUS (plain)				Threat										
				Atomic Bomb	Dirty Bomb	Biological Weapon	Chemical Weapon	Arson Attack	Bomb Threat	IED	Car Bomb	Rocket-Propelled Grenade	Suicide Attack	Sabotage
<b>Target</b>														
En-route stops <u>with</u> vehicles	Street A	more than 6,000 passengers/day		/										
	Street A	Vandalism hot spot												
	Street B	Vandalism hot spot												
	Street C	Vandalism hot spot												
	Street D	Vandalism hot spot												
	Street E	Vandalism hot spot												
	Street F	Vandalism hot spot												
	Street G	Vandalism hot spot												
	Stops with special features													
	Other stops en route	Centre												
		Suburban												
En-route stops <u>without</u> vehicles	Street A	more than 6,000 passengers/day		/										
	Street A	Vandalism hot spot												
	Street B	Vandalism hot spot												
	Street C	Vandalism hot spot												
	Street D	Vandalism hot spot												
	Street E	Vandalism hot spot												
	Street F	Vandalism hot spot												
	Street G	Vandalism hot spot												
	Stops with special features													
	Other stops en route	Centre												

Matrix BUS (plain)				Threat										
				Atomic Bomb	Dirty Bomb	Biological Weapon	Chemical Weapon	Arson Attack	Bomb Threat	IED	Car Bomb	Rocket-Propelled Grenade	Suicide Attack	Sabotage
<b>Target</b>														
Terminal Stop	<u>With</u> Vehicle in service (passengers on board)	Centre		/										
		Suburban												
	<u>Without</u> Vehicle	Centre												
	Suburban													
Layover vehicles		Centre		/										
		Suburban												
Stops and Routes	Adjacent to places/persons at risk	Religious Site A	Holy Street	/										
			Paradise Street											
		Consulate of State A	Consulate Street											
		Consulate of State B												
		US-Infrastructure												
		Religious Site B												
		Military Facility												
		Controversial Multinational HQ												
Residence of famous controversial person														

Matrix BUS (plain)			Threat																	
			Atomic Bomb	Dirty Bomb	Biological Weapon	Chemical Weapon	Arson Attack	Bomb Threat	IED	Car Bomb	Rocket-Propelled Grenade	Suicide Attack	Sabotage	Hijacking	Unspecified Threat					
Central Bus Interchange	Target																			
Route <u>with</u> vehicles in service (passengers on board)	Target																			
Route <u>without</u> vehicles in service	Target																			
Deadhead and pull-out journey	Target																			
OCC	Target																			
Technological equipment for Control and Safety	Within Operator's Premises																			
	Outside Operator's Premises																			

Matrix BUS (plain)			Threat																	
			Atomic Bomb	Dirty Bomb	Biological Weapon	Chemical Weapon	Arson Attack	Bomb Threat	IED	Car Bomb	Rocket-Propelled Grenade	Suicide Attack	Sabotage	Hijacking	Unspecified Threat					
Depots and empty vehicles	Depot A	Workshop																		
		Stapling Yard																		
		Other Bldgs																		
	Depot B	Workshop																		
		Stapling Yard																		
		Other Bldgs																		
Company vehicle	Operations Surveillance																			
	Mobile Workshop																			
	Mobile Customer Service Centre																			
Personnel	Mobile Security-Staff																			
	Mobile Ticket-Inspectors																			
	Mobile Operational Surveillance																			

The Metro System is described in nine tables:

Matrix METRO (plain)				Threat																	
				Atomic Bomb	Dirty Bomb	Biological Weapon	Chemical Weapon	Arson Attack	Bomb Threat	IED	Car Bomb	Rocket-Propelled Grenade	Suicide Attack	Sabotage	Hijacking	Unspecified Threat					
Target																					
Underground Stations with Trains	Pivotal Station	more than 300,000 passengers/day	several lines, symbolic place	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
	Main Railway Station	more than 200,000 passengers/day	several lines, symbolic place	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
	Downtown Shopping Area Station	more than 150,000 passengers/day	complex station and vandalism hot-spot	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
	Station Beatiful	more than 100,000 passengers/day	several lines	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
	Station Nice	geographically sensitive		/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
	Historical Town Station	several lines, controversial, multinational adjacent		/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
	Other underground stations			/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
	Service rooms			/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/

Matrix METRO (plain)				Threat																	
				Atomic Bomb	Dirty Bomb	Biological Weapon	Chemical Weapon	Arson Attack	Bomb Threat	IED	Car Bomb	Rocket-Propelled Grenade	Suicide Attack	Sabotage	Hijacking	Unspecified Threat					
Target																					
Stations above ground with trains	Historic Centre Station A	high passenger volumes at times	symbolic place	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
	Historic Centre Station B	high passenger volumes at times	symbolic place	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
	Centre for Events	high passenger volumes at times		/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
	Vandalism hot spots	Quarter A			/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
		Quarter B			/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
	Other stations above ground	Centre			/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
		Suburban			/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
	Interchanges Metro-Regional Trains (except Main Railway Station)				/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
	Interchanges Metro-Bus				/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
	Stations with special features				/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Service Rooms				/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	

Matrix METRO (plain)				Threat																		
				Atomic Bomb	Dirty Bomb	Biological Weapon	Chemical Weapon	Arson Attack	Bomb Threat	IED	Car Bomb	Rocket-Propelled Grenade	Suicide Attack	Sabotage	Hijacking	Unspecified Threat						
Target																						
Stations <u>above</u> ground <u>without</u> trains	Historic Centre Station A	high passenger volumes at times	symbolic place	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	
	Historic Centre Station B	high passenger volumes at times	symbolic place	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	
	Centre for Events	high passenger volumes at times		/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	
	Vandalism hot spots	Quarter A			/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
		Quarter B			/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
	Other stations above ground	Centre			/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
		Suburban			/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
	Interchanges Metro-Regional Trains (except Main Railway Station)				/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
	Interchanges Metro-Bus				/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
	Stations with special features				/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Service Rooms				/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	

Matrix METRO (plain)				Threat																	
				Atomic Bomb	Dirty Bomb	Biological Weapon	Chemical Weapon	Arson Attack	Bomb Threat	IED	Car Bomb	Rocket-Propelled Grenade	Suicide Attack	Sabotage	Hijacking	Unspecified Threat					
Target																					
Stations particularly exposed <u>with</u> trains	Station X			/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Stations particularly exposed <u>without</u> trains	Station X			/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Tracks <u>with</u> trains	Above Ground	Centre		/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
		Suburban		/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
	Underground			/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Tracks <u>without</u> trains	Above Ground	Centre		/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
		Suburban		/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
	Underground			/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/







Matrix BUS (qualitative assessment)				Threat																	
				Atomic Bomb	Dirty Bomb	Biological Weapon	Chemical Weapon	Arson Attack	Bomb Threat	IED	Car Bomb	Rocket-Propelled Grenade	Suicide Attack	Sabotage	Hijacking	Unspecified Threat					
Target																					
En-route stops with vehicles	Street A	more than 1000 passengers/day		dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis
	Street B	more than 1000 passengers/day		dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis
	Street C	validates hot spot		dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis
	Street D and E	validates hot spot		dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis
	Street F	validates hot spot		dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis
	Other stops en route including those with special features	validates hot spot		dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis
Terminal Stop	With Vehicle in service (passengers on board)	entry and exit		dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis
En-route stops with vehicles	Adjacent to places/persons at risk	religious site A	city street	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis
		consulate of state A	critical site	To be assessed if necessary (at critical times)																	
		EU-Infrastructure		To be assessed if necessary (at critical times)																	
		Continental Airterminal IIC		To be assessed if necessary (at critical times)																	
Route with vehicles in service (passengers on board)	OCC			dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis
				dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis
Technological equipment for Control and Safety	Within Operator's Premises	equipment A		dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis
	Outside Operator's Premises	equipment B		dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis

Matrix BUS (qualitative assessment)				Threat																	
				Atomic Bomb	Dirty Bomb	Biological Weapon	Chemical Weapon	Arson Attack	Bomb Threat	IED	Car Bomb	Rocket-Propelled Grenade	Suicide Attack	Sabotage	Hijacking	Unspecified Threat					
Target																					
Depots and empty vehicles	Depot A	Workshop		dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis
		Stapling Yard		dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis
		Other Bldgs		dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis
	Special Servicing Place			dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis	dis

PROBABILITY OF OCCURRENCE		IMPACT SEVERITY	
vhg	very high	dis	disastrous
hig	high	cri	critical
pos	possible	mar	marginal
low	low	unc	uncritical
vlo	very low		

Impossible scenario or not relevant for assessment
Intolerable risk
precarious risk
tolerable risk
negligible risk

The result of the risk assessment for the **Metro** system comes in five parts instead of nine:

Matrix METRO (qualitative assessment)				Threat												
				Atomic Bomb	Dirty Bomb	Biological Weapon	Chemical Weapon	Arson Attack	Bomb Threat	IED	Car Bomb	Rocket-Propelled Grenade	Suicide Attack	Sabotage	Hijacking	Unspecified Threat
Underground Stations with Trains	Target			no	no	no	low	hig	hig	pos	pos	hlo	pos	pos	low	hlo
	Pivotal Station	more than 300,000 passengers/day	several lines, symbolic place	dis	dis	crf	dis	dis	mar	dis	dis	crf	dis	mar	crf	mar
	Main Railway Station	more than 200,000 passengers/day	several lines, symbolic place	hlo	hlo	hlo	low	hig	hig	pos	pos	hlo	pos	pos	low	hlo
	Downtown Shopping Area Station	more than 150,000 passengers/day	complex station and vandalism hot-spot	dis	dis	crf	dis	dis	mar	dis	dis	crf	dis	mar	crf	mar
	Station Beatiful	more than 100,000 passengers/day	several lines	hlo	hlo	hlo	low	hig	hig	pos	low	hlo	pos	pos	low	hlo
	Station Nice	geographically sensitive		dis	dis	crf	dis	dis	mar	dis	dis	crf	dis	mar	crf	mar
	Historical Town Station	several lines, controversial multinational adjacent		hlo	hlo	hlo	low	hig	pos	low	hlo	hlo	pos	pos	low	hlo
	Sports-Station	high passenger number after events		hlo	hlo	hlo	low	hig	pos	pos	hlo	hlo	pos	pos	low	hlo
	Other underground stations			hlo	hlo	hlo	low	hig	pos	low	hlo	hlo	low	pos	low	hlo
Service rooms			dis	dis	crf	dis	dis	mar	dis	dis	crf	dis	mar	crf	mar	

Matrix METRO (qualitative assessment)				Threat											
				Atomic Bomb	Dirty Bomb	Biological Weapon	Chemical Weapon	Arson Attack	Bomb Threat	IED	Car Bomb	Rocket-Propelled Grenade	Suicide Attack	Sabotage	Hijacking
Target															
Stations above ground <u>with</u> Trains	Historic Centre Station A	high passenger volumes at times	symbolic place	[Risk Matrix Grid]											
	Historic Centre Station B	high passenger volumes at times	symbolic place	[Risk Matrix Grid]											
	Vandalism hot spots	Quarter A			[Risk Matrix Grid]										
		Quarter B			[Risk Matrix Grid]										
	Other stations above ground incl. those with special features	Centre and suburban			[Risk Matrix Grid]										
Interchanges Metro-Bus and Rail-Rail				[Risk Matrix Grid]											
Stations (above ground) particularly exposed <u>with</u> trains	Station X			[Risk Matrix Grid]											
Tracks <u>with</u> trains	Above Ground	Centre and suburban		[Risk Matrix Grid]											
	Underground			[Risk Matrix Grid]											
Tracks <u>without</u> trains	Above Ground	Centre and suburban		[Risk Matrix Grid]											
	Underground			[Risk Matrix Grid]											
Tracks and stations	Adjacent to places/persons at risk	Religious Site A	Holy Street	[Risk Matrix Grid]											
		Consulate of State A	Consulate Street	To be assessed if necessary (at critical times)											
		US-Infrastructure		To be assessed if necessary (at critical times)											
		Controversial Multinational HQ		To be assessed if necessary (at critical times)											

Matrix METRO (qualitative assessment)				Threat											
				Atomic Bomb	Dirty Bomb	Biological Weapon	Chemical Weapon	Arson Attack	Bomb Threat	IED	Car Bomb	Rocket-Propelled Grenade	Suicide Attack	Sabotage	Hijacking
Target															
Depots at terminal stations with parked trains	Station A-H			[Risk Matrix Grid]											
	Control Centres and Administrative Bldgs	Main Administration incl. Managing Director, Post Room, etc.		[Risk Matrix Grid]											
		OCC			[Risk Matrix Grid]										
		Central Customer Service Centre			[Risk Matrix Grid]										
		Peripheral Administration			[Risk Matrix Grid]										
		Security Control Centre			[Risk Matrix Grid]										
		Data Processing Centre			[Risk Matrix Grid]										
Technological equipment for Control and Safety	Outside Operator's Premises	special equipment		[Risk Matrix Grid]											
Power Supply	Within Operator's Premises			[Risk Matrix Grid]											
	Outside Operator's Premises	above ground		[Risk Matrix Grid]											
		underground		[Risk Matrix Grid]											



## 13.6 Final steps

### *13.6.1 Ranking of Results*

*See Guidelines part 6, page 33*

The results of the risk analysis shown in these tables above are ranked according to

- locations/aspects; and
- threats.

With the Rankings at hand, it becomes clear where the most urgent needs are to be handled.

### *13.6.2 Vulnerability Assessment*

*See Guidelines part 6, page 32*

Then, the identified risks are assessed against the background of existing (and potential) safeguards, i.e. the vulnerability assessment is performed.

### *13.6.3 Evaluation of additional safeguards, Conclusion Report and Action Plan*

The next step is the evaluation of additional safeguards according to their effectiveness, cost efficiency, time of implementation, factors potentially hindering their implementation, and other aspects. The result of this step is a list of prioritised measures (according to their performance in the assessment).

A conclusions report is composed, based on the risk analysis and identification of list of potential measures.

An executive summary and decision making outline for management is prepared, supplemented by a draft action plan containing precise tasks, responsible units/personnel, timelines, budgets, etc.

Finally, it is decided to do yearly updates and the responsible person to oversee this is appointed.

## 14 APPENDIX 4: TESTING THE GUIDELINES

As foreseen in the “Proposal for targeted study”, the final step in the development of PT4, “Generic guidelines for conducting risk assessment in public transport networks” was to test the guidelines with the cooperation of a Public Transport Operator, in this case the multi-modal operator in Brussels, STIB-MIVB. Due to the limited time frame of the study, however, it was decided to limit the test to the STIB-MIVB metro network only and to the risk analysis. Vulnerability assessment has to be conducted later, internally.

Following the guidelines, the test consisted of two separate workshops, both taking place on site in Brussels:

- First workshop: 20/02/2009 (one day);
- Second workshop: 11-12/03/2009 (two days).

Participants from among STIB-MIVB came from the following areas of operation: Operational Control Centre, Security, High voltage, Building management, Financial, representatives of the Brussels region. They were assisted by a deputy officer of the Brussels Metro Police department.

From the COUNTERACT consortium, representatives of study leader, UITP, as well as the study subcontractor, Hamburg-Consult, were in attendance to observe the process.

The aim of the first workshop was to establish a common understanding among the participants of the aims and the purpose, the methodology and the alternative approaches for conducting risk assessments. Secondly, it was to define all the documents and information necessary, as well as the necessary participants for the second workshop, to perform the risk analysis for filling in the matrix. Thirdly, it was to decide on the scope of the undertaking and the definitions to be used. Finally, it was to establish the repartition of the tasks to be performed (“who is doing what”) before the second workshop.

The second workshop was dedicated to starting with the trial and error regarding the suitability of the definitions to be used, i.e. the adjustment of the definitions, and finally to the filling in of the matrix, the permanent cross-checking and documentation, and the ranking of the results.

From these workshops, several lessons learned were drawn.

### 14.1 Involvement of the police

It was immediately apparent that the input of the police forces was essential in order to judge the realistic situation of the risk level in Brussels: the PT operator alone was only able to perform a detailed analysis of the risk level within the metro environment whereas police forces brought more information about the surrounding neighbourhoods and general context.

STIB-MIVB had statistics covering:

- The amount of people using each station per day;
- The number of assaults per station.

Police forces brought statistics concerning:

- Sensitive points in the immediate neighbourhood of the metro stations;
- Criminality level in the neighbourhood of the metro stations.

For example, it is important to consider the impact on the risk of a certain metro station due to the presence of an embassy in its immediate neighbourhood, information that might be unknown by the PT operator.

## 14.2 Trial and error

The most time-consuming part of the process was agreeing on the definitions of probability of occurrence and impact/severity, especially the difference between the “disastrous” and “critical” categories. At first, the group tended to use the “disastrous” label too often. This resulted in a flat matrix with mainly “red” squares. It also highlighted that the different statistics (from the operator and from Police forces) had to be integrated and that the matrix had to be adapted to take them into account and provide much more diversified results.

The process therefore was based on an essential “trial and error” concept until all parties agreed on the definitions which resulted in a more diversified matrix.

## 14.3 Adapting the guidelines

The test proved that the guidelines are flexible enough for an operator to adapt them to its specific needs. The operator must not stick to any definition but needs to modify them and tailor them according to its specific situation and determining framework. The guidelines allow for and explicitly encourage exactly this approach.

The main conclusion of the test is clearly that law enforcement agencies (police forces) have to be associated to the process from the beginning: the public transport operator cannot limit the risk analysis study to the immediate premises without taking into account wider context.

## 15 APPENDIX 5: MEMORANDUM OF UNDERSTANDING

As has been continually stated, the involvement of Police is very important to conduct a risk assessment successfully. A good way of ensuring full cooperation with and support from the Police, or other law enforcement agencies, is to establish a Memorandum of Understanding (MOU). This could define the roles and responsibilities of each party for the risk assessment process, their expected input, the procedure, as well as the expected output of the process.

A typical MOU might cover the following aspects:

- Purpose
- Scope
- Definitions
- Legal Framework & Responsibilities
- Duration
- Roles and responsibilities
- Expected input from all parties
- Expected output
- Information sharing
- Confidentiality agreement
- Frequency (and duration) of meetings

## 16 APPENDIX 6: QUESTIONNAIRE FOR PUBLIC TRANSPORT OPERATORS ON RISK ASSESSMENT

Dear Sir/Madam,

As suggested by the PT TUG, a study on Risk Assessment is being carried out in the framework of the COUNTERACT project. The aim of the study is to provide public transport operators with guidelines describing how to conduct a Risk Assessment of their networks, and how to identify weak-points as far as security is concerned, i.e. serious crime and terrorism.

This short questionnaire is one of the first steps. Your valuable input is needed in order to ensure that the guidelines for Risk Assessment will be most practicable and really meet operators' needs. We kindly ask you to complete it, no matter whether or not you have been active in this field already.

*Any information received will not be given to any third party and will be treated in the strictest confidence.*

**Risk Assessment** is a tool for an Operator to analyse potential threats to the public transport network in a systematic way. This includes the analysis of a range of potential threats regarding their likelihood (or improbability) of occurrence, and their potential impact. Also, a vulnerability analysis might be included.

**Safety** Risks refer to unintentional threats to technical or operational matters including severe weather conditions, accidents, etc. It covers problems that arise as result of an accidental danger. In this purpose, traffic-related safety includes accidents arising from **NON-MALICIOUS** interactions among passengers, vehicles and pedestrians.

**Security** Risks refer to intentional threats and include among others severe crime and terrorism.

### Does your organisation consider Risk Assessments relevant and necessary?

Please, tick one or several appropriate answers and explain if possible

- Yes, for **Safety** aspects (regarding unintended technical threats)
- Yes, for **Security** aspects (intended criminal threats)
- No, because:

---

---

---

*If you have already conducted a Risk Assessment, proceed to page 3*

*If you have not yet conducted a Risk Assessment, proceed to page 2*

Does your organisation plan to conduct a risk assessment in the near future?

- Yes
- No

Please explain why: \_\_\_\_\_

\_\_\_\_\_

If yes, please give details (regarding timing, approach, methodology, technical instructions, support of external/internal experts, etc.): \_\_\_\_\_

\_\_\_\_\_

What are potential obstacles / hindrances to conducting Risk Assessment regarding security in your organisation?

\_\_\_\_\_  
\_\_\_\_\_

What would be prerequisites for conducting Risk Assessment regarding security in your organisation?

\_\_\_\_\_  
\_\_\_\_\_

What kind of support for conducting Risk Assessment regarding security would you find helpful or necessary?

- Written Guidelines / Manuals
- (Interactive) Websites with instructions
- Seminars
- Technical Support by Experts
- Other

\_\_\_\_\_  
\_\_\_\_\_

Your organisation has already conducted a Risk Assessment for:

- Safety-Aspects (regarding unintended technical threats)
- Security-Aspects (intended criminal threats)

Please specify why you decided to carry out Risk Assessment, including legal obligations:

\_\_\_\_\_  
\_\_\_\_\_

**Who conducted the Risk Assessment of your Organisation?**

- Internal Experts of the Organisation
- Internal Experts of the Organisation with the support of External Experts (e.g. Consultants)

*Please specify the number of experts involved, their background, positions, and the source of external support (if applicable):*

---

---

---

**What methodology did your organisation use for conducting the Risk Assessment?**

- Methodology developed by organisation itself
- Methodology developed outside
- Methodology developed outside and modified by organisation

*Please specify the methodology (qualitative, semi-quantitative or quantitative), its origin/source, approach, systematic, etc.:*

---

---

---

**Did the Risk Assessment result in new insights and findings?**

- Yes
- No

Please specify:

---

---

---

**Did the results of the Risk Assessment result in changes to the Security Concept of your Organisation?**

- Yes
- No

---

---

---

**Did you encounter any problems while conducting the Risk Assessment?**

- Yes
- No

*Please specify:*

---

---

---

**Will/Does your Organisation update and follow-up the Risk Assessment?** Yes No

*If yes, please specify when and how the update is planned, and whether regular updates (which intervals?) are foreseen:*

---

---

---

**Please, describe your experiences, observations, or any highlights and particularities:**

---

---

---

***If you have any documents or written information on your experiences conducting Risk Assessment or other interesting information (e.g. articles about the used method) which you are willing to share, please send them to UITP.***

**Please, indicate your name and contact details:**

Name:

Organisation Name:

Position:

Country:

Postal Address:

Telephone Number:

E-mail Address:

**Please return the filled-in questionnaire and materials etc. if possible before **FEBRUARY 18<sup>th</sup>, 2008:****

Once your response has been received, from 18 – 22 February and at your convenience, we will conduct short phone interviews in case any answers need to be clarified or more details required.

**Thank you very much indeed for your kind support!!**

## 17 ACKNOWLEDGEMENTS

The study team was made up of the following COUNTERACT partners:

- UITP (leader)
- ISDEFE
- NLR
- VTI
- I-SEC

With the support of subcontractor

- Hamburg-Consult

The study team would like to thank the following organisations for their valuable input and support:

- Hamburg-Consult, especially Matthias Müth
- London Underground, especially Geoff Dunmore and Kevin Clack
- Metropolitana de Lisboa, especially Armando Silva Neves
- RATP, especially Patrick Dillenseger
- Hamburger Hochbahn Wache, especially Rainer Cohrs
- STIB, especially Jean-Pierre Van Keymeulen and Daniel Bernard
- Movia, especially Lars Hven Troelsen
- Met.Ro, especially Gianluca Lucisano
- Mohamed Mezghani
- The whole COUNTERACT Passenger Public Transport Cluster
- The whole COUNTERACT Passenger Public Transport Cluster Thematic User Group
- The organisations who responded to the Questionnaire
- TMB, especially Ricardo Ortega and Miguel Rodriguez