SECURITY MANUAL FOR EUROPEAN ROAD INFRASTRUCTURE

With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme (CIPS) European Commission – Directorate-General Home Affairs

SECMAN

Security Risk Management Processes for Road Infrastructures

Preamble

Trans-national transport routes play a vital role in goods traffic and the supply of the population and are a necessary prerequisite for ensuring that Europe remains competitive. Besides the fact that roads have be safe, they also have to be secure from attacks, natural disasters and accidents and any disruptions or manipulations that could affect their availability and their level of service.

Important road infrastructures like bridges and tunnels very often have a bottle-neck function. Even minor disruptions can cause domino effects that can lead to temporary supply bottlenecks and significant losses for the economy. Disruptions or manipulations of these infrastructures should therefore, to the extent possible, be brief, infrequent, manageable and minimally detrimental to the welfare of the population and the society.

Up to date, no common approach to identify, quantify and assess security risks and the identification of possible protection measures for road infrastructures exists. This manual, as a final product of the EU project SecMan, supports owners and operators of European road infrastructures in the management of security risks and thereby contributes to an adequate and equal level of security throughout the Union.

Furthermore, the manual supports the European Security Strategy in bringing together the different instruments, methodologies and practices across Europe. By learning from each other and exchanging knowledge on the security of transport structures in Europe, best-practices are identified. In the end, the European society and economy profit from a more secure European transport system.

We are happy to be able to present you the results of our research over the past two years and we hope that you enjoy reading and applying this manual. Finally, we would like to thank the people behind the project consortium for the fruitful cooperation and the valuable inputs without which this manual would not have been possible.

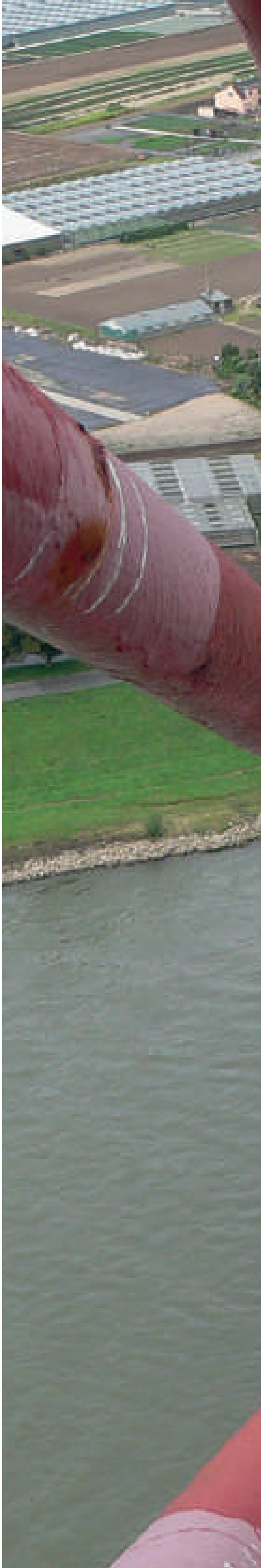
Dr. Jürgen Krieger (BASt))

Bernhard Kohl (ILF)

Marko Žibert (ELEA)

Drago Dolenc (DARS)

Table of Contents



Acronyms

AADT	Average Annual Daily Traffic
BLEVE	Boiling Liquid Expanding Vapour Explosion
CAV	Criticality-Attractiveness-Vulnerability
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
DG	Dangerous Goods
DP	Damage Potential
ECI	European Critical Infrastructure
EPCIP	European Program for Critical Infrastructure Protection
EU MS	European Union Member State
FOA	Feasibility of Attack
HGV	Heavy Goods Vehicle
IED	Improvised Explosive Device
ISO	International Organization for Standardization
IT	Information Technology
ITA	International Tunnelling Association
NATM	New Austrian Tunnelling Method
RABT	Guidelines for the equipment and operation of road tunnels, Germany
SeRoN	Security of Road Transport Networks, Project
SKRIBT	Schutz Kritischer Brücken und Tunnel im Zuge von Straßen (Protection of Critical Bridges and Tunnels in a Road Network)
TBM	Tunnel Boring Machine
TEN-T	Trans-European Transport Network
WP	Work Package

Definitions

Term	Definition	Source
Asset	An item of value or importance. Assets may include physical elements, cyber elements (information and communication systems), human or living elements (critical knowledge and functions)	SeRoN
Consequence	The outcome of an event in terms of damage to the health of people, to property or to the environment.	SeRoN
Consequence Analysis	Systematic procedure to describe and/or calculate consequences.	PIARC
Construction Method	The method by which a tunnel is constructed, usually either conventional/TBM, cut and cover or immersed	SecMan
Control Staff	All employees dealing with traffic and/or technical management.	PIARC
Critical Infrastructure	An asset, system or part thereof which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact as a result of the failure to maintain those functions" (cf. [EC, 2008])	SeRoN
Critical Situation	Situation (congestion, vehicle breakdown, accident, fire) requiring special attention or action from users.	PIARC
Criticality	Criticality refers to the transport network, meaning that it indicates the importance of a specific network section to the functioning of the whole transport network. Hence, a structure can be vulnerable to a specific threat but not critical to the network if it is located on a non-critical network section. On the other hand, it may be critical for the functioning of the network but less vulnerable to a specific threat.	SecMan
Detection	The action of being aware of the occurrence of an event. [Generally, a detection can be human (see, hear, smell, etc.) or depend on a system (heat detection, automatic incident detection, CO level, etc.]	PIARC
Emergency	Sudden, unexpected event requiring immediate action owing to potential threats to health and safety, the environment, or property	PIARC
Emergency Operation Plan	Plan that each service or agency and the tunnel operating body has and maintains for responding appropriately to hazards.	PIARC
Emergency Preparedness	The discipline that ensures a covered entity's readiness to respond to an emergency in a coordinated, timely, and effective manner.	PIARC
Emergency Services	Fire-fighters, police and medics.	PIARC
Event	Occurrence of a particular set of circumstances, which may cause harm	PIARC
Graduated Security Measures	Measures which can be activated according to varying risk and threat levels	2008/114/EC
Frequency	The number of times a specified event occurs within a specified interval (e.g. accidents per year).	PIARC
Harm	Physical injury or damage to the health of people, or damage to property or the environment.	PIARC
Hazard	Potential source of harm.	PIARC
Hydrogeological Conditions	Conditions dealing with water below the earth's surface and the geological aspects of it.	SecMan
Incident	Abnormal and unplanned event (including accidents) adversely affecting tunnel operations and safety	PIARC

Permanent Security Measures	Measures which identify indispensable security investments and means which are relevant to be employed at all times, such as technical measures (including installation of detection, access control, protection and prevention means); organizational measures (including procedures for alerts and crisis management); control and verification measures; communication; awareness raising and training; and security of information systems.	**2008/114/EC**
Predominant Geotechnical Conditions	The conditions of the surrounding material around a tunnel, usually either stable rock or soft soil.	**SecMan**
Probability	Likelihood that an event may occur, expressed as a number between 0 and 1.	**PIARC**
Probability Analysis	Systematic procedure for describing and/or calculating the probability of a future event	**PIARC**
Quantitative Risk Analysis	A risk analysis method based on numerical calculations.	**PIARC**
Risk	Combination of the probability of occurrence of harm and the severity of the harm (ISO IEC 51).	**PIARC**
Risk Analysis	Systematic use of available information to identify hazards and to estimate the risk	**PIARC**
Risk Management	A systematic process undertaken by an organization in order to reach and maintain a tolerable level of risk	**PIARC**
Road Network	The complete system of the routes pertaining to road transport, available in a particular area, usually the entire network the user of this manual is responsible for.	**SecMan**
Road Network Part	A defined extract of a road network with multiple routes.	**SecMan**
Road Section	A defined extract of a part of a road network, based on differences in the traffic parameters	**SecMan**
Safety	The protection of transport structures against unintentional events such as accidents, covered by relevant standards	**SecMan**
Security	The preparedness, protection and preservation of transport structure against intentional man-made events	**SecMan**
Scenario	A combination of events, system states and conditions that lead to an outcome of interest. This set of events and conditions may be used in a risk assessment or other model. For example it may include a specific threat to an asset or object, with associated probabilities and consequences	**SeRoN**
Single / Dual Shell	In a single shell tunnel there is only one lining while in a dual shell tunnel, the hull consists of an outer lining (shot-concrete) and an inner lining (in-situ)	**SecMan**
Single / Multiple Cell	In a tunnel with a rectangular cross section, the cells may be divided by a partition wall into multiple cells	**SecMan**
Superstructure Section (Bridge)	All elements of a bridge that bear loads, situated above the supports are regarded as the superstructure. It carries the traffic.	**SecMan**
System (Bridge)	The statically system of a bridge defines the design method of a bridge	**SecMan**
Threat	Any circumstance or event with the potential to cause the loss or damage to an asset. In the case of terrorism threat represents intention and capability, as well as the attractiveness of that asset relative to alternate assets. In the case of 'natural' hazards threat refers to the historical (or estimated) frequency of the natural event to which the asset may be subjected. In both cases for the purposes of risk analysis the threat is defined as the likelihood the event will occur.	**SeRoN**
Tunnel Control Centre	Operation centre dedicated to control and coordinate the operation of a tunnel and to maintain, where required, communication between operating personnel and other agencies concerned.	**PIARC**
Vulnerability	The characteristics and circumstances of a community or system or asset that make it susceptible to the damaging effects of a hazard (threat, event). It is linked to risk by a specific event or scenario.	**SeRoN**

Executive Summary

Transport is one of the most important sectors for the European economy and society as a whole, with its infrastructure being essential for the well functioning of the entire network. Owners and operators of these infrastructures today are faced with multiple challenges to ensure the smooth operation of traffic within their responsibility. These challenges can range from normal traffic to accidents as well as major disruptions due to intentional attacks.

The present manual deals in particular with the protection of road infrastructure, such as runnels and bridges, against man-made intentional threats. It presents a thorough yet simple 4-step procedure for the assessment of infrastructures in respect to their criticality for the network, attractiveness for an attack and vulnerability of the object itself. This approach enables the user to identify weak spots in the road network with regards to multiple security hazards and supports the decision on the allocation of attention towards a reduced number of highly critical, attractive or vulnerable objects. Furthermore, a number of measures are introduced and presented to the user in a comparable way. Hence, possibilities for the protection of the identified infrastructure are given.

The open and holistic approach of the methodology allows for a European-wide application of the methodology, supporting the security of transport infrastructure and thus the security of Europe’s arteries; the transport system.

PART I: Basics

Part 1: Basics

The following part introduces the background, motivation, purpose and benefits of the manual as well as its scope and limitations. Furthermore, the three underlying principles of the methodology are explained.

1. Introduction

The following handbook was developed for road infrastructure owners and operators to assess their infrastructure regarding security hazards and identify potential measures for the protection of the former. It is a ready-for-practice manual, allowing the user to develop an understanding of security risks towards his network. The result is a comprehensive assessment of the investigated road structures, enabling the user to obtain a first indication of which structures might be potentially critical or vulnerable and what measure could be introduced to tackle these issues.

1.1 Background and Motivation

Trans-national transport routes play a vital role in goods traffic and the supply of the population. In this respect, critical road infrastructures like bridges or tunnels can have a bottle-neck function, any disturbance of which could lead to negative consequences for the population and the economy. Up to date, no ready for practice handbook dealing with the security of these infrastructures exist. However, there is an apparent need for the harmonisation of the identification of critical and vulnerable road infrastructures in Europe. Differences in security standards and equipment as well as a lack of knowledge of important sections or structures within road networks across Europe could negatively affect the security of transport routes and hence the supply chain within the European economy.

Since the events of September 11th 2001, terrorism and other security related threats have gained importance in various fields in Europe, with transport infrastructure as an easy target with immense potential consequences for owners, users and the society as a whole. Since then, much research has been conducted on the identification and assessment of vulnerable transport infrastructure in respect to various threats [SeRoN, SKRIBT]. However, the results of this research have not yet been applied in the day to day business of owners and operators of these infrastructures. This manual aims to bridge this gap between academia and practice and introduces a ready for practice guide on how to identify and assess existing highway sections and structures as well as provide a first indication on which measures could be introduced in order to reduce the damage potential of a certain threat to a road structure or highway section. On a general level, this manual aims to contribute to the strengthening of the resilience of the European Transport Network against various man-made hazards. Furthermore, the awareness of the road owners and operators with respect to these types of hazards is increased.

1.2 Purpose and Benefits

In light of the recent EU Directives [2008/114/EC] this manual supports the European efforts for a homogenous, collective methodology for the identification of critical infrastructures and adequate security measures. It provides road owners and operators with an easy to manage, practice-oriented tool for the assessment of their infrastructure. Furthermore, a risk based approach for the assessment of road infrastructure is made available, while at the same time identifying possibilities for detailed, in-depth quantitative follow-up analyses.

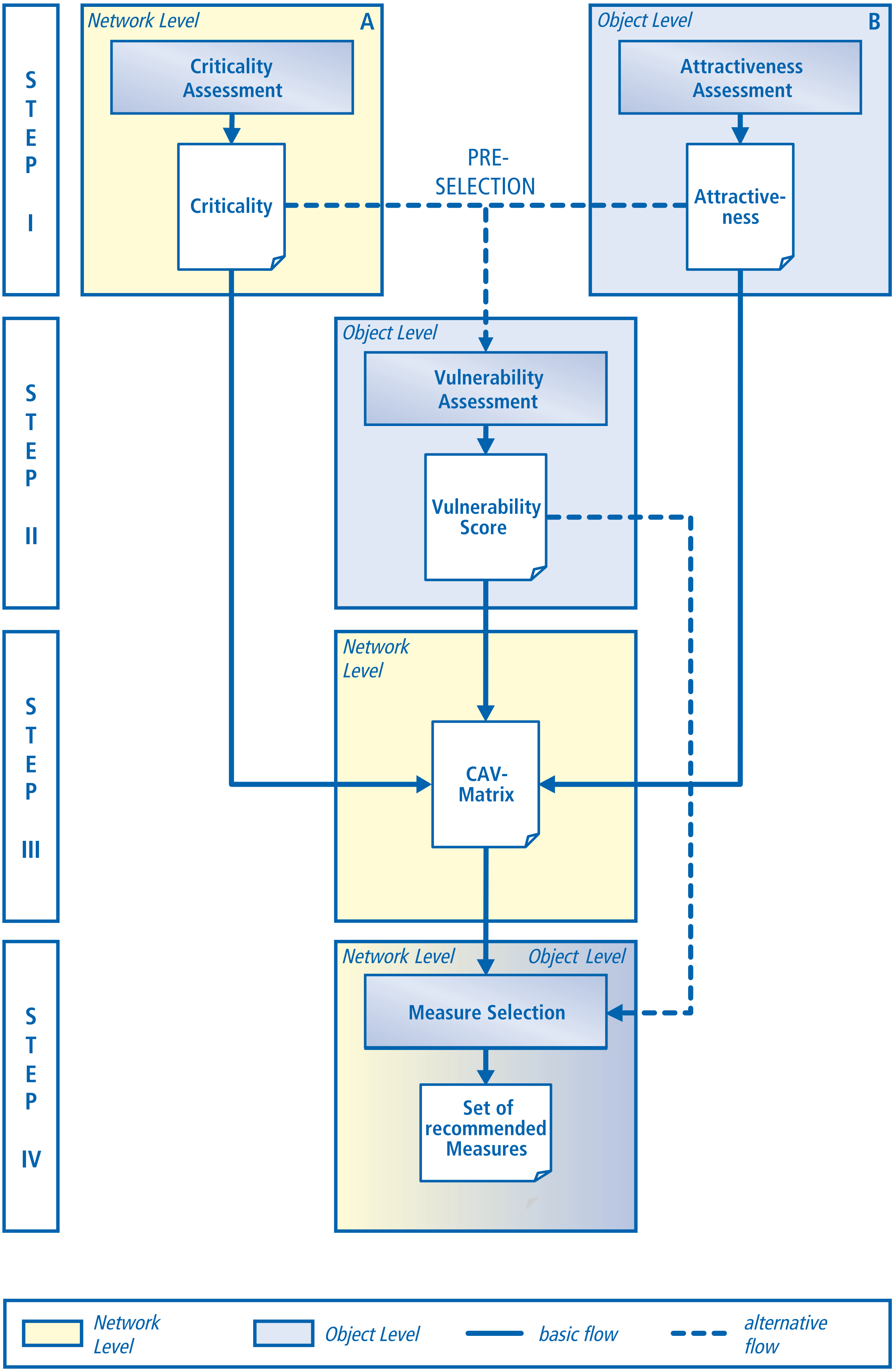
Another benefit of this manual is to foster the debate between academia and practice. As stated above, much research has been conducted on this topic. However, difficulties may occur when these results are applied in real day-to-day situations. Hence, the approach of this manual is to be as detailed as possible while still being accessible for practicable use. Additionally, the manual was developed to be applicable across Europe. While this necessarily meant the reduction of the level of detail of the assessment, it makes the results comparable and fosters the harmonization of practice across the EU.

2. Scope and Limitations

In general, the presented methodology provides a holistic assessment of road structures concerning their criticality, vulnerability and potential security measures. Although being widely applicable across Europe, the presented methodology has few limitations with regards to its scope, the threats investigated and the structures under consideration. In general, the manual deals with road infrastructures such as bridges and tunnels. These infrastructures were categorized to make the method as detailed as possible while at the same time being as concise as necessary for the applicability of the former. In the frame of a holistic security assessment, other engineering structures can in certain cases also be of relevance. Nevertheless, by addressing major road infrastructures (bridges, tunnels) this security manual gives a first indication on the most relevant structures in a road network.

Furthermore, only man-made hazards are considered. This means that natural threats, such as extreme weather events, or minor

» Figure 1 - Methodological Flowchart



accidents are not considered in the methodology. Additionally, it has to be stated that the scenarios which were investigated do not include cyber threats. Although this issue has been identified to become increasingly important in the next years, detailed investigations are necessary to adequately assess and evaluate the impact of a cyber-attack on road infrastructure. The focus of the approach is on the availability of a road network. Hence, only threats were considered which may cause damage to the structure itself. This means that threats which have an effect only on the user of the structure are not part of the methodology. In addition, no combinations of threats, for example an explosion with a simultaneous contamination with a hazardous substance, are addressed. During the development of the relevant scenarios resulting from the identified threats, the scenarios with the highest consequence were considered.

During the measure selection process, no quantification of the effectiveness of the measures is given. Hence, the set of measures should be seen as a first indication on what could be done. Further recommendations are given where deemed relevant. Combined effects of measures are not included in the selection process.

In summary, the present manual gives the user a first indication on the criticality/vulnerability of his road infrastructure. A detailed analysis could be necessary, depending on a case-by-case situation.

3. Principles

The manual has two basic underlying principles:

The methodology follows a four step procedure, where each step may either be executed individually or in combination with the others.

Furthermore, the manual employs a two level approach, meaning that the entire assessment of infrastructures can be done via this methodology on a semi-quantitative basis (level 1), keeping in mind that detailed, object specific investigations are not part of this manual but may be necessary in order to fully assess the respective transport network (level 2).

In general, the manual is based on expert judgement. The default values which are given in the methodology have been developed during the course of the project SecMan in several internal as well as external project workshops in consideration of road infrastructure experts from various fields. These values can be changed by the user, if case-specificities require him to do so.

3.1 Four Step Procedure

The methodology of the Security Manual for European Road Infrastructure is divided into four steps. Step 1 is comprised out of the criticality and the attractiveness assessment, step 2 entails the vulnerability analysis and step 3 combines the results from the previous steps into a comprehensive matrix. Finally, step 4 introduces protection and mitigation measures for the identified objects. The assessment procedures act either on network or object level. During the assessments on the network level, a part of the network with different sections is studied. On the object level, individual objects are checked with more specific parameters.

3.2 Two Level Approach

The methodology is divided into 2 levels of detail. The methodology presented in the flowchart (see Figure 1) acts on level one, meaning that it gives a first overview on the criticality of certain sections or the vulnerability of certain objects within a given road network. However, in the course of the method, several points are identified where a more detailed analysis is necessary to obtain a holistic and in-depth analysis of the road network and/or the structure. At these points, recommendations are given which procedures or analyses are most effective or useful in the respective cases.

PART 2: Method & Guidance

1. Step One

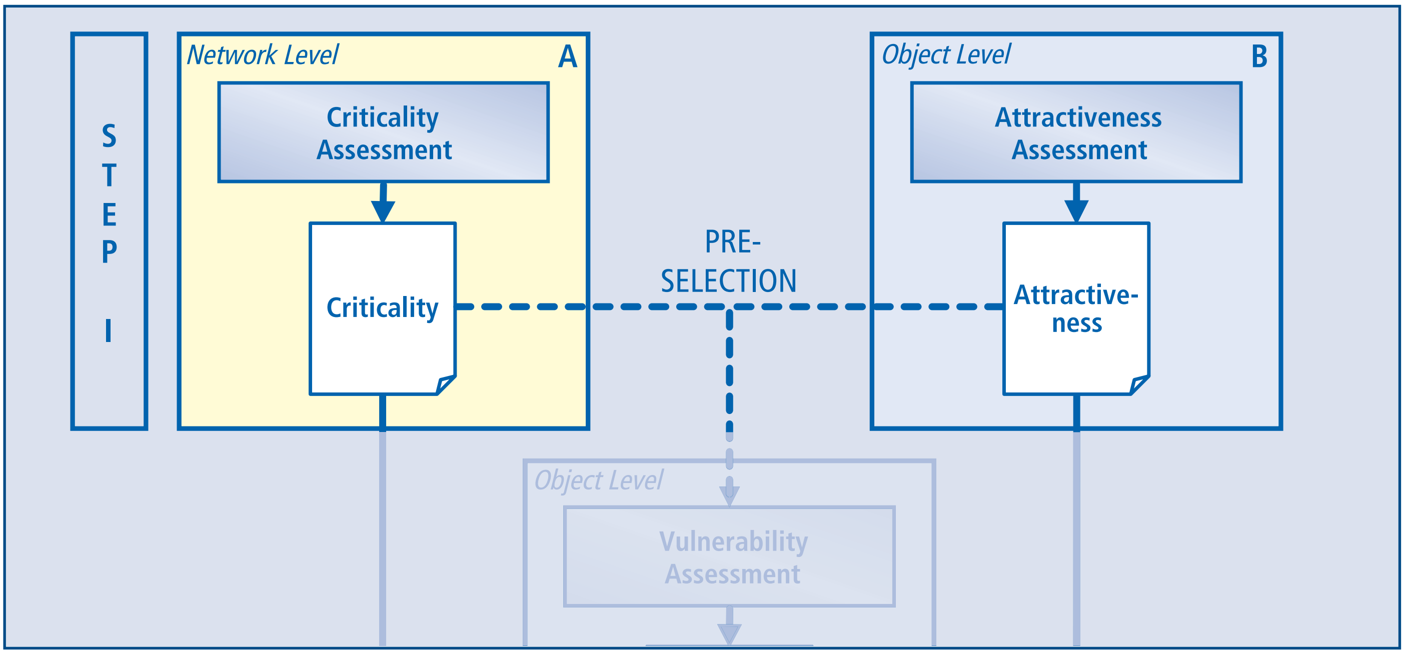
1.1 Introduction

The methodology developed in the course of the project SecMan is a decision support tool which enables owners and operators of a road network to check bridges and tunnels on their road network with respect to potential security risks. The methodology is easily applicable and relies on infrastructure data which is typically available for the user. However, it needs to be applied in the context of the specific security strategy of the owner/operator of the road network under investigation. For the final decision-making process – in addition to the results of the methodology – the user has to set his own priorities following these underlying strategic goals. In order to apply the methodology, the part of the road network to be investigated by the methodology has to be defined. The size of the network depends on the scope of the study.

The first step of the method is divided into two separate sub-steps: step 1A (criticality assessment) and step 1B (attractiveness assessment) which can be applied in parallel. Both steps use a simple qualitative assessment procedure and the output of both, "criticality" and "attractiveness" are crucial input for the following assessment procedures.

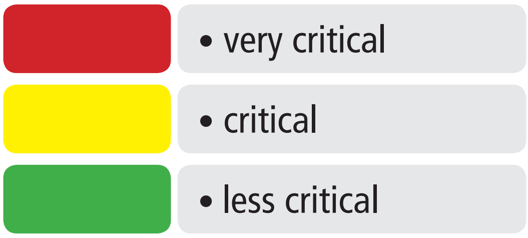
Additionally, both assessment procedures can be used as pre-selection methods in order to reduce the number of objects investigated in the more detailed "vulnerability assessment" in step 2.

» Figure 2 – Step 1 (Criticality and Attractiveness Assessment)



1.2 Step 1A: Criticality Assessment (Network level)

In a road network there are a set of sections which are important for the availability and the level-of-service of the whole network. In this step, each section in the defined road network part is assessed on the basis of a set of traffic parameters. During the assessment, each section on the road network has to be evaluated regarding its "criticality" by using a simple qualitative assessment procedure based on a "traffic light system" (see Figure 3). The criticality is an indicator for the importance of the functioning of section in the road network. The traffic parameters used for the assessment can also be used to divide the network into sections.



» Figure 3: Evaluation parameters for criticality assessment

The assessment can be done based on the following network parameters:

1. Alternative routes

The network section is more important if it has no or only less suitable alternative routes. These alternatives are suitable if the additional reroute time is not considerably higher and it is able to carry the existing and additional traffic in terms of traffic volume and traffic type.

2. Annual average daily traffic

The more traffic volume a specific road network section carries (the higher the AADT), the more important the section is.

3. Heavy goods vehicles

The higher the HGV share on a route, the more important it is for the traffic network. A high number of heavy goods vehicles can for example indicate to an important link for the economy.

4. Special transport

HGV-transport denoted as "special transport" requires certain permission for object types and is sometimes not allowed to cross certain object types. For tunnels e.g. dangerous goods transport is relevant; for bridges e.g. heavy load transportation.

However, these four parameters are given by the manual as default. There is still the possibility to add individual parameters or to carry out the assessment depending on a selection of the proposed parameters. If (very) critical road network sections are already known, this step can even be skipped.

Moreover, no thresholds for e.g. AADT or HGV share are proposed. Generally, these values depend strongly on the respective traffic network and differ from country to country.

This simple approach supports in dividing the road network into sections of different criticality based on the above mentioned parameters. On this basis, it gives an impression on the first sight, where (in which region) the most critical sections are located and it enables to rank the sections in the road network. Therefore, it supports the decision-making process by giving priorities where further assessment is necessary.

1.3 Step 1B: Attractiveness Assessment (Object level)

In step 1B, an attractiveness assessment of specific objects shall be performed. The recent past shows that there are certain factors, which could increase the feasibility of an attack and motivate attackers due to e.g. the resulting high media attention.

Each (possible attractive) object has to be evaluated on the basis of its "Attractiveness" using a simple qualitative assessment procedure based on a "traffic light system" (see Figure 4). The more attractive an object is to an attacker, the higher is the feasibility to be attacked and therefore a further assessment is recommended.

🟥	• very attractive
🟨	• attractive
🟩	• less attractive

Figure 4: Evaluation parameters for attractiveness assessment

Nevertheless, the attractiveness assessment is only a subjective procedure. In order to improve the outcome, a set of experts of different disciplines is recommended for the judgement of attractiveness. To support the experts, the following three different parameters can be used as a starting point for the assessment:

1. Symbolic value

The object may not be on a very important transport route, but it is well known in and outside of the country. An attack would probably result in high media attention worldwide.

2. High number of fatalities due to infrastructure collapse

The attractiveness increases, if an attack on the object, or one of its systems, can result in a high number of fatalities inside, above or beneath the infrastructure.

3. Secondary effects

An object can be more attractive for an attack if secondary effects of the attack influence for example other transport modes close to the infrastructure.

However, these three parameters are given by the manual as default. There is still the possibility to add individual parameters or to do the assessment only on a selection of the proposed parameters. If (very) attractive objects are already known, this step can be skipped.

1.4 Application for pre-selection

The two assessment processes in step 1 can be used as pre-selection methods for the vulnerability assessment. In practice, the investigated road network part can include a huge number of objects, which would lead to a very time-consuming assessment in step 2. By the use of these pre-selection methods the set of objects can be filtered and the number of objects to be assessed reduced. Objects with lower attractiveness and/or road sections with lower criticality do not have to be assessed in the subsequent steps. Additionally, it is recommended to filter out bridges with a span width less than 10-12 m. In practice, these objects can be replaced very fast by the use of mobile bridges.

1.5 Further recommendation

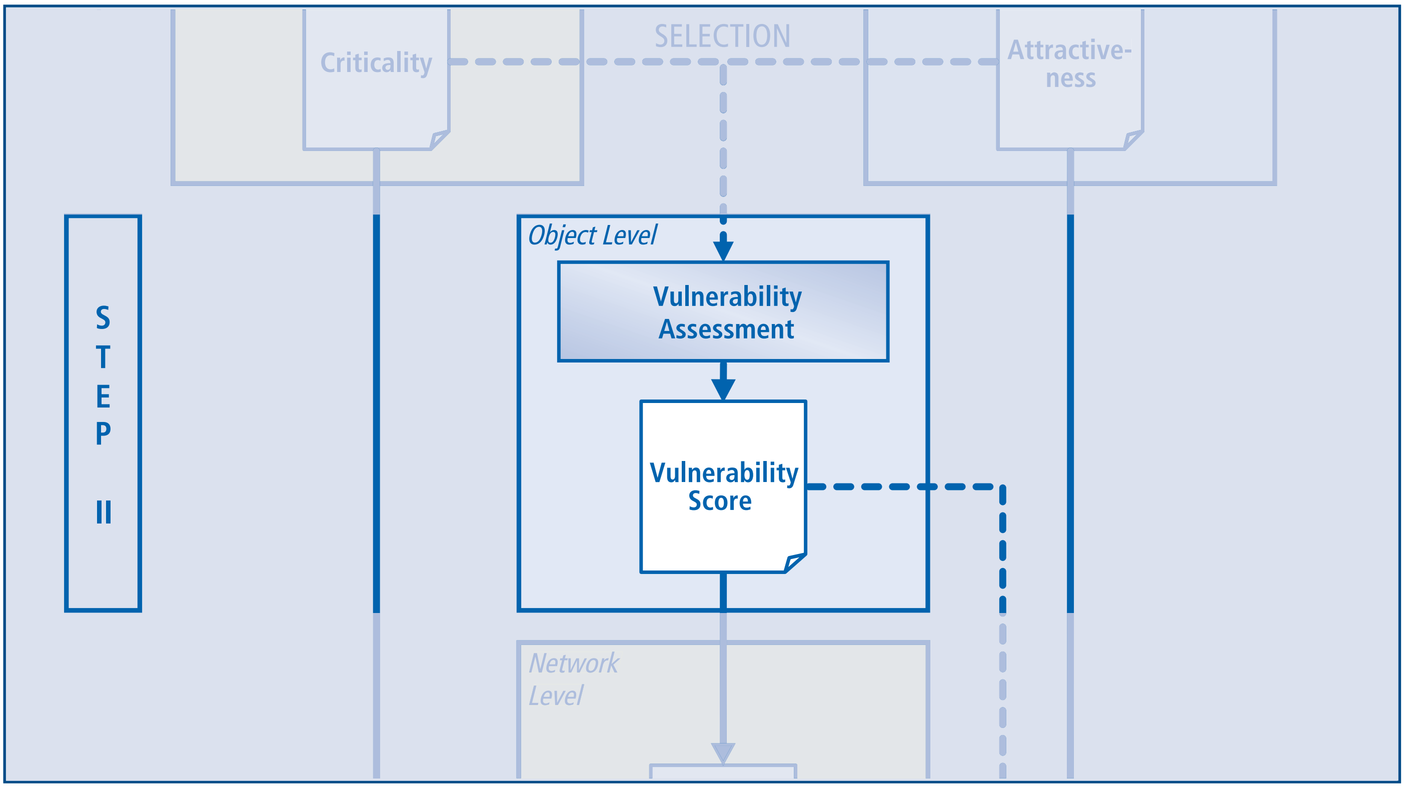
If the qualitative assessment procedures in Step 1 are not sufficient, the following methods can be used for a more in-depth analysis (level 2). For example, a detailed road network analysis with a detailed traffic and transport model can be applied to analyse the network and assess the criticality of different road sections.

2. Step Two

2.1 Introduction

Step 2 is an object-specific assessment of a tunnel or bridge regarding certain threat types called vulnerability assessment (see Figure 5). On the one hand, this step can be used individually in order to assess a specific object. On the other hand, this step can be used as one of the four steps in terms of the overall assessment of a network. However, it is recommended to use step 1 as pre-selection method in order to reduce the amount of objects which have to be assessed in more detail in step 2.

The output of this step is a quantitative value called "vulnerability score" which is crucial input for the following assessment procedures.

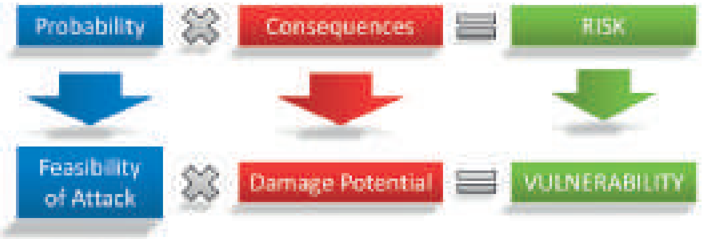


» Figure 5 – Step 2 (Vulnerability)

In traffic safety the term "risk" is often used, which is calculated by multiplying the chance (or probability) of a particular event occurring, with the impact (or consequence) associated with that event (risk equation). In the present context, a similar equation is used in order to define the vulnerability score as the product of "feasibility of attack" and "damage potential".

In terms of security, it is very not possible to deal with the probability of an intended event. Therefore, the term "feasibility of attack" was defined. It is determined using several aspects including the complexity of the attack and the capability of the attacker. To deal with the consequences of an intentional threat, the outcome of a very unfavourable scenario for the structure is assumed. Therefore, the damage potential comprises the potential material damage quantified by the time until the object can be used again ("out-of-service time").

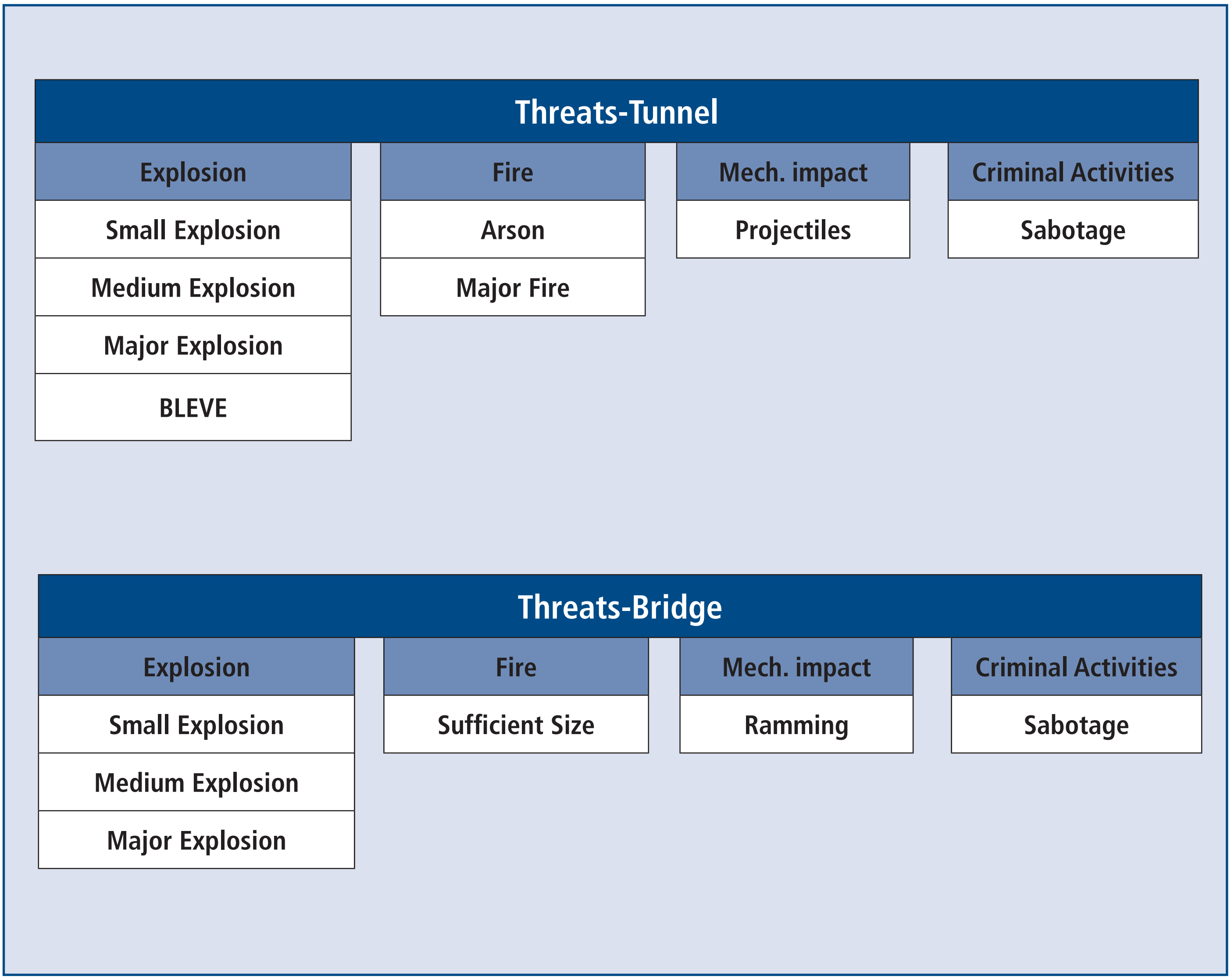
In Figure 6, the transition from probability, consequences and risk to feasibility of attack, damage potential and vulnerability – from safety to security – is shown.



» Figure 6: Risk vs. Vulnerability

2.2 Threats

As mentioned, the vulnerability assessment is a procedure to assess tunnels and/or bridges regarding certain threat types. In total, four threat types are considered relevant for both object types; whereas some are divided into sub-types (see Figure 7).



Threats-Tunnel			
Explosion	Fire	Mech. impact	Criminal Activities
Small Explosion	Arson	Projectiles	Sabotage
Medium Explosion	Major Fire		
Major Explosion			
BLEVE			

Threats-Bridge			
Explosion	Fire	Mech. impact	Criminal Activities
Small Explosion	Sufficient Size	Ramming	Sabotage
Medium Explosion			
Major Explosion			

» Figure 7: Set of relevant threats for tunnels and bridges

For tunnels explosions and major fires are within the tunnel tubes are relevant. Arson, projectiles and sabotage are only relevant for local tunnel operation centres and ventilation stations for smoke extractions systems. In case a tunnel includes one of these two special infrastructures, the vulnerability of the accompanying object has to be added to the respective tunnel vulnerability.

Additionally, for each specific threat a very unfavourable scenario for the structure was selected in order to develop the default values given in the user sheets. Due to very sensitive information on the weak spots of tunnel and bridge structures, these reference scenarios are not published in this manual.

2.3 Categorization

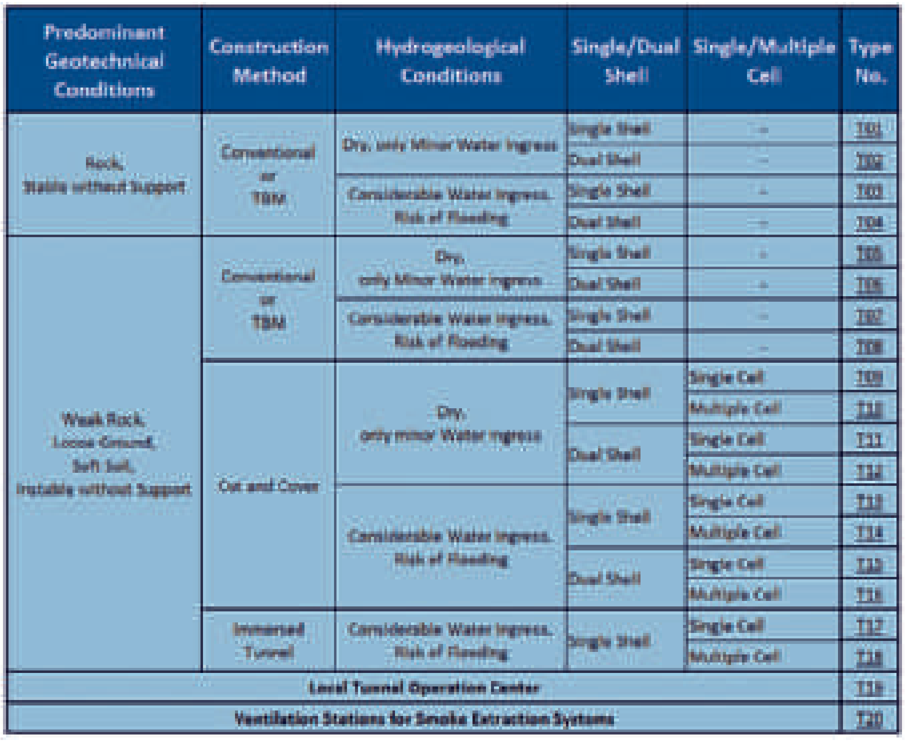
In practise, a wide variety of tunnels and bridges exists with each object having its specific properties. For the purpose of an assessment of these infrastructures and for the sake of comprehensibility, the infrastructures are categorized into a condensed number of representative object types. The criteria for the categorization of tunnels and bridges show huge distinctions between both tunnels and bridges. That is why they have been separated.

2.3.1 Tunnels

Figure 8 shows the categorization of tunnel structures based on the following five criteria:

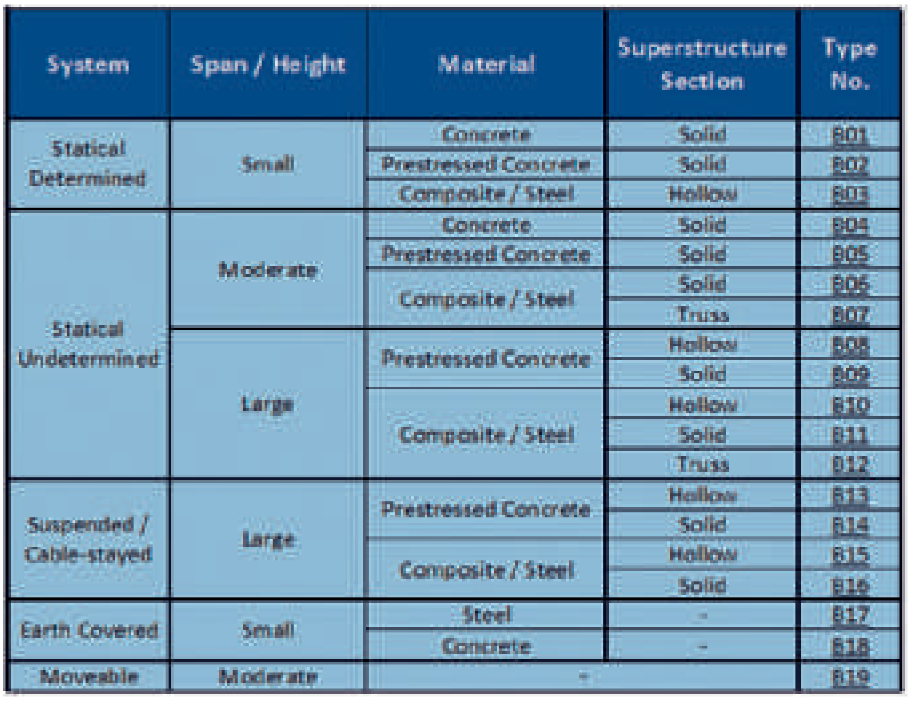
- Predominant geotechnical conditions
- Construction method (Conventional / NATM, TBM)
- Hydro-geological conditions
- Single shell vs. Dual shell
- Single cell vs. Multiple cells

Additionally, Local Tunnel Operation Centers and Ventilation Stations for Smoke Extraction Systems have been considered as relevant components of tunnel systems. For certain threat types of attack (e.g. sabotage) these components are crucial for the secure operation of the overall tunnel system. Including those two additional tunnel related components the categorization results in a total number of 20 tunnel types.



Predominant Geotechnical Conditions	Construction Method	Hydrogeological Conditions	Single/Dual Shell	Single/Multiple Cell	Type No.
Rock, Stable without Support	Conventional or TBM	Dry, only Minor Water Ingress	Single Shell	-	T01
			Dual Shell	-	T02
		Considerable Water Ingress, Risk of Flooding	Single Shell	-	T03
			Dual Shell	-	T04
Weak Rock, Loose Ground, Soft Soil, Instable without Support	Conventional or TBM	Dry, only Minor Water Ingress	Single Shell	-	T05
			Dual Shell	-	T06
		Considerable Water Ingress, Risk of Flooding	Single Shell	-	T07
			Dual Shell	-	T08
	Cut and Cover	Dry, only minor Water Ingress	Single Shell	Single Cell	T09
				Multiple Cell	T10
			Dual Shell	Single Cell	T11
				Multiple Cell	T12
		Considerable Water Ingress, Risk of Flooding	Single Shell	Single Cell	T13
				Multiple Cell	T14
			Dual Shell	Single Cell	T15
				Multiple Cell	T16
	Immersed Tunnel	Considerable Water Ingress, Risk of Flooding	Single Shell	Single Cell	T17
				Multiple Cell	T18
Local Tunnel Operation Center					T19
Ventilation Stations for Smoke Extraction Systems					T20

» Figure 8: Tunnel categorization



System	Span / Height	Material	Superstructure Section	Type No.
Statical Determined	Small	Concrete	Solid	B01
		Prestressed Concrete	Solid	B02
		Composite / Steel	Hollow	B03
Statical Undetermined	Moderate	Concrete	Solid	B04
		Prestressed Concrete	Solid	B05
		Composite / Steel	Solid	B06
			Truss	B07
	Large	Prestressed Concrete	Hollow	B08
			Solid	B09
		Composite / Steel	Hollow	B10
			Solid	B11
			Truss	B12
Suspended / Cable-stayed	Large	Prestressed Concrete	Hollow	B13
			Solid	B14
		Composite / Steel	Hollow	B15
			Solid	B16
Earth Covered	Small	Steel	-	B17
		Concrete	-	B18
Moveable	Moderate	-		B19

» Figure 9: Bridge categorization

2.3.2 Bridges

Figure 9 shows the categorization of bridge structures based on the following four criteria:

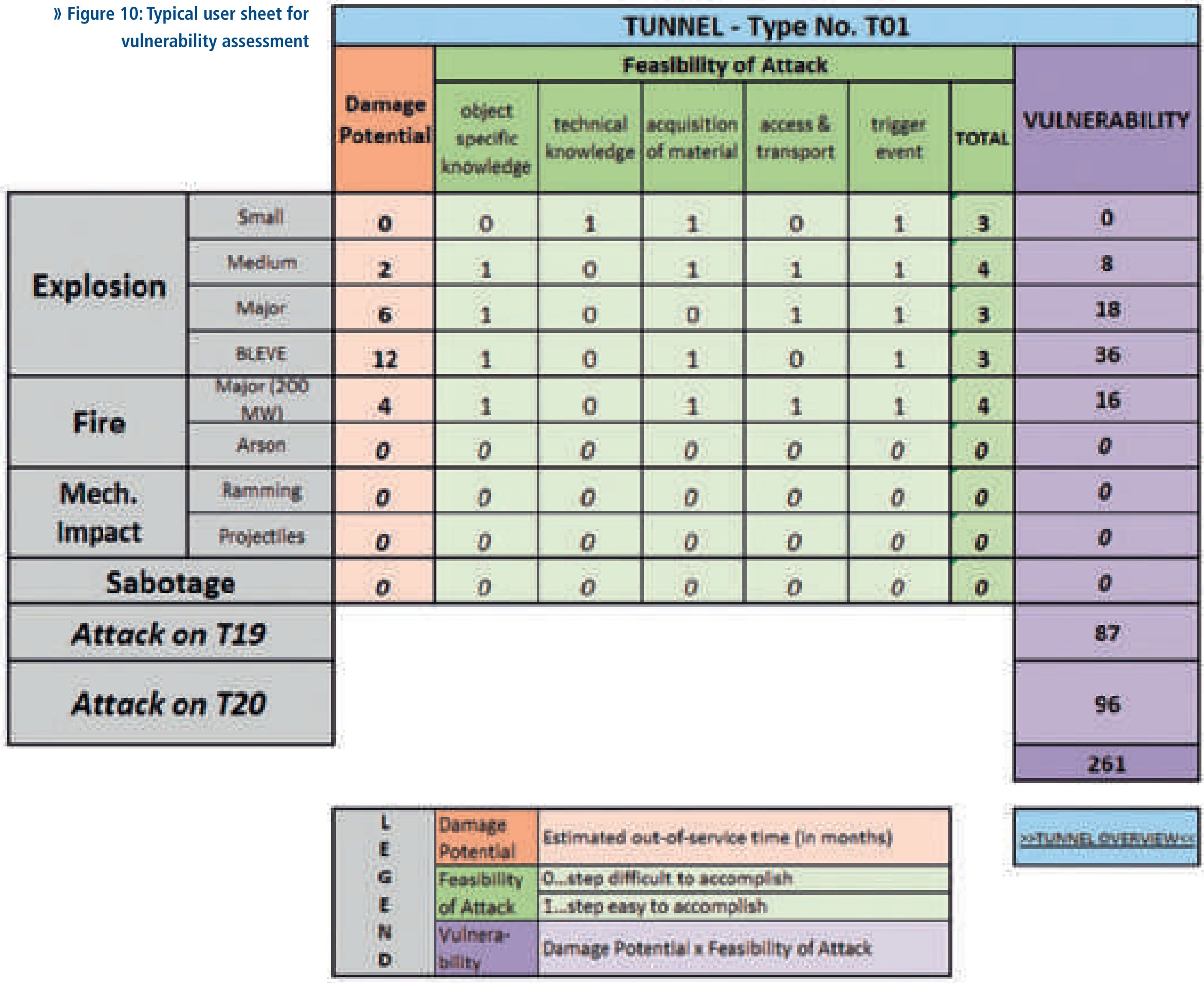
- System
- Span or height
- Construction material
- Superstructure cross-section

Including the special type of movable bridges a total number of 19 bridge types evolve.

2.4 Vulnerability Assessment

For the actual assessment procedure in step 2 the manual provides the user a set of user sheets (see Annex) where for each object type default values of the vulnerability score are given. Based on the categorization tables showed in Figure 8 and 9, detail sheets are available for each bridge and tunnel type. These sheets show a breakdown of the total vulnerability score into a set of relevant threats. Furthermore, for each threat type the two components (damage potential, feasibility of attack) are shown (see Figure 10). In practice, the user can adapt the given default values according to the specific situation. Due to the huge variety in tunnels and bridges it is recommended that (if necessary) both damage potential and feasibility of attack shall be modified for every object within the study.

» Figure 10: Typical user sheet for vulnerability assessment



		TUNNEL - Type No. T01							
		Damage Potential	Feasibility of Attack						VULNERABILITY
			object specific knowledge	technical knowledge	acquisition of material	access & transport	trigger event	TOTAL	
Explosion	Small	0	0	1	1	0	1	3	0
	Medium	2	1	0	1	1	1	4	8
	Major	6	1	0	0	1	1	3	18
	BLEVE	12	1	0	1	0	1	3	36
Fire	Major (200 MW)	4	1	0	1	1	1	4	16
	Arson	0	0	0	0	0	0	0	0
Mech. Impact	Ramming	0	0	0	0	0	0	0	0
	Projectiles	0	0	0	0	0	0	0	0
Sabotage		0	0	0	0	0	0	0	0
Attack on T19									87
Attack on T20									96
									261

LEGEND	Damage Potential	Estimated out-of-service time (in months)
	Feasibility of Attack	0...step difficult to accomplish 1...step easy to accomplish
	Vulnerability	Damage Potential x Feasibility of Attack

>>TUNNEL OVERVIEW<<

In order to make adaptions in the user sheets, background information about the two components of the vulnerability score is necessary. In the following chapters, detailed information about the feasibility of attack and damage potential is given.

2.4.1 Feasibility of attack

In order to perform a successful attack on a tunnel or bridge, the following five subsequent steps are necessary to be carried out by an attacker:

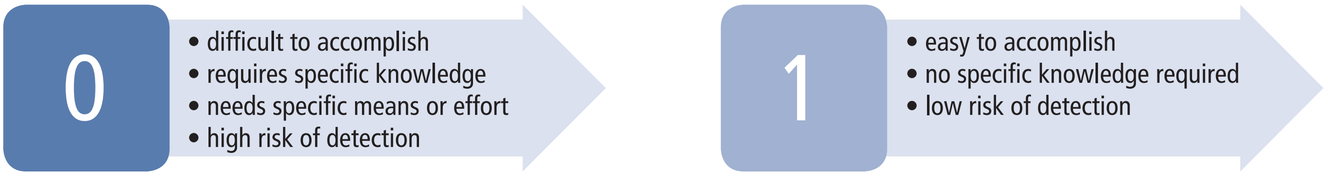
1. Object-specific knowledge: Specific engineering knowledge about the respective objects, like for example the weak spots of the tunnel or bridge in relation to a specific threat.

2. Knowledge of technology: Particular knowledge of the material or equipment intended to be used for the attack, like for example chemical know-how to produce TNT or technical know-how to build a remote release.

3. Acquisition of material in sufficient quantity: Possibility to successfully acquire the material in sufficient quantity to be dangerous for the specific structure to be attacked.
4. Access/transport of material to vulnerable components: First, the successful transport of the dangerous material to the object without being detected. Second, to have access to vulnerable components (weak spots) of the object – either in terms of the structure's design or of already implemented security measures.

5. Trigger event: Ability to trigger the event either remotely via technological equipment or the intention to conduct a suicide attack.

For each type of structure and threat, the likelihood that these five steps can be successfully accomplished can be assessed with a simple binary approach, by setting each step either to 0 or 1 (see Figure 11).



0
- difficult to accomplish
- requires specific knowledge
- needs specific means or effort
- high risk of detection

1
- easy to accomplish
- no specific knowledge required
- low risk of detection

» Figure 11: Binary approach for feasibility of attack assessment

2.4.2 Damage potential

As mentioned in the introduction, the focus of this manual is on the availability of important traffic infrastructure in order to maintain the functionality of important transport routes. In this respect, the relevant criteria for the assessment of the damage potential of an attack is the usability of a relevant transport infrastructure. Therefore, the relevant parameter to measure the consequences of an impact is the out-of-service time.

This parameter measures both the damage caused to the construction by a specific scenario and the typical reconstruction time of a specific structure (time required to repair or replace a damaged structure) in an integrated approach.

However, this value cannot be taken as prediction of the real reconstruction time of a specific structure, which may differ considerably in dependence of local and individual parameters. The maximum value was set to 36 (months). The reconstruction time also includes replacement of equipment (e.g. tunnel equipment, if an attack destroys equipment but does not hamper the structure), the repair of deformation (e.g. for bridges – in situations, where the structure does not collapse).

2.4.3 Output

The vulnerability assessment is on object level, meaning it has to be repeated for every object within the study. The user can either use the default values or modify them for the individual bridge or tunnel. For this purpose, the out-of-service time and/or the difficulty to accomplish the five subsequent steps for a successful attack can be adapted for individual threat types.

Based on the resulting vulnerability score, objects within a part of a network can be ranked according to their vulnerability against a set of threats. This information is important for the decision-making process in step 3.

2.5 Further recommendation

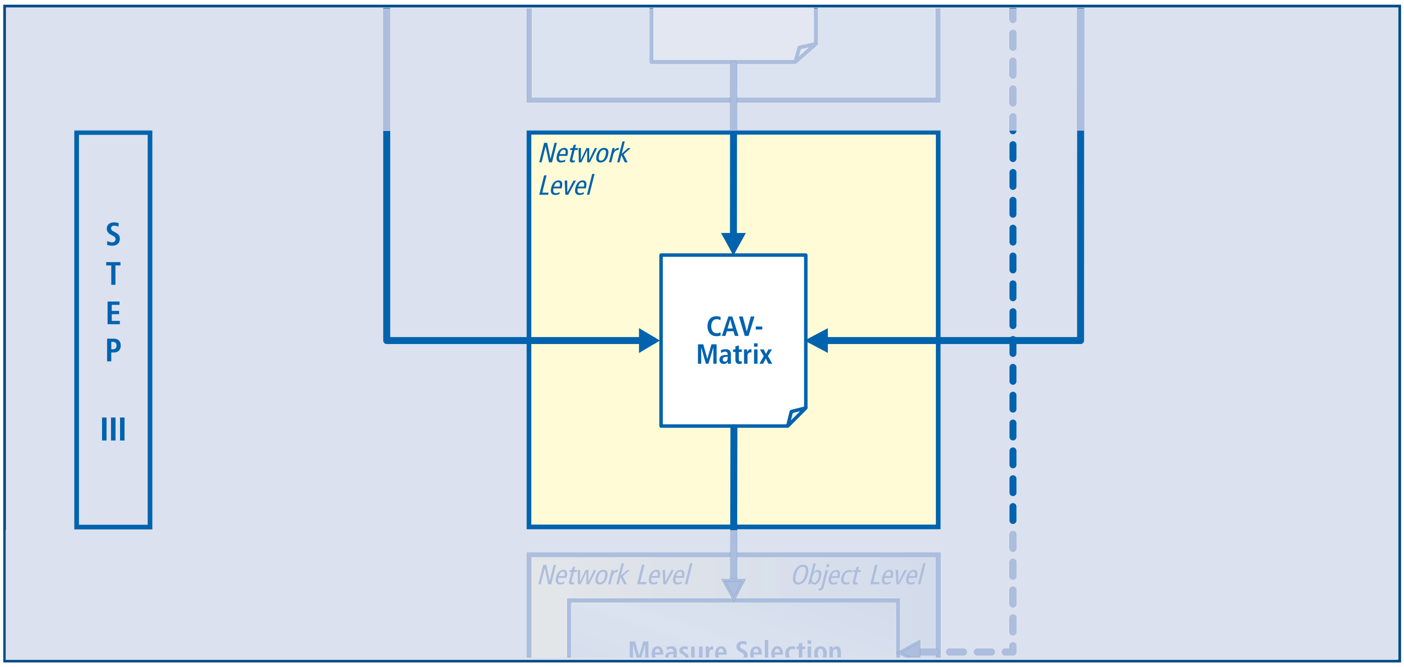
The vulnerability assessment in step 2 is a rough approach in order to identify the most vulnerable objects in a network. For a more detailed assessment of the most vulnerable infrastructures it is recommended to perform a risk analysis on object level. In order to assess the damage potential of individual objects, simulation tools for fires, explosions or ramming can be used. In the research projects SeRoN (http://www.seron-project.eu) and SKRIBT (http://www.skribt.org) a variety of detailed analyses has been performed. For more information please visit the respective website or the publically available reports.

3. Step Three

3.1 Introduction

Step 3 is a simple procedure on network level combining all outputs from the previous assessment steps and neatly arranges them in the "CAV-matrix" (Criticality-Attractiveness-Vulnerability) with the objective to sort or rank objects based on the three parameters and to support the decision-making process concerning security-relevant aspects. At this stage of the process strategic aspects are coming into play: the methodology produces a structured survey of more or less critical/ attractive or vulnerable objects, but does not automat cally produce an unambiguous ranking; to achieve this, the user has to set priorities for the individual security parameters or introduce other aspects relevant for a decision.

This step can be skipped if only individual objects are to be assessed based on their vulnerability. The CAV-matrix is crucial input for the measure assessment in step 4.



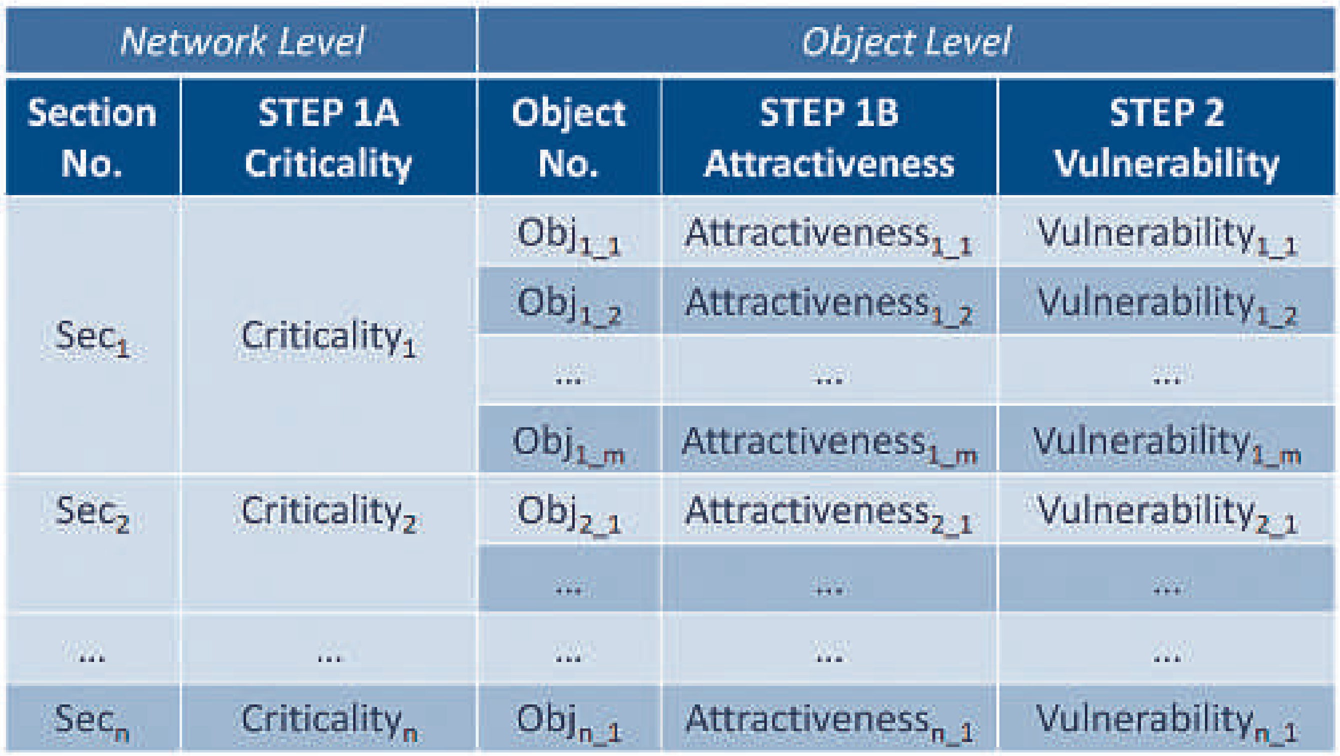
» Figure 12: Step 3 (CAV-Matrix)

3.2 Methodology

In more detail, the inputs for the matrix are:

- Step 1A: Criticality (network level)
- Step 1B: Attractiveness (object level)
- Step 2: Vulnerability (object level)

The three CAV-parameters are summarized into a table according to Figure 13. In the left columns, the road network sections are listed including their criticality. On each section, a number of objects (tunnels and/or bridges) exist, where each has a certain attractiveness and vulnerability.



Network Level		Object Level		
Section No.	STEP 1A Criticality	Object No.	STEP 1B Attractiveness	STEP 2 Vulnerability
Sec$_1$	Criticality$_1$	Obj$_{1\_1}$	Attractiveness$_{1\_1}$	Vulnerability$_{1\_1}$
		Obj$_{1\_2}$	Attractiveness$_{1\_2}$	Vulnerability$_{1\_2}$
		...	...	...
		Obj$_{1\_m}$	Attractiveness$_{1\_m}$	Vulnerability$_{1\_m}$
Sec$_2$	Criticality$_2$	Obj$_{2\_1}$	Attractiveness$_{2\_1}$	Vulnerability$_{2\_1}$
		...	...	...
...	...	...	...	...
Sec$_n$	Criticality$_n$	Obj$_{n\_1}$	Attractiveness$_{n\_1}$	Vulnerability$_{n\_1}$

» Figure 13: CAV-Matrix (abstract illustration)

Basically, the matrix is a summary of all results in order to allow for a ranking of the different CAV parameters according to the user's needs. After filling in, all values for the three CAV-parameters, the user can sort objects in the matrix based on the given priority of each column. Which CAV-parameter is most important depends on the demands of the user.

This method does not define priorities for the three CAV-parameters, but it enables a ranking procedure of infrastructures. If the strategic goal would be the availability of the traffic network, a possible approach could be to assess first the objects within the most critical sections. However, other approaches are possible depending on each individual problem.

On the SecMan-website a simple software tool can be downloaded which shall support to set up the CAV-matrix and rank sections and objects according to the defined priorities (see **http://www.secman-project.eu**).

- In the end, the matrix shall support the user in answering the question which section or object in the network is the most critical, (and what are the reasons for this result), and

- in the decision-making process for which objects on which sections measures shall be implemented first.

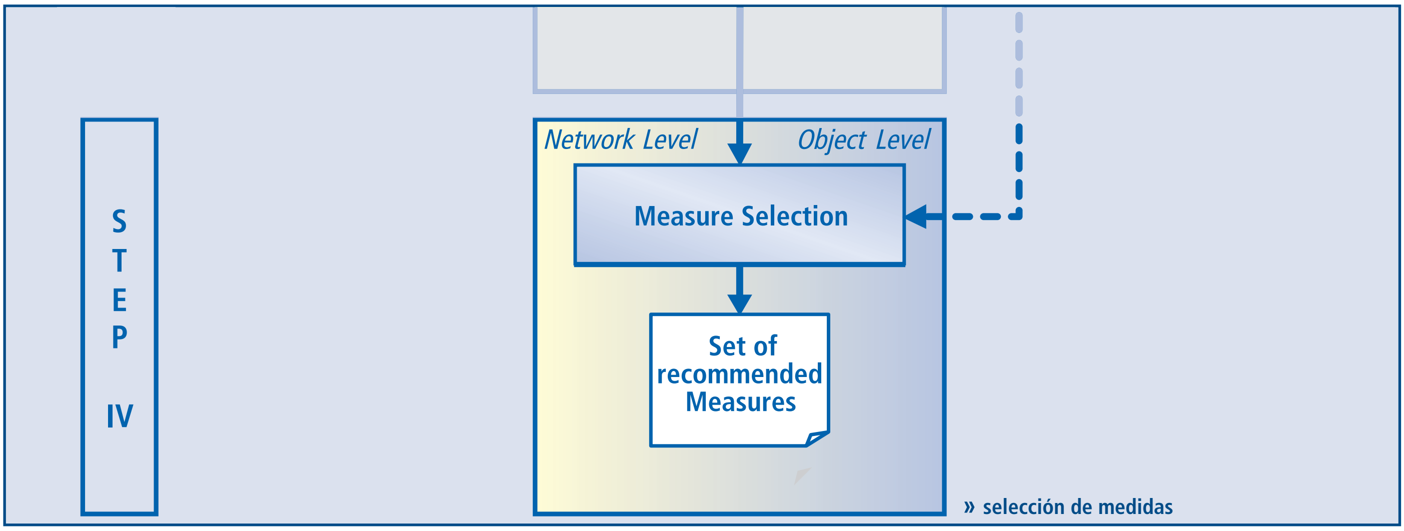
4. Step Four

4.1 Introduction

In general, the aim of the measure selection process is to present the user a decision support for the selection of measures for structures or network sections which have been prioritised during the previous step. The process is automated to allow the user to apply different measures and test them in a repetitive manner. To increase the efficiency and transparency of such repetitive process, simple yet efficient software was developed. Hereinafter, general descriptions and definitions are given. More details and the background can be found in the measures selection software user guide, which is available for download together with the software itself on **http://www.secman-project.eu.**

It is important to understand that the measure selection process gives a first indication on what possible security measures could be. Therefore, the results obtained need to be compared and analysed diligently against object/network specific data which could affect the risks and efficiency of counter measures but are not comprise in the step 1, 2 or 3.

Furthermore as already stated previously, the user must clearly distinguish between safety and security measures. At the moment, many safety measures are already included in the design and operation of the observed objects or networks. With detailed analyses, which are not part of this manual, it can be further evaluated, which of the already existing safety measures affects the security of the object/network. Security measures can have a beneficial effect on safety but this topic is beyond the scope of the manual.



» Figure 14: Step 4 (Measure Selection)

4.2 Categorizatio of measures

In the manual the measures are grouped according to the following table.

Measure type		Description
Network level measures		Network level measures are relevant for the entire network part under consideration. This means that measures are implemented for entire road network parts and not the objects on the former. The measures selection in is not affected by variation in the characteristics of the network part. Additionally, network measures are efficient to mitigate Criticality and Feasibility of attack.
General object level measures		General object level measures cover those measures, which are relevant for all objects (bridges, tunnels and accompanying infrastructures). General measures are efficient to mitigate Criticality and Feasibility of attack.
Measures for bridges	All bridges	Object level measures which are valid for all bridges.
	Different bridge types	Object level measures which are relevant for specific bridge types according to Step 2 of the methodology.
Measures for tunnels	All tunnels	Object level measures which are valid for all tunnels.
	Different tunnel types	Object level measures which are relevant for specific tunnel types according to Step 2 of the methodology.
Measures for accompanying infrastructures		Three additional object types are added: Operation and Control centres, Ventilation Stations for Smoke Extraction Systems, Other electro-technical objects and elements.

» Figure 15: Categorization of measures

In each group a set of default measures are proposed by the manual. The method allows adapting the set of measures by adding or removing individual measures.

4.3 Measure selection process

The methodology of the measure selection process allows the user to determine the relevant measures for each type of structure and for each threat, combining them into a measure catalogue. Additionally, it has to be noted that this process may also be used individually, apart from the other steps, as a first indication on possible strategies to deal with security issues.

Furthermore, the user has the possibility to add, remove or modify measures. However, the relevant regulations, technical approach, political, societal view, legal system, etc. of the country should be considered. When adding a new measure, the user also has to define a connection (effect) of the new measure on the CAV parameters (discussed in Step 3).

In order to get the most suitable list of measures based on the individual problem, the user is encouraged to choose the relevant parameters. In the software three different groups of parameters are existent:

Measure type:

First, the user can select measures according to his/her object type or network section. As explained in 4.2, measures are categorized into five groups. The selection process allows adapting the query according to the individual problem. With that, the user can choose between network level or object level measure. Additionally, measures for all or only for one specific object type can be selected.

New Object or Retrofitting:

Some measures are only relevant for new objects, others only for existing ones. In this group of parameters the user can choose if the observed object is not yet constructed (new object/network) or if the measures should be included during a retrofitting cycle.

CAV parameters:

By selecting individual CAV parameters the method allows us to obtain the output of measures according to object/network section specific criticality, damage potential and feasibility of attack parameters. However, it is recommended that in the first run of the selection process all parameters are selected and in the second run the set of parameters is reduced.

4.4: Further Recommendations

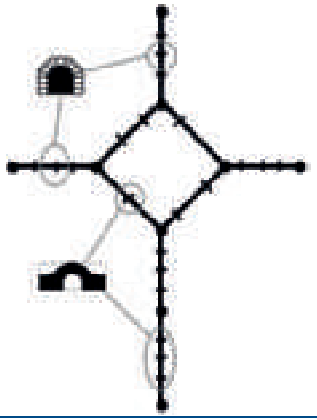
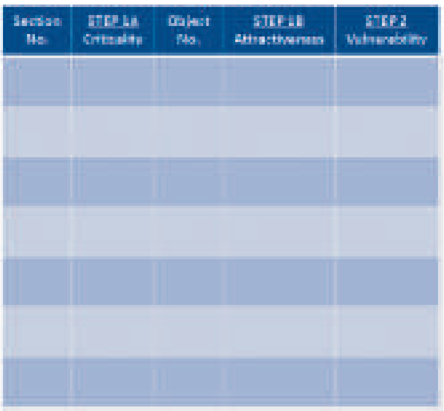
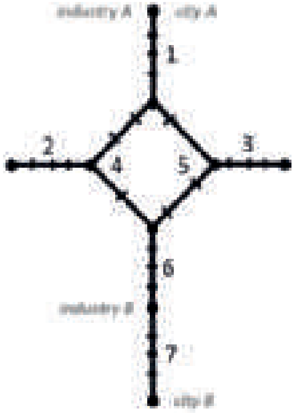
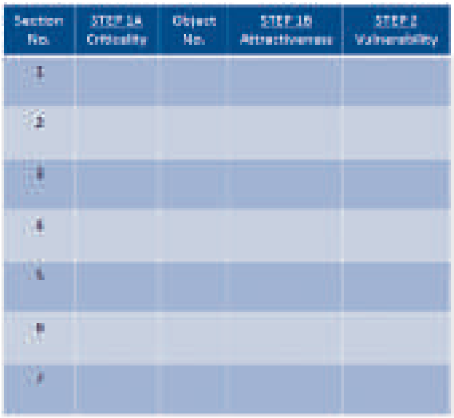
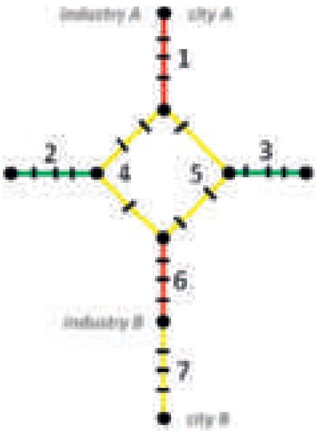
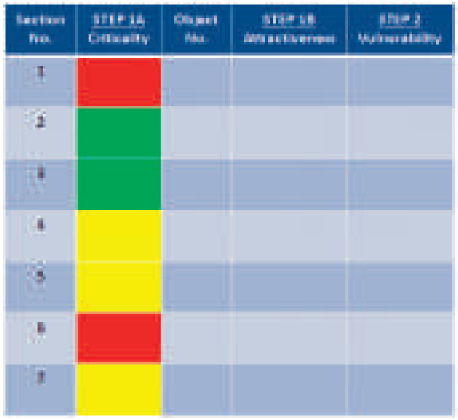
The measure selection process is made according to common properties, characteristics and features of objects/networks in an automated and repetitive manner for different networks, bridges, tunnels and accompanying infrastructure. The advantage of this is that the measure selection process can be done for a great number of objects, networks with the same procedure and definitions. However, not all of the details and properties of the objects/networks could be included in the methodology. Therefore, a critical review of the output of measures is necessary. Via this review, the following questions should be tackled:

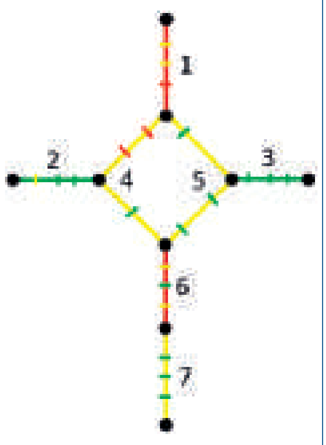
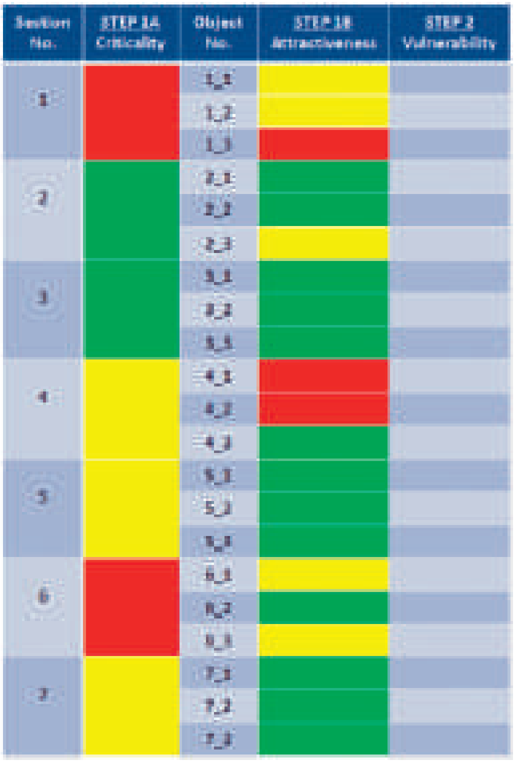
- Are measures efficient for the observed object/network?
- Are measures cost-justified?
- Do measures cover the assessed risks?
- Are there any negative effects with the measure implementation?
- Is safety reduced because of the measures?
- Is the overall effect of the measures combinations and decision making correct?
- Is the combination of measure selection parameters suitable and do they cover all major threats?
- Are measures and their effects defined properly and do they reflect properties of the real object?

For answering these questions, detailed investigations (Level 2) are necessary. These could include a detailed risk analysis with and without measures to received information on the effectiveness of a measure. Additionally, this could be supported via a cost-benefit analysis. Discussions on the applicability and method for these analyses have been presented in the research projects SeRoN **(http://www.seron-project.eu)** and SKRIBT **(http://www.skribt.org).**

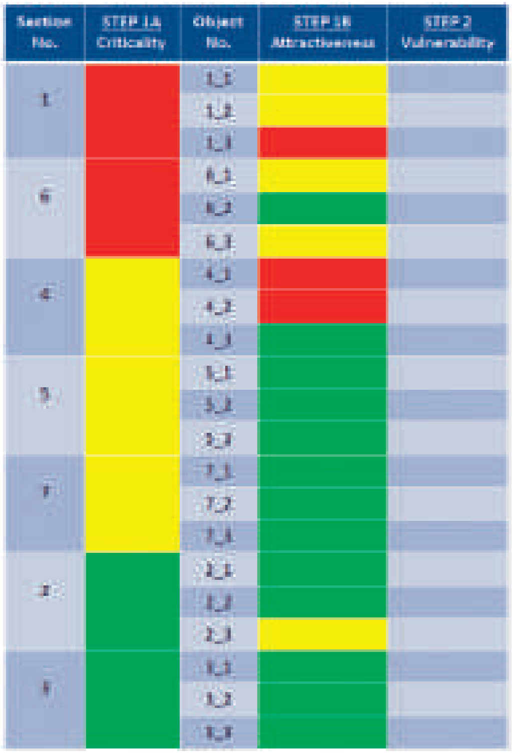
PART 3: Practical Example

The following practical example illustrates the methodology based on a very simple part of a network. This example should help the user to follow the 4 step procedure. However, it should be noted that this example is very limited. The actual implementation of the user might differ in terms of scope and results.

<table>
<tr><th></th><th>Network</th><th>CAV-Matrix</th><th>Comments</th></tr>
<tr><td>1</td><td></td><td>
<table>
<tr><th>Section No.</th><th>STEP 1A Criticality</th><th>Object No.</th><th>STEP 1B Attractiveness</th><th>STEP 2 Vulnerability</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td><td>In the beginning it has to be decided which network part shall be assessed and the boundaries have to be defined.
On the network part there is a set of tunnels and bridges. In this example, 21 objects are existent.
For the application of the subsequent steps, certain traffic data and basic knowledge about the network part and its objects are necessary. It is assumed that this general data is normally available by the target group of this manual.</td></tr>
<tr><td>2</td><td>
</td><td>
<table>
<tr><th>Section No.</th><th>STEP 1A Criticality</th><th>Object No.</th><th>STEP 1B Attractiveness</th><th>STEP 2 Vulnerability</th></tr>
<tr><td>1</td><td></td><td></td><td></td><td></td></tr>
<tr><td>2</td><td></td><td></td><td></td><td></td></tr>
<tr><td>3</td><td></td><td></td><td></td><td></td></tr>
<tr><td>4</td><td></td><td></td><td></td><td></td></tr>
<tr><td>5</td><td></td><td></td><td></td><td></td></tr>
<tr><td>6</td><td></td><td></td><td></td><td></td></tr>
<tr><td>7</td><td></td><td></td><td></td><td></td></tr>
</table></td><td>Based on general transport nodes, the network part is divided into 7 sections, where each section is numbered. The criteria to assign sections depend on the user, but it is recommended to use the same traffic parameters as in step 1A for the criticality assessment.
In this example, there are two main cities and two industrial areas in the north and south which are connected via a main road. In between, the link is split into two equivalent roads.</td></tr>
<tr><td>3</td><td>
</td><td>
<table>
<tr><th>Section No.</th><th>STEP 1A Criticality</th><th>Object No.</th><th>STEP 1B Attractiveness</th><th>STEP 2 Vulnerability</th></tr>
<tr><td>1</td><td>🟥</td><td></td><td></td><td></td></tr>
<tr><td>2</td><td>🟩</td><td></td><td></td><td></td></tr>
<tr><td>3</td><td>🟩</td><td></td><td></td><td></td></tr>
<tr><td>4</td><td>🟨</td><td></td><td></td><td></td></tr>
<tr><td>5</td><td>🟨</td><td></td><td></td><td></td></tr>
<tr><td>6</td><td>🟥</td><td></td><td></td><td></td></tr>
<tr><td>7</td><td>🟨</td><td></td><td></td><td></td></tr>
</table></td><td>Each section is qualitatively assessed based on traffic parameters such as alternative routes, annual average daily traffic (AADT), heavy goods vehicle share (HGV) and suitability for special transports. Sections are either classified as "very critical", "critical" or "less critical".
In this example, the north-south link is a transit route which is very critical due the high AADT and HGV share between city A and city B and the lack of alternative routes. In section 4, 5 and 7 the criticality is decreased due to the availability of an alternative route for section 4 and 5 and the reduced HGV share in section 7. The section 2 and 3 are not on the transit route and of minor importance for the traffic.</td></tr>
</table>

	Network	CAV-Matrix	Comments
4			In step 1B the attractiveness assessment is performed for all objects on the network part, based on parameters like symbolic value, high number of fatalities or other secondary effects in case of an attack onto the infrastructure. Objects are either "very attractive", "attractive" or "less attractive". In this example, most of the objects are less attractive except for some internationally known tunnels and bridges (e.g. historic bridge which is important for the townscape, tunnel on a route to holiday area and well-known due to news about congestion during summer, etc.). Those objects are assessed with a different degree of attractiveness.

Section No.	STEP 1A Criticality	Object No.	STEP 1B Attractiveness	STEP 2 Vulnerability
1	🟥	1_1	🟨	
		1_2	🟨	
		1_3	🟥	
2	🟩	2_1	🟩	
		2_2	🟩	
		2_3	🟨	
3	🟩	3_1	🟩	
		3_2	🟩	
		3_3	🟩	
4	🟨	4_1	🟥	
		4_2	🟥	
		4_3	🟩	
5	🟨	5_1	🟩	
		5_2	🟩	
		5_3	🟩	
6	🟥	6_1	🟨	
		6_2	🟩	
		6_3	🟨	
7	🟨	7_1	🟩	
		7_2	🟩	
		7_3	🟩	

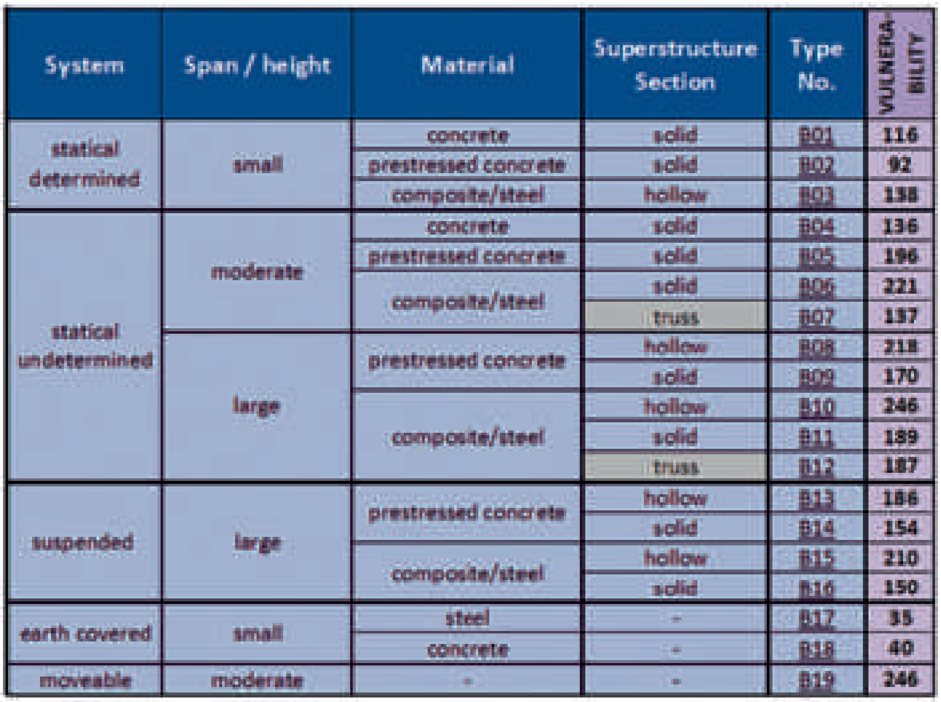
	Network	CAV-Matrix	Comments
5			As mentioned, step 1 can be used as pre-selection method in order to reduce the number of objects assessed in the next steps. Depending on the individual priorities, the user has to decide which objects shall be assessed in step 2. The CAV-matrix gives the user the opportunity to rank the sections/objects according to the defined priority. In this example, first priority is given to criticality, followed by attractiveness. Furthermore, it is decided that very critical and critical sections, as well as very attractive and attractive objects shall be further assessed. This results in a detailed vulnerability assessment of 16 objects.

Section No.	STEP 1A Criticality	Object No.	STEP 1B Attractiveness	STEP 2 Vulnerability
1	🟥	1_1	🟨	
		1_2	🟨	
		1_3	🟥	
6	🟥	6_1	🟨	
		6_2	🟩	
		6_3	🟨	
4	🟨	4_1	🟥	
		4_2	🟥	
		4_3	🟩	
5	🟨	5_1	🟩	
		5_2	🟩	
		5_3	🟩	
7	🟨	7_1	🟩	
		7_2	🟩	
		7_3	🟩	
2	🟩	2_1	🟩	
		2_2	🟩	
		2_3	🟨	
3	🟩	3_1	🟩	
		3_2	🟩	
		3_3	🟩	

CAV-Matrix

Comments

6



System	Span / height	Material	Superstructure Section	Type No.	VULNERA-BILITY
statical determined	small	concrete	solid	B01	116
		prestressed concrete	solid	B02	92
		composite/steel	hollow	B03	138
statical undetermined	moderate	concrete	solid	B04	136
		prestressed concrete	solid	B05	196
		composite/steel	solid	B06	221
			truss	B07	137
	large	prestressed concrete	hollow	B08	218
			solid	B09	170
		composite/steel	hollow	B10	246
			solid	B11	189
			truss	B12	187
suspended	large	prestressed concrete	hollow	B13	186
			solid	B14	154
		composite/steel	hollow	B15	210
			solid	B16	150
earth covered	small	steel	-	B17	35
		concrete	-	B18	40
moveable	moderate	-	-	B19	246

In the vulnerability assessment in step 2, the overview table (available for tunnels and bridges) is used to categorize the objects. The table contains default values valid for common bridges and tunnels without any special characteristics.

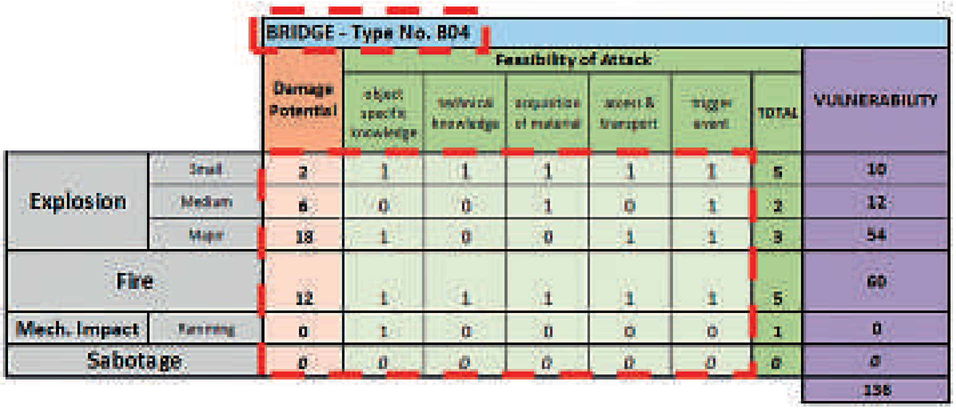
Beginning from the first object in the matrix, object 1_1 is a moderate statically undetermined bridge with the construction material concrete and a solid superstructure section.

According to the SecMan categorization, it is bridge type B04 with the default vulnerability score of 136.

CAV-Matrix

Comments

7



BRIDGE - Type No. B04

		Damage Potential	Feasibility of Attack						VULNERABILITY
			object specific knowledge	technical knowledge	acquisition of material	access & transport	trigger event	TOTAL	
Explosion	Small	2	1	1	1	1	1	5	10
	Medium	6	0	0	1	0	1	2	12
	Major	18	1	0	0	1	1	3	54
Fire		12	1	1	1	1	1	5	60
Mech. Impact	Ramming	0	1	0	0	0	0	1	0
Sabotage		0	0	0	0	0	0	0	0
									136

The manual gives the user the possibility to adjust the damage potential and/or feasibility of attack according to the specific characteristics of the assessed bridge.

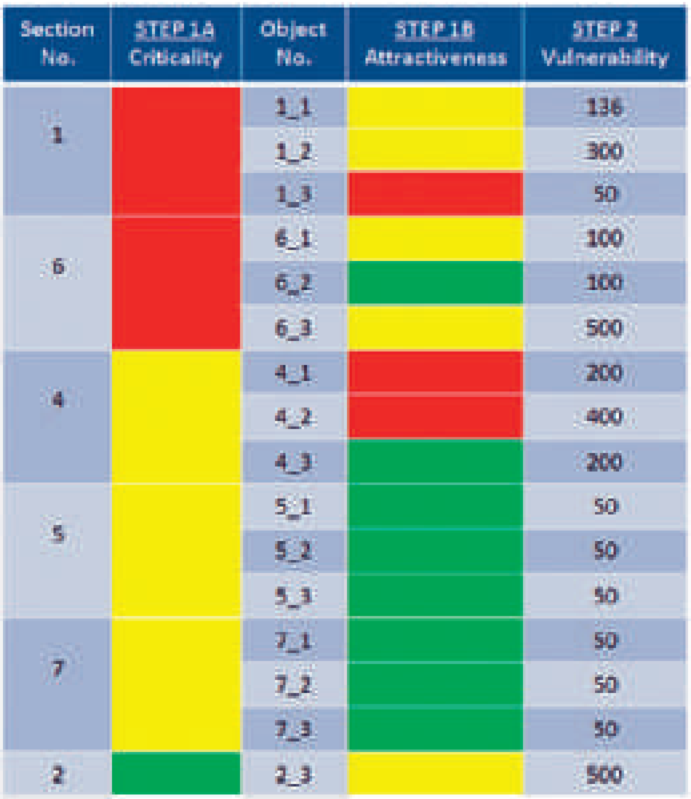
Adjustments can be made in case of for example:

- » protection measures are already implemented (e.g. blast protection) àreduce damage potential
- » access to specific bridge is difficult due to topographic circumstances àaccess & transport is 0 for all threats
- » etc.

It is recommended to make adjustments for every object within the study. However, this is not a prerequisite since the method can be applied with the default values as well

8

CAV-Matrix



Section No.	STEP 1A Criticality	Object No.	STEP 1B Attractiveness	STEP 2 Vulnerability
1	🟥	1_1	🟨	136
		1_2	🟨	300
		1_3	🟥	50
6	🟥	6_1	🟨	100
		6_2	🟩	100
		6_3	🟨	500
4	🟨	4_1	🟥	200
		4_2	🟥	400
		4_3	🟩	200
5	🟨	5_1	🟩	50
		5_2	🟩	50
		5_3	🟩	50
7	🟨	7_1	🟩	50
		7_2	🟩	50
		7_3	🟩	50
2	🟩	2_3	🟨	500

Comments

After repeating step 2 and assessing the vulnerability for all prioritized objects, the results can be entered into the CAV-matrix.

Note: Due to the possibility of user adjustments, two objects of the same object type can have different vulnerabilities.

Now step 1 and step 2 are finished and the CAV-matrix is complete. The main process in step 3 is the decision setting of the priority of the three CAV-parameters. Depending on the priorities set by the user, the ranking of objects can differ significantly. The following example shows that by setting different priorities three different objects can be top-ranked:

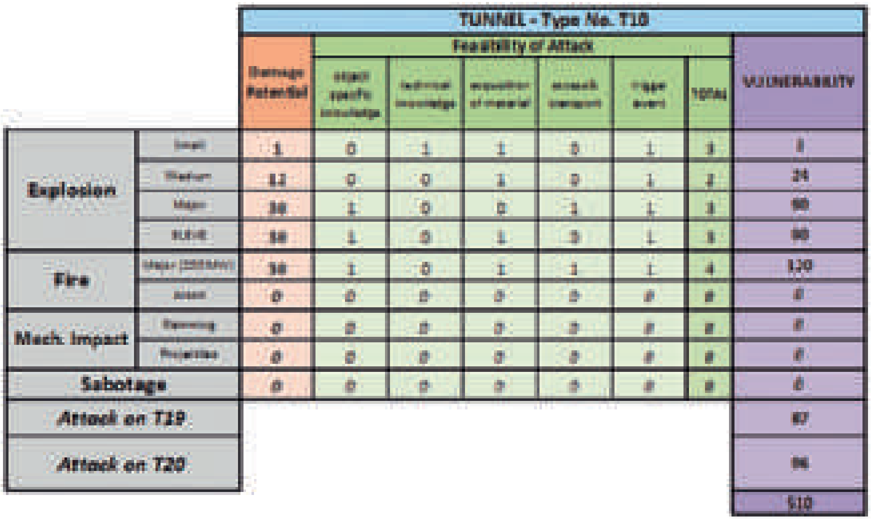
- 1. Criticality, 2. Attractiveness: object 1_3
- 1. Criticality, 2. Vulnerability: object 6_3
- 1. Attractiveness, 2. Vulnerability: object 4_2

It lies within the responsibility of the user to prioritize the CAV parameters according to his strategic goals.

This final ranking can be used as input into step 4 or to identify relevant objects for further assessment (e.g. detailed risk assessment).

9

CAV-Matrix



		TUNNEL - Type No. T10							
		Damage Potential	Feasibility of Attack						VULNERABILITY
			object specific knowledge	technical knowledge	acquisition of material	[illegible]	trigger event	TOTAL	
Explosion	Small	1	0	1	1	0	1	3	3
	Medium	12	0	0	1	0	1	2	24
	Major	30	1	0	0	1	1	3	90
	BLEVE	30	1	0	1	0	1	3	90
Fire	Major [illegible]	30	1	0	1	1	1	4	120
	[illegible]	0	0	0	0	0	0	0	0
Mech. Impact	Ramming	0	0	0	0	0	0	0	0
	Projectiles	0	0	0	0	0	0	0	0
Sabotage		0	0	0	0	0	0	0	0
Attack on T19									87
Attack on T20									96
									510

Comments

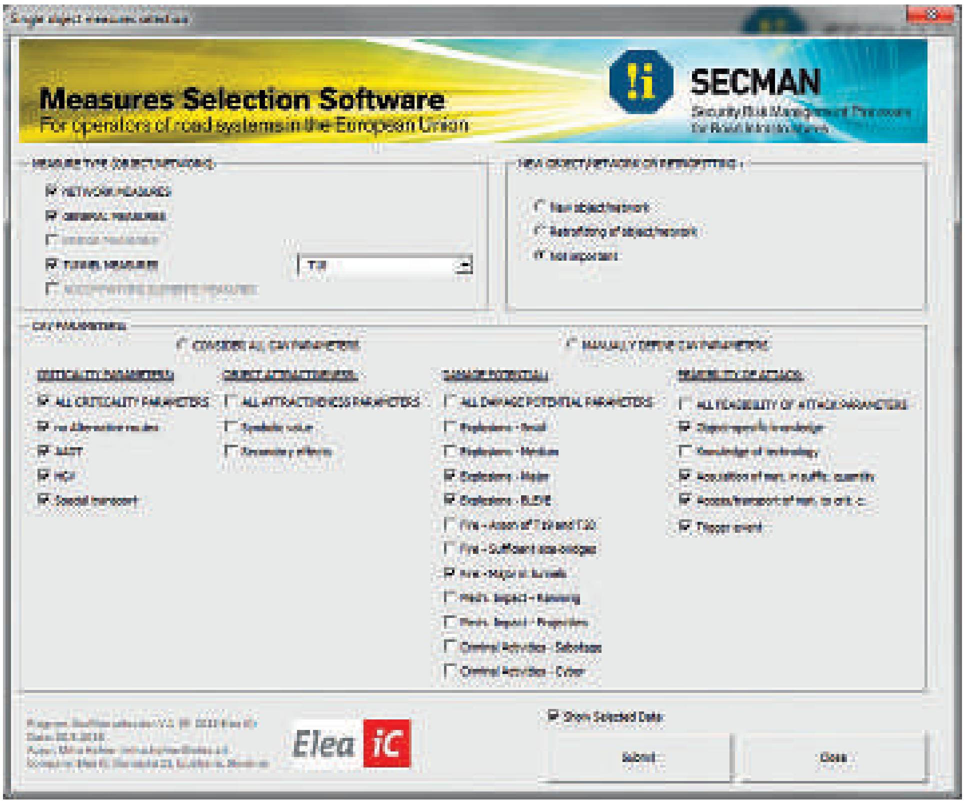
The result of the decision-making process in step 3 is a (reduced) list of objects which are ranked according to their priority to implement measures.

In this example, the first priority is set to criticality and then to vulnerability. That is why, the first object on the list is object 6_3 which is on a very critical network section and has a total vulnerability score of 510.

To reduce the overall security risk, measures to reduce the criticality and vulnerability have to be identified.

The detailed vulnerability sheet of the specific object is used to identify the threats with the highest damage potential (major explosion, BLEVE and major fire) and the critical feasibility of attack parameters.

In the next step, measures shall be identified to reduce the damage potential as well as the feasibility of attack parameters.

	CAV-Matrix	Comments
10	 Single object measures selection Measures Selection Software For operators of road systems in the European Union SECMAN Security Risk Management Processes for Road Infrastructures MEASURE TYPE (OBJECT/NETWORK): ☑ NETWORK MEASURES ☑ GENERAL MEASURES ☐ BRIDGE MEASURES ☑ TUNNEL MEASURES T10 ☐ ACCOMPANYING ELEMENTS MEASURES NEW OBJECT/NETWORK OR RETROFITTING: ○ New object/network ○ Retrofitting of object/network ● Not important CAV PARAMETERS: ○ CONSIDER ALL CAV PARAMETERS ○ MANUALLY DEFINE CAV PARAMETERS CRITICALITY PARAMETERS: ☑ ALL CRITICALITY PARAMETERS ☑ no Alternative routes ☑ AADT ☑ HGV ☑ Special transport OBJECT ATTRACTIVENESS: ☐ ALL ATTRACTIVENESS PARAMETERS ☐ Symbolic value ☐ Secondary effects DAMAGE POTENTIAL: ☐ ALL DAMAGE POTENTIAL PARAMETERS ☐ Explosions - Small ☐ Explosions - Medium ☑ Explosions - Major ☑ Explosions - BLEVE ☐ Fire - Arson of T2 and T20 ☐ Fire - Sufficient size of object ☑ Fire - Major in tunnels ☐ Mech. Impact - Ramming ☐ Mech. Impact - Projectiles ☐ Criminal Activities - Sabotage ☐ Criminal Activities - Cyber FEASIBILITY OF ATTACK: ☐ ALL FEASIBILITY OF ATTACK PARAMETERS ☑ Object-specific knowledge ☐ Knowledge of technology ☑ Acquisition of mat. in suffic. quantity ☑ Access/transport of mat. to crit. c. ☑ Trigger event Elea iC ☑ Show Selected Data Submit Close	The measure selection software supports the user in identifying appropriate measures for the specific object based on the defined priorities. In the software tool, the measure selection process is started and the following options are checked: » Network measures on network level » General measures and tunnel type T10 specific measures on object level » Measures for all criticality parameters » Measures for specific damage potential parameters » Measures for specic feasibility of attack parameters After submitting the query, the software tool lists a set of 21 recommended measures. For each measure a fact sheet containing detailed information is available in the annex. Based on this list, the user can decide which measures can be implemented for the individual object in this specific case.

PART 4: List of Measures

NETWORK LEVEL MEASURES:

N.01 Network, section traffic redundancy

Network redundancy is a measure with very wide range of applicability. It means that in the case of some object closure on the network section, the possibility of transport is provided with parallel transportation networks in the vicinity. Three types of redundancy can be proposed:

- Redundancy provided by a parallel road network on a similar level,
- Redundancy provided by a parallel road network on a lower (higher) level,
- Redundancy provided by a parallel network with other transportation methods in order to provide a minimal required level of transport capacity.

It should be emphasized, that network redundancy should be provided for a limited time period with predefined logistics, equipment, infrastructure, plan for the case of closure etc.

N.02 Protection of sensitive information related to network importance

Secondary undesirable effects of the unexpected closure of the road section can be extensive. It is most undesirable to reveal these effects to unauthorised people or to the general public. Therefore, a strategy for protection of this data must be prepared. High connectivity between different authorities and services is crucial.

In general, information on the object attractiveness, particularly on the symbolic value is known to the public. Secondary effects are less known for many networks even for infrastructure owners and authorities. If the public has the information on secondary effects, this can cause a major increase of the attractiveness of the network. Information on secondary effects information can be:

- Economic impact
- Societal damage
- Etc.

N.03 Education, training and exercises for the cases of the attack (network level)

Education, training and exercises on network level are important measures which can be implemented for many groups:

- Infrastructure users: The main task is to guide the users out of the affected zone and to assure the undisturbed work of the emergency services.
- Endangered elements (secondary effect potential etc.), if they are identified: Each secondary effect has its own characteristics. Thus, education, training and exercises need to be planned accordingly. Contingency plans addressing different incidents can be very efficient.
- Education, training and exercises addressing control centre personnel and emergency services.
- Education, training and exercises addressing operators and owners.

It is important to notice, that these measures can have negative effects because public become aware of the critical points of the object/structure/network.

N.04 Contingency plan for the case of the attack

After the assessment of security risk, the user should be able to predict or decide:

» which of the threats can be mitigated

» which of the potential consequences are relevant and should be mitigated

Both questions address the critical object/section/network characteristics. Therefore, the measures should be targeted accordingly. This should guide the organisation of the intervention and the responsibilities for the emergency actions. If the analysis of the detected threats and already organised forces shows insufficient efficiency, two steps can follow:

» additional forces can be mobilised, trained, educated and included in the intervention team

» existent forces can be equipped, educated and trained

In this way, the infrastructure operator will not be surprised if one of for the assessed threats materialises. Moreover, automatic systems should respond properly in various cases like multiple attacks, confusing information, lack of information, unpredicted events etc.

N.05 Police and security services control of the section/network

If identified as critical, entire networks or sections are controlled by police, security services etc. This can be implemented by means of patrols, helicopter surveillance, presence etc. at or near to the vital locations.

GENERAL OBJECT LEVEL MEASURES

GO.01 Control centre surveillance for the attacks and suspicious activities detection

Control centre personnel have the necessary information on the risk exposure of the object (according to the assigned responsibilities). The personnel know how to act in case of different possible attack incidents. In order to control these events as well as to detect suspicious activities, the following techniques can be used for security issues:

» CCTV for security purposes;

» Movement detectors for security purposes;

» Automatic video detection for security purposes;

» Dangerous goods detection by RFID for security purposes;

» Gas detection for security purposes.

By that, safety purposes of these techniques are extended to the scope of object/network security. It must be pointed out, that measures should be targeted according to the assessed security risks. Therefore existing equipment and procedures must be analysed and readjusted for the security purposes to:

» critical events detection and/or

» critical events prevention and/or

» critical events control

Therefore, each object/section/network needs its own surveillance system in order to cover the assessed risks as well as its own response plan in the form of contingency plan or similar.

GO.02 Education, training and exercises for the cases of the attack (object level)

Education, training and exercises on object level are important measures which can be implemented for many groups:

- Infrastructure users: Despite of self-rescuing being the users' main interest, they lack awareness of the actual situation and risk potential in the case of an incident. The main task with respect to the users is to guide them out of the affected zone and to assure the undisturbed work of emergency services.
- Education, training and exercises addressing control centre personnel and emergency services
- Education, training and exercises addressing operators and owners.

It is important to notice, that this measure can have negative effects because the public may become aware of the critical points of the object/structure/network.

GO.03 Access and approach prevention (signs, fences, doors, barriers)

This is the main measure to reduce the feasibility of the attack. Many different types of measures can be designed in order to meet different assessed risks:

- Signs and preventions
- Fences and doors
- Barriers etc.

These measures can address persons, personal cars, lorries, heavy vehicles etc.

Designing these measures in a way that arouses attention can have negative effects (highly guarded elements can be very attractive to attack). In order to prevent this effect, architectural measures can be necessary.

GO.04 Contingency plan for man-made attacks (object level)

Immediately after the detection of the attack or of any suspicious activities all responsible services and organisations must be informed of the event. Necessary data must be sent according to the contingency and emergency plans. At the moment, these action plans are already established as a part of the safety organisation. It is important to emphasise that attacks are a specific problem which combine many different services, organisations, effected groups with specific object properties (vulnerability). Therefore, alarm systems must consider and include all of them according to their responsibilities.

GO.05 Architectural measures

The following architectural design techniques can be implemented:

- Safety area in order to assure visibility
- Safety fences and obstacles in order to maintain visibility
- Proper lighting
- Wide profiles of underpasses, opened spaces in front of the infrastructure
- Architecturally smooth shapes of the objects, facades, no potential hiding places, corners etc.
- Combining many objects into one closed and architecturally clear unit
- No shapes where object can be placed, e.g. shelves or windows gratings
- Covering Objects entirely or partly by earth
- Elements to hide the operation and events in critical areas like the control centre

It is very important to implement these measures according to the assessment of security risk. An important role of architectural measures is also to mitigate the attractiveness. Very protected objects are attractive!

GO.06 Protection of object documentation and vulnerability information

The assessment of security risk provides information which must not be shared with unauthorised people or the general public. Therefore, a set of rules must be established, defining how to deal with this information and who is authorized to access it.

In addition, all related data, instructions and plans for the case of an attack must follow the same restrictions.

GO.07 Intelligence services and antiterrorist activities

This measure can greatly affect the feasibility of attack parameters. Each country has its own legal system and organisation regarding this topic; therefore, this measure must be considered with great care and proper coordination between responsible authorities and services.

GO.08 Police and security services control of the object

If identified as critical, the element/object is controlled by police, security services etc. according to the security plan. This can be implemented by means of patrols, helicopter observations, presence etc. at or near to the vital locations.

MEASURES FOR BRIDGES

B.01 Traffic redundancy for the bridge

This measure is effective in terms of increasing the usability of a bridge after an event with large damage potential. It is relevant for the design phase of a new object. Global redundancy means that at least half of the bridge (in one direction) is available for traffic after minor maintenance works following an event. This can be achieved by two approaches:

- By establishing separated superstructures with a longitudinal joint. In this way, it is possible to repair or replace the damaged part of the superstructure while traffic continues on the undamaged part of the superstructure.
- Second, by establishing separate substructures (superstructures on separate pillars). This way, it is possible to not only repair or replace a damage superstructure, but also the damaged pillars, while the undamaged part (separated substructure with superstructure) is still under traffic.

In cases where object redundancy cannot be achieved, network level redundancy is proposed for critical, attractive or vulnerable objects.

B.02 Parking under the bridge prevention

This measure can reduce the possibility of placing explosive or flammable materials under the bridge. In this way, it is possible to reduce the feasibility of the attack in the first place but also the damage potential of relevant threats.

B.03 Preventing of waste material disposal or material storage under the bridge

Flammable or explosive disposed material under or near a bridge can be a great threat for bridges with relatively low abutments. By preventing the disposal of different materials under the bridge, it is possible to reduce the feasibility of the attack in the first place but also the damage potential of relevant threats.

B.04 Explosion barriers

Regarding bridges, the effects of major explosions can be mitigated or eliminated by means of explosion barriers (e.g. embankments).

B.05 Increase of clearance profile and/or safety height

If the clearance profile and/or the safety height is sufficient (high abutments), the effects of explosions and heavy fires can be mitigated or eliminated. Careful analysis is needed in order to show that the height of the abutment of the respective object is sufficient with respect to the relevant threats.

BT.01 Improved design

This measure is relevant for the design phase for new objects. It mainly considers the static system of the bridges. Statically undetermined systems allow load redistribution in case of failure of a certain number of sections. Thus, statically undetermined structures are more resistant to local damage caused by fire, explosion or collision.

BT.02 Micro-reinforced / ductile high performance concrete (construction material)

The measure is effective in scenarios with mechanical impacts and explosions and is primarily used for building protection. If a relevant threat is identified, crucially slim elements should be avoided or protected according to impact design values.

In the case of explosions or impacts, the shape of the supports (columns) should be circular; square cross sections are not as efficient in cases where the load acts along the direction of the least element resistance.

Proper diameter or dimensions for explosion or impact protection of the column should be provided.

BT.03 Micro-reinforced / ductile high performance concrete (construction material)

In case of large deformability of the object, energy is absorbed without (or with minimal) damage. This is relevant with respect to impact consequences prevention and structure protection. New bridges can be made of high strength concrete instead of normal concrete. At the same dimensions, elements exhibit higher resistance to dynamic effects such as collisions and explosions.

Supporting elements, in particular the bridge substructure can be protected with micro-reinforced concrete and/or high performance concrete against impacts from explosions.

BT.04 Bearing protection

This measure is effective in explosion scenarios and is used primarily for building protection.

Bridge bearings protection can be important measure since they can be critical structural elements of bridges. Bearings can be protected with:

- physical cover to disable the access to the bearings.
- approach prevention measures – sufficient distance between bearing end potential explosion location must be achieved.
- making the approach to the bearings difficult (bearings high above the ground level or very low (low or high abutments).

It is important to note that there is no perfect protection; therefore, surveillance and interventions by the responsible services (police etc.) are needed for very critical objects/networks.

BT.05 Design for the explosion load

Many bridge types can be very susceptible to explosions on some locations of the bridge. Even relatively small explosions can have disproportional consequences due to the reduced load caring capacity of elements or loos of the stability. This is because current design codes do not include these load cases in the design. Therefore critical sections and locations must be defined and checked according to the assessed risks. Access to the critical components may play the vital part in this assessment.

BT.06 Collision protection (collision protection walls, collision protection rails)

In order to protect the columns of the bridge against collisions the following measures can be implemented:

- Barriers consisting of rails (steel or concrete) serving to redirect the vehicle (or ship) as well as to reduce the velocity of the vehicle (or ship) and thus the impact force
- Barriers located in front of the object serving to dissipate the energy of the impact

BT.07 Collision prevention (derailing fences, median space)

To prevent the collisions in the columns of the bridge following measures can be implemented:

- Barrier with rail (steel or concrete) to redirect vehicle (or ship) and with that, changing the velocity of the vehicle;
- Sufficient median space should be provided, if there is no other collision protection.

BT.08 Parking in the vicinity of the critical columns prevention

This is an important measure in order to reduce the feasibility of an attack as well as the explosion damage potential. Many different types of measures can be designed for different critical (CAV) parameters:

- Signs and preventions
- Fences, doors
- Barriers
- Architecture
- Surveillance and intervention etc.

Designing these measures in a way that arouses attention can have negative effects (highly guarded elements can be very attractive to attack). In order to prevent this effect, architectural measures can be necessary.

MEASURES FOR TUNNEL

T.01 Traffic redundancy for the tunnel

Tunnel redundancy means the availability of at least one tunnel tube after the incident. Two types of tunnels are distinct:

- Bidirectional tunnel -the redundancy can be created with a second tube. For longer bidirectional tunnels, redundancy can be achieved by additional tunnel.
- Unidirectional tunnel
- two tubes are separated enough, that the collapse of one tube does not affect the structural stability of the other tube. This is usually fulfilled if the construction method is Conventional or TBM in stable rock conditions.
- in the open design (cut and cover), the central wall between the tubes should be designed to withstand the relevant explosion and fire loading. The tunnel roof must follow the design loads criteria.

In cases where object redundancy cannot be achieved, network level redundancy is proposed for critical, attractive or vulnerable objects

T.02 DG restriction / categorisation

This measure aims to limit the Feasibility of attack. With that the threat of large fire scenarios is reduced because the transport of the substance is restricted and the event cannot be triggered.

T.03 Design for the explosion loads

The measure is effective against explosions and is used primarily as a structural protection measure. It can be implemented at the time of the design of a new tunnel.

Example: Dimensioning of cut and cover tunnel with square section for the internal pressure load of an explosion. A better robustness could be achieved by implementing a symmetrical reinforcement in the field and support areas as well as in frame corners which could cope with negative and positive bending moments. Basic characteristics of the measure are:

» Design for high internal pressures,

» Symmetric steel reinforcement of the concrete section,

» Forming of ductile frame corners for negative and positive bending moments.

» Increase the thickness and reinforcement (only locally)

» Proof of the residual cross-section capacity (failure assessment) considering all external loads.

T.04 Fixed fire fighting systems

Systems, in road tunnels, that consist of fire-fighting equipment which is permanently attached to the tunnel, consisting of a piping system with a fixed supply of water or extinguishing agent which when operated has the intended effect of reducing the heat release and fire growth rates by discharging the water of extinguishing agent directly on the fire. Examples of fixed fire fighting systems include sprinkler, deluge and mist systems.

TT.01 Fire resistant concrete

In general, concrete is not flammable, but at high heat loads, the bearing capacity of the reinforcement could be reduced if the temperature inside the tunnel cross section increases above 300°C. This process is accelerated if concrete spalling occurs. In the worst case the bearing capacity of the tunnel cross section is reduced considerably which could lead to the collapse of the tunnel ceiling. Fire resistant concrete should prevent concrete spalling and by this reduce and decelerate the heat diffusion into the tunnel cross section.

Basic characteristics of the measure are:

» addition of polypropylene (PP) fibres,

» use of carefully selected aggregates,

» maximum aggregate size is limited,

» additional mesh reinforcement to reduce spalling.

TT.02 Fire protection cladding

Classic concrete lining (existing or new) can be protected with fire protection cladding. There are different fire protection systems which could be used:

» fire proof lining/plates,

» fire protection render (spray on systems)

» other insulation material reducing the heat diffusion into the tunnel lining,

The cladding acts as a thermal insulation and reduces the heating rate and minimizes the concrete temperature – the reinforcement temperature stays below 300°C. Special care must be given to the following possible disadvantages:

» In the case of dynamical loads, pressure effects can damage the cladding;

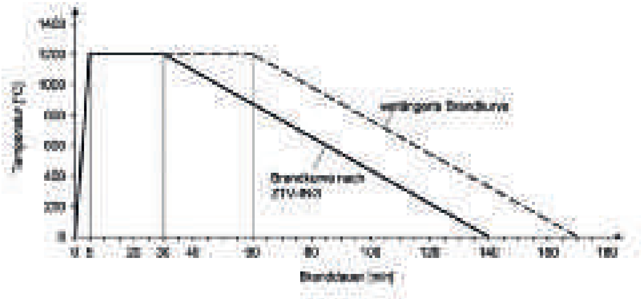
» Cleaning can damage the cladding;

» Some types of implementations are susceptible to concrete lining leaking and moisture.

» The regular inspection of the structure is hindered, e.g. leakages or cracks are hard to detect behind the cladding.

TT.03 Tunnel design for higher fire loads

The tunnel structure could be designed for a more severe fire curve. For example by extension of the fully developed fire phase by e.g. 30 minutes or by increasing the maximum fire temperature. One example which is included in German regulations is presented in the figure below:



As a result of prolonged fire curve, often an additional structural measure such as fire protection cladding or fire resistant concrete is required.

TT.04 Two shell structure

Especially in immersed tunnels or TBM tunnels below the ground water level; even small explosions can lead in heavy consequences. With a second shell additional structural redundancy is provided even if it is not necessary from the static point of view.

MEASURE FOR ACCOMPANYING INFRASTRUCTURE

A.01 Explosions, projectile protection with concrete elements

In the cases of small explosions and projectile effects in the vicinity of sensitive elements or major explosions in far distance from the sensitive elements, resistant physical protection can greatly reduce the consequences. Protection can be achieved via walls, cladding, micro-reinforced / ductile or high performance concrete etc.

A.02 Fire protection cladding

Passive fire protection which may consist of:

- plates,
- cloth,
- plaster

The measure affects only fire scenarios and is used primarily for buildings or closed compartment interior protection. It is mainly efficient against manmade arson.

A.03 Explosion barriers

Explosion barriers mitigate the consequences of heavy explosions. In many cases, this is the major threat which cannot be mitigated by other measures.

PART IV

A.04 Equipment robustness and redundancy

This is the general measure for all sensitive parts and elements. General guidance can be given, in the cases of damaging (ramming, physical braking…) the element should be:

- robust,
- redundant,
- protected.

A.05 Sabotage prevention

Prevention of the malfunctioning and damaging of the equipment and elements is the main target of this measure. Each element has its own characteristics and operation procedures, therefore each element should be considered separately.

A.06 Collision protection (collision protection walls, collision protection rails)

To protect the sensitive elements against the collisions, the following measure can be implemented:

- Barrier to dissipate the energy of the impact in front of the element.

A.07 Collision prevention (derailing fences, median space)

To prevent the collisions in the sensitive elements, the following measures can be implemented:

- Barrier with rail (steel or concrete) to redirect vehicle and with that, changing the velocity of the vehicle;
- Sufficient median space should which slows down the vehicle or makes the approach with the vehicle impossible.

A.08 Parking in the vicinity of the accompanying object prevention

Major explosions and pressure effects (also BLEVE) can have a great impact on the sensitive parts even if the distance between explosion and elements is relatively large. On the other side, even small explosions in the vicinity of the elements can have a disproportional effect on the infrastructure and its reconstruction time. Additional desirable effect of this measure is to reduce the possibility to observe the activities and infrastructure by unauthorised people.

Many different measure forms can be designed to prevent this effects:

- signs and preventions,
- fences, doors,
- barriers,
- architecture,
- surveillance and intervention…

In the design of these measures, excitation of attention must be checked and mitigated if necessary. The protection of infrastructure can have also negative effects; highly guarded elements can be very attractive for the attack. In this case additional Architectural measures can be used.

A.09 Fixed fire fighting systems

This measure is an active fire protection to prevent the development of the fire in the first phase and to also suppress already a developed fire in the compartment in the. Therefore fire detection is crucial. A currently well-established method is automatic fire suppression with gas. Also other Fixed fire fighting systems are possible but their efficiency in the case of an attack must be examined.

SECURITY MANUAL FOR EUROPEAN ROAD INFRASTRUCTURE

This manual was developed by the Consortium of the EU Project SecMan,

coordinated by the Federal Highway Research Institute (BASt) (Germany)

in cooperation with:
ILF Consulting Engineers (Austria),

ELEA iC Consulting Engineers (Slovenia) and

DARS Motorway Company (Slovenia).

SecMan was funded by the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme (CIPS) of the Directorate General Home Affairs of the European Commission.

The manual was prepared by:
Jakob Haardt (Federal Highway Research Institute)
Harald Kammerer (ILF Consulting Engineers)
The contributors to this manual are:
Miha Hafner (ELEA iC Consulting Engineers)
Drago Dolenc (DARS Motorway Company)
The manual was reviewed by:
Jürgen Krieger (Federal Highway Research Institute)
Ingo Kaundinya (Federal Highway Research Institute)
Bernhard Kohl (ILF Consulting Engineers)
Marko Žibert (ELEA iC Consulting Engineers)

The manual is also available online at: www.secman-project.eu
The manual is also available in print in German, French and Spanish.
For acquisition of a printed version of the manual, please contact:
Federal Highway Research Institute
Section B3
Brüderstraße 53
51427 Bergisch Gladbach
Germany
0049-2204-43858
secman@bast.de

Disclaimer:
Any opinions, findings, conclusions and recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of their organisations or companies. Any results indicative and the authors are not liable for damages or resulting costs from the application of the presented methodology.

Images are property of the Federal Highway Research Institute / René Legrand.

The flowchart and tables are property of the SecMan Consortium.

The consortium would like to acknowledge the EU DG Home Affairs for funding the project SecMan and supporting the implementation of the former. Furthermore, the authors would like to thank the participants of the Advisory Board, the workshops as well as the survey of the project SecMan. In particular, the valuable input of the subcontractors during the course of the project has to be noted. Additionally, credit should be given to the providers of the road infrastructure data for the validation of the methodology.