Cost-effectiveness of protection measures to mitigate terrorist attacks on bridges and tunnels

C. A. Andersen, K. C. Jørgensen & E. K. Lauritzen
NIRAS A/S, Denmark

Abstract

The SeRoN project, which is a part of the 7th EC Framework Programme, is now nearing completion. The focus of the SeRoN project is on security issues related to the European road transport network. The primary objective of the project is to investigate the impacts of possible terrorist attacks on the transport network. Resulting regional and supra-regional impacts on transport links and their economic implications are of particular concern. During the project, a risk assessment methodology to assess the cost-effectiveness of protective measures has been developed and the methodology has been applied to four infrastructure objects: A multi-span concrete box girder bridge, a three-span cable stayed bridge, a cut and cover tunnel and a NATM tunnel. For each infrastructure object, 2–4 scenarios have been chosen. Example scenarios include the detonation of 250 kg TNT in a vehicle in the middle of a tunnel, the cutting of cable stays using cutting charges or the spontaneous release of 300 l/s of flammable liquid in a tunnel. Protection measures have been conceptually designed for each scenario and a cost-benefit analysis has been carried out to determine the cost-effectiveness of each measure. The methodology can also be used to select potentially critical infrastructure objects. The methodology is furthermore generic in nature, as all types of infrastructure objects, threats and protective measures can be investigated. The method is currently being validated by investigating a further four infrastructure objects. The preliminary results show that very few protection measures are cost effective. The protection measures that might be cost-effective are generally very inexpensive and address the main risk contributors.

Keywords: terrorism, road network, bridges, tunnels, risk assessment, protective measures, cost-effectiveness.

WIT Transactions on The Built Environment, Vol 134, © 2013 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE130311

1 Introduction

The European road network is of major importance for the European economy and equally for the mobility of the European citizens and goods. Therefore, a major task of owners and operators of highways and roads in Europe is to ensure a high availability of all important links. Even smaller disruptions due to traffic restrictions or failure of some elements of the road network may lead to intense traffic interferences resulting in high economic follow-up costs and negative environmental impacts. Due to the interdependence of the road transport network with other traffic modes like rail, air and shipping traffic, a failure of important connections could have a domino effect.

Particularly bridges and tunnels are key elements of the road network. Due to their bottleneck function often based on geographical constraints, they are highly vulnerable to terrorist attacks. Besides severe accidents, e.g. involving trucks carrying dangerous goods, terrorist attacks are one of the most dangerous threats for such key infrastructure objects.

Following the EC overall strategy for protection of critical infrastructure (the EPCIP directive [1]), the SeRoN project, which is a part of the EC 7th framework programme, is addressing this issue, inter alia by developing a methodology that can be used to assess the cost-effectiveness of protection measures. SeRoN is an acronym of Security of Road Transport Networks.

This paper describes the current status and findings of the SeRoN project, particularly it describes the developed risk assessment methodology.

2 The SeRoN methodology

The SeRoN methodology distinguishes between the network level and object level (see Figure 1).

As road owners and operators often manage several infrastructure objects, the first step of the SeRoN methodology is to determine which infrastructure objects are the most important at the network level.

2.1 Ranking of infrastructure objects according to network importance

The ranking is done in two steps, first the number of infrastructure objects is narrowed down by excluding all infrastructure objects that do not meet one or more threshold values within traffic volume, amount of heavy goods vehicles, length, reconstruction time and symbolic value. The remaining infrastructure objects are then ranked according to their network importance, which is defined as the monetised benefit which arises from a prevented non-availability of a certain infrastructure object.

The monetised benefit of prevented non-availability of each infrastructure object is calculated by means of transport modelling by examining the effects of increased mileage and travel times. The examination includes fatalities and injuries from traffic accidents, greenhouse gas emissions, effects on regional economy from increased travel times, reconstruction costs and a number of other indicators. In total 20 different indicators are examined by Dahl *et al*. [2]. To perform these network calculations, a software tool was developed.

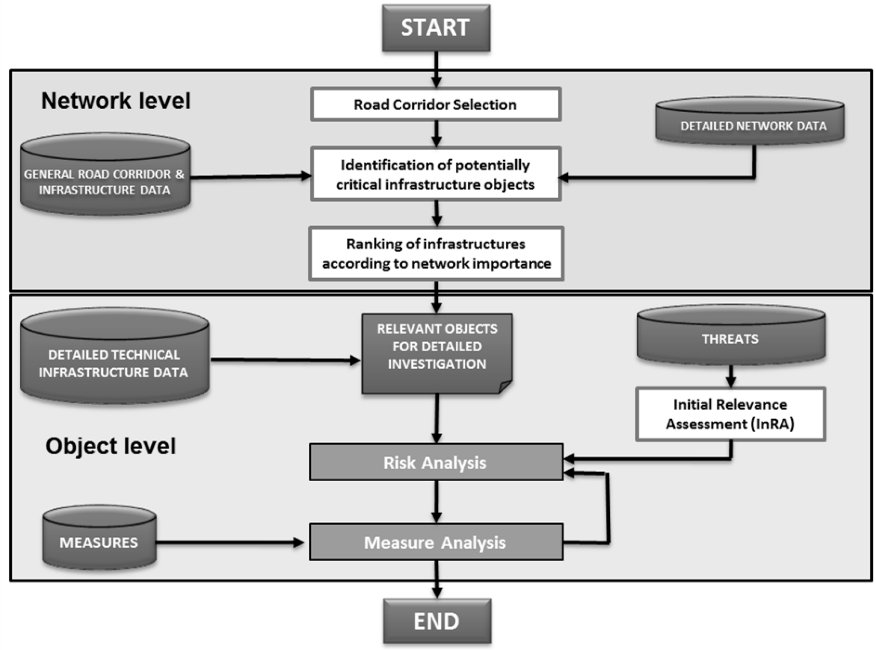
START
Network level
Road Corridor Selection
DETAILED NETWORK DATA
GENERAL ROAD CORRIDOR & INFRASTRUCTURE DATA
Identification of potentially critical infrastructure objects
Ranking of infrastructures according to network importance
DETAILED TECHNICAL INFRASTRUCTURE DATA
RELEVANT OBJECTS FOR DETAILED INVESTIGATION
THREATS
Initial Relevance Assessment (InRA)
Object level
Risk Analysis
MEASURES
Measure Analysis
END

Figure 1: Flowchart of the SeRoN methodology.

3 SeRoN risk assessment methodology

In general, the risk associated with a particular event is characterised as a combination of the consequences of the event and the frequency at which the event occurs according to ISO/IEC31010:2009 [3]. However, as the probability of a terrorist attack is not determinable, the general risk assessment approach cannot be used. Therefore a modified approach is used by Lauritzen *et al*. [4], where instead of calculating the absolute risk and comparing it to a threshold value, the cost and risk reduction of a protection measure is used to calculate the break-even frequency. The break-even frequency is the frequency at which an incident must take place for the protection measure to be cost-effective.

The developed risk assessment methodology consists of the following elements

- Selection of scenarios
- Risk assessment without protection measures
    - Probability analysis, Bow-tie analysis
    - Consequence assessment
    - Calculation of conditional risk

- Protection measures
    - Identification of protection measures
    - Conceptual design of protection measures
- Risk assessment with protection measures
    - Update bow-tie analysis
    - Update consequence assessment
    - Recalculation of conditional risk
- Cost-benefit analysis of protection measures
    - Assessment of break-even frequency
    - Subjective evaluation of break-even frequency
    - Protection measure to be implemented: yes/no?

3.1 Selection of scenarios

Holthausen *et al*. [5] analyses a number of possible threats and assesses their relevance to different types of infrastructure objects. The examined threats are various types of explosions, fire, mechanical impact, contamination, cyber-attack and menacing. It was found that attacks using explosives on bridges and tunnels, along with attacks with fire on tunnels are the most relevant.

3.2 Risk assessment without protection measures

The SeRoN risk assessment methodology is based on a bow-tie analysis approach for determining conditional probabilities, engineering assessments for determining direct consequences and transport modelling for determining indirect consequences.

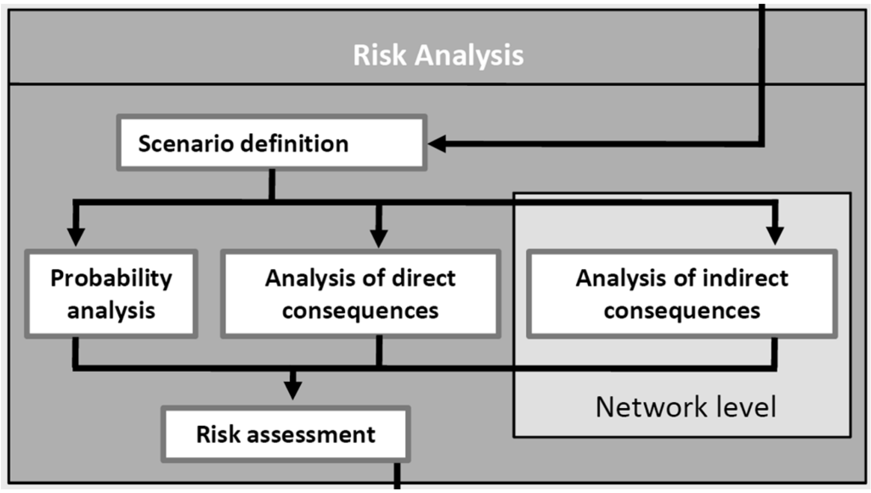

Figure 2: Principle of risk assessment in the SeRoN project.

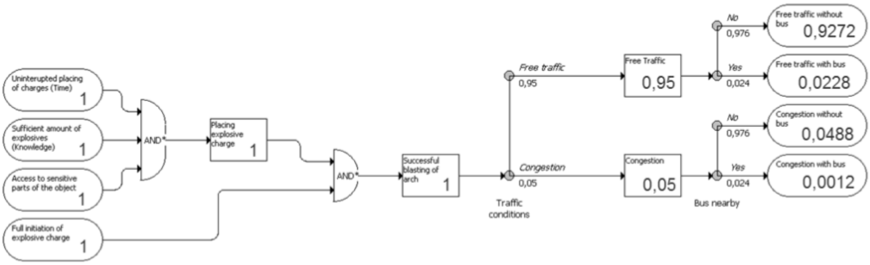

Figure 3: Example bow-tie diagram

3.2.1 Probability analysis

To determine probability, the bow-tie approach [3] is utilised. A bow-tie diagram consists of a left-hand side describing the events leading up to the critical event and a right-hand side describing possible outcomes of the critical event. An example bow-tie diagram can be seen in Figure 3.

The left-hand side is generic in nature and can, with minor modifications, be used for all types of attacks. The branching points on the right-hand side are selected to reflect the effects of the attack on the infrastructure object in question and the desired level of detail.

Because the absolute probability of a terrorist attack is very difficult to determine, conditional probabilities, assuming the probability of the prerequisites on the left-hand side are 1.0, are calculated instead. The probabilities of the branching points on the right-hand side in Figure 3 are determined either statistically, from engineering calculations or expert judgement [4].

3.2.2 Consequence assessment

When the bow-tie analysis has been done, and the conditional probability of each branch is known, the consequences in terms of costs for each branch should be determined. For instance, if the bow-tie diagram has a branching point of traffic conditions, the end state at some end branches will be congestion and free traffic at other end branches. These different states will lead to different consequences, should the event take place. The consequences can be divided into direct and indirect consequences. The direct consequences are the consequences that follow immediately from the event and are further broken down into

- Fatalities
- Reconstruction costs
- Damage to vehicles and nearby buildings

Other direct consequences can be included as needed.

The threat is simulated to the desired level of detail using either engineering assessments, numerical simulation or experience etc., and the consequences are monetised.

The indirect consequences are the additional socio-economic costs which are caused by non-availability of the analysed infrastructure object. This includes aspects like increased travel times, mileage and accidents. The indirect costs are calculated using the method described in section 2.1.

3.2.3 Calculation of conditional risk

After the bow-tie analysis has determined the conditional probability of each branch and the consequence assessment has determined the associated monetised consequences for each branch, the total risk can be calculated. The risk contribution of each branch is calculated as the probability at the end of the branch multiplied by the sum of all the monetised consequences of the particular branch. The overall method for calculating risk is shown in Figure 4. The unit of risk will be €.

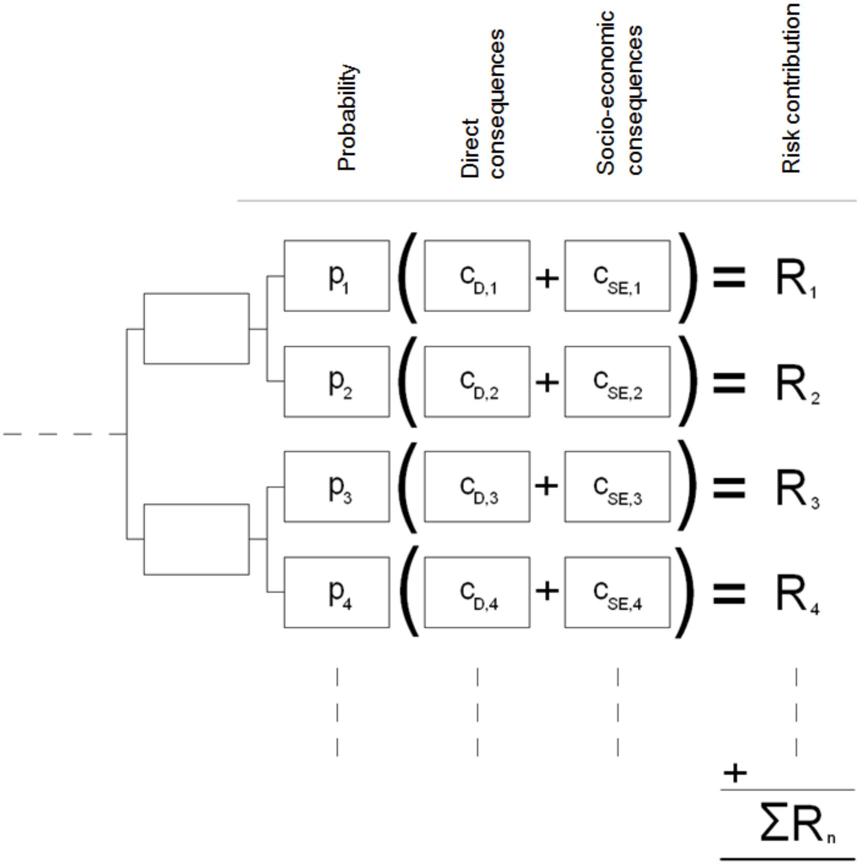
Probability
Direct consequences
Socio-economic consequences
Risk contribution
p_1 $\left(c_{D,1} + c_{SE,1} \right) = R_1$
p_2 $\left(c_{D,2} + c_{SE,2} \right) = R_2$
p_3 $\left(c_{D,3} + c_{SE,3} \right) = R_3$
p_4 $\left(c_{D,4} + c_{SE,4} \right) = R_4$
+
ΣR_n

Figure 4: Principle of calculating total conditional risk.

3.3 Protection measures

In SeRoN Deliverable D200 [6] suitable protection measures for infrastructure objects have been defined and listed. Depending on the approach protection measures can be described either by their types or their effects. They stand in opposition to a multiple number of possible threats and have to counteract with them. Therefore, the description of the measures is broken down into:

- Measures taking effect preventively (pre-incident)
- Measures taking effect while an incident is taking place (incident)
- Measures taking effect after the incident (post-incident)

Measures can furthermore be said to be structural, operational or organisational.

The conceptual design of a protection measures also includes the expected cost of the measure in terms of both investment operating and maintenance costs as well as the expected service life of the protection measure.

3.4 Risk assessment with protection measures

The overall method for conducting the risk assessment including the effects of protection measures is exactly the same as without protection measures. Depending on how the protection measure takes effect, the protection measure is implemented in the risk assessment. Often the protection measure is implemented in the bow-tie diagram. However, it can also influence the consequences alone. In Figure 5, ways of implementing the protection measure in the bow-tie diagram are depicted. The protection measure can have effect on both the bow-tie analysis and the consequence assessment, hence the bow-tie analysis, consequence assessments and resulting total risk is re-evaluated.

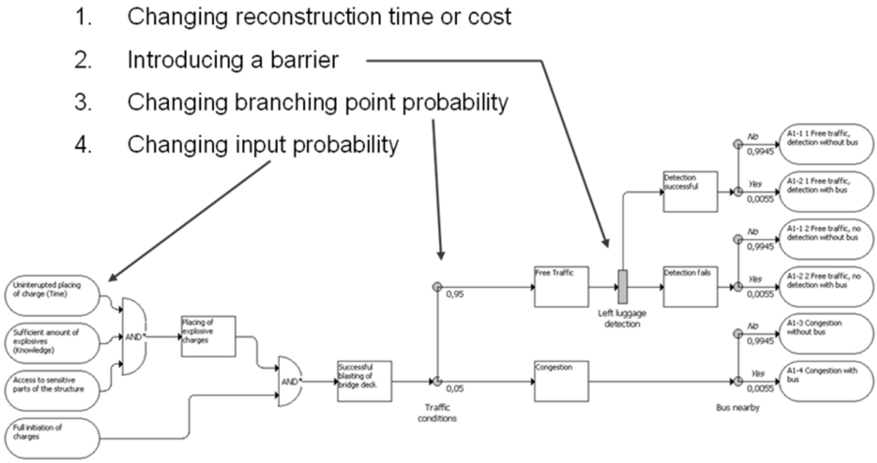
1. Changing reconstruction time or cost
2. Introducing a barrier
3. Changing branching point probability
4. Changing input probability
Uninterupted placing of charge (Time)
Sufficient amount of explosives (Knowledge)
Access to sensitive parts of the structure
Full initiation of charges
AND*
Placing of explosive charges
AND*
Successful blasting of bridge deck
0,95
0,05
Traffic conditions
Free Traffic
Congestion
Left luggage detection
Detection successful
Detection fails
No
0,9945
Yes
0,0055
Bus nearby
A1-1 1 Free traffic, detection without bus
A1-2 1 Free traffic, detection with bus
A1-1 2 Free traffic, no detection without bus
A1-2 2 Free traffic, no detection with bus
A1-3 Congestion without bus
A1-4 Congestion with bus

Figure 5: Possible ways of implementing protection measures

3.5 Cost-benefit analysis of protection measures

Because the frequency of a terrorist attack is not determinable, a general cost-benefit ratio cannot be calculated. Therefore, the break-even frequency of a particular measure is calculated instead. The break-even frequency is the frequency at which an attack of that particular type must occur for that particular protection measure to be cost-effective. The break-even frequency of a protection measures is assessed based on the risk reductive effect of the measure:

$$F_{BE} = \frac{C_y}{R_{without\ protection\ measures} - R_{with\ protection\ measures}} \qquad (1)$$

where F_{BE} is the break-even frequency [year^{-1}], C_y is the annual cost of the protection measure [€/year] and R is the total conditional risk with and without protection measures respectively [€]. The break-even frequency will help the decision maker in deciding whether or not the protection measure should be implemented. If the break-even frequency is below a plausible frequency, then the measure should be implemented. Otherwise, the measure is not cost-effective. Historic events can be used to assess whether the break-even frequency is above a plausible frequency.

4 Application of methodology to case-study infrastructure objects

During the development of the method, it was applied to four European infrastructure objects. For each infrastructure object 2-4 scenarios were selected and appropriate protection measures were investigated. The chosen infrastructure objects, see Table 1, are anonymised for security reasons.

Table 1: Investigated infrastructure object types and scenarios.

Infrastructure object	Type	Number of explosion scenarios	Number of fire scenarios
Object A	Multi-span concrete box girder bridge	2	0
Object B	Three span cable stayed bridge	1	3
Object C	300 m cut and cover tunnel	1	2
Object D	900 m NATM tunnel	1	2

A full description of the infrastructure objects and scenarios can be found in [4].

The main results of applying the SeRoN methodology on the test infrastructure objects are presented in Table 2.

Table 2: Summary of the results after applying the SeRoN methodology for risk assessment to four case-study infrastructure objects.

Object/ Scenario	Protection measure	Total risk [1e6 €]	Break-even frequency [events/year]	Protection measure cost-effective?
Object A Charge on deck	None	19,2	-	-
	Left luggage detection and communication gantries	17,3	2,4·10-3	No
Object A Charge on pillar	None	24,5	-	-
	Physical barrier	2,5	3,2·10-4	No
Object B Explosive charges on cable stays	None	959,7	-	-
	Pedestrian detection	115,2	1,8·10-5	Maybe
	Physical barrier	143,9	5,6·10-6	Maybe
Object B 300 l/s fire on rail deck, mid-span	None	1.023	-	-
Object B 300 l/s fire on rail deck, near pylon	None	2.141	-	-
Object B 300 l/s fire on road deck, near pylon	None	2,7	-	-
Object C 250 kg explosion	None	111,4	-	-
	Landscaping on top of tunnel	74,9	1,4·10-3	No
Object C 20 L/s gasoline fire in tunnel	None	149,6	-	-
	Fast detection of the event	125,3	1,4·10-4	No
	Shorter distance between emergency exits	136,1	5,1·10-5	Maybe
	Barriers	149,6	-	No
Object C 300 L/s gasoline fire in tunnel	None	152,4	-	-
	Fast detection of the event	127,2	1,3·10-4	No
	Shorter distance between emergency exits	134,9	3,9·10-5	Maybe
	Barriers	152,4	-	-
Object D 250 kg explosion	None	134,0	-	-
	AID and communication gantries	112,2	1,1·10-3	No
Object D 20 L/s gasoline fire in tunnel	None	153,3	-	-
	Fast detection of the event	144,5	2,0·10-3	No
	Shorter distance between emergency exits	147,2	4,2·10-3	No
	Smoke extraction	148,1	3,7·10-2	No
	Water mist system	153,1	-	No
Object D 300 L/s gasoline fire in tunnel	None	157,0	-	-
	Fast detection of the event	144,5	1,4·10-3	No
	Shorter distance between emergency exits	147,7	2,8·10-3	No
	Smoke extraction	156,0	0,22	No
	Water mist system	157,0	-	No

5 Validation

The SeRoN methodology is validated by its exemplary application to four different validation infrastructure objects. The infrastructure objects selected for that purpose generally differ from the infrastructure objects previously investigated with regard to their location, their properties and characteristics.

Table 3: Investigated infrastructure object types and scenarios for validation.

Infrastructure object	Type	Number of explosion scenarios	Number of fire scenarios
Object E	30 m continuous prestressed concrete beam bridge	1	0
Object F	400 m NATM tunnel with two tubes	0	2
Object G	Long immersed tunnel with three tubes	0	2
Object H	Long prestressed concrete multi-span beam bridge	2	0

One of the chosen validation objects, object E, is not critical according to the ranking process in Section 2.1, yet it is chosen to show that the methodology does not end up suggesting the implementation of costly protection measures on irrelevant infrastructure objects.

The validation process is still on-going at present, therefore not all results are available yet and those that are, are currently only available in draft form in [7]. However, the preliminary results of the validation process indicate that the SeRoN methodology is suitable and able to help decision makers allocate limited security funding.

6 Conclusions

As the SeRoN project is still on-going, the conclusions are preliminary. However, based on the results of the case study examples, the following points can be made

- The SeRoN methodology can be used to assess which infrastructure objects in a road network that are the most critical to the network and furthermore to assess whether a given protection measure will be cost-effective to implement.
- The methodology can advantageously be applied to planned infrastructure objects during the design phase.

- Very few protection measures prove cost-effective. Given the relatively low probability of a terrorist attack against a random infrastructure object, the cost of protection measures must be very low or the infrastructure object must be very important to the road network for the protection measure to be implemented.
- If a single protection measure can prevent/mitigate more threats or have other benefits, e.g. in relation to traffic safety or traffic management, it will have a positive influence on its cost-effectiveness.
- The level of detail in the bow-tie analysis and the simulations in the consequence assessment should be comparable. Experience from the application to the case-study infrastructure objects suggest that a relatively low level of detail is sufficient.
- It can be difficult to make a clear decision whether a calculated break-even frequency is above or below a realistic frequency.
- When selecting which protection measures to investigate, it is important to consider protection measures that influence the risk indicator that has the largest contribution to the risk. For example, it is not effective to aim at reducing the amount of damage to vehicles if the risk contribution thereof is insignificant.

Further information on the SeRoN project can be found at the project website http://www.seron-project.eu/ [8].

References

[1] COM/2006/0786, *Communication from the Commission on a European Programme for Critical Infrastructure Protection (EPCIP)*, December 2006.

[2] Dahl, A. *et al.*, *Importance of the Structures for the Traffic Network*, The SeRoN Consortium, Deliverable D400, December 2011.

[3] ISO/IEC 31010:2009, *Risk Management – Risk Assessment Techniques.*

[4] Lauritzen, E. K., Andersen, C. A., Jørgensen, K. C. *et al.*, *Risk Assessment*, The SeRoN Consortium, Deliverable D500, March 2012.

[5] Holthausen, N., Zulauf, C. Ruf, D. *et al.*, *Identification of Threats to Transport Infrastructures*, The SeRoN Consortium, Deliverable D100, June 2010.

[6] Beer, G., Thöni, K., Ulbrich, J. *et al.*, *Identification and Risk Classification of Critical Infrastructures*, The SeRoN Consortium, Deliverable D200, January 2011.

[7] Mayer, G., Groβmann, S. *et al.*, *Validation*, The SeRoN Consortium, Deliverable D600, Draft version, August 2012.

[8] SeRoN, http://www.seron-project.eu/