RAIN – Risk Analysis of Infrastructure Networks in Response to Extreme Weather

Project Reference: 608166

FP7-SEC-2013-1 Impact of extreme weather on critical infrastructure

Project Duration: 1 May 2014 – 30 April 2017

Security Sensitivity Committee Deliverable Evaluation

Deliverable Reference	**D 6.1**
Deliverable Name	**Quantification of single-mode risks and impacts**
Contributing Partners	**Roughan & O'Donovan**
Date of Submission	**June 2015**

A: The suggested evaluation is:

- **The content is not related to general project management**
- **The content is not related to general outcomes as dissemination and communication**
- **The content is related to critical infrastructure vulnerability or sensitivity**
- **The content is not publicly available or commonly known**
- **The content does not add new information that might be misused; there is only a description of the methodology of D3.1 (confidential), D4.1 and D5.1 (to be evaluated) and does not include any content**
- **The content does not cause harm to the essential interests of EU or member states**
- **The content does not cause societal anxiety or social unrest**
- **There are no uncertainties that might need to contact the National Security Authority**

Diagram path: 1-2-3-4-6-7-8-9. Therefor the evaluation is: Public.

B: the alternative evaluation is:

- **The content is not related to general project management**
- **The content is not related to general outcomes as dissemination and communication**
- **The content is related to critical infrastructure vulnerability or sensitivity**
- **The content is publicly available or commonly known because it describes the existing methodologies**
- **The content does not add new information on vulnerabilities, sensitivities or incident scenario's on specific objects**
- **The content does not add new information on vulnerabilities, sensitivities or incident scenario's on assets in general**
- **There are no uncertainties that might need to contact the National Security Authority**

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608166

This project is funded by the European Union

Diagram path 1-2-3-4-5.1-5.2-9. Therefor the evaluation is Public.

Decision of Evaluation	**Public**	**~~Confidential~~**
	~~Restricted~~	

Evaluator Name	**P.L. Prak, MSSM**
Evaluator Signature	
Date of Evaluation	**2015-07-17**

RAIN – Risk Analysis of Infrastructure Networks in Response to Extreme Weather

Project Reference: 608166

FP7-SEC-2013-1 Impact of extreme weather on critical infrastructure

Project Duration: 1 May 2014 – 30 April 2017

Deliverable 6.1-Quantification of single-mode risks and impacts

Authors

Donya Hajializadeh* (Roughan & O'Donovan)
Mark Tucker (Roughan & O'Donovan)
Noel Van Erp (TU-Delft)
Pieter Van Gelder (TU-Delft)
Carlos Bárcena Martín (DRAGADOS)
Maria Luskova (UNIZIA)
Zdenek Dvorak (UNIZA)
Chiara Bianchizza (ISIG)
Olivia Ferrari (ISIG)
Milenko Halat (AIA)
Jose Luis Marin (AIA)
Brian Caulfield (TCD)
William Brazil (TCD)
Peter Prak (PSJ)
Timo Hellenberg (Hellenberg)

***Correspondence author: Arena House, Arena Road, Sandyford, Dublin 18, donya.hajializadeh@rod.ie, +35312940800**

Date: 7/07/2015

Dissemination level: (PU, PP, RE, CO): PU

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608166

This project is funded by the European Union

DOCUMENT HISTORY

Index	Date	Author(s)	Main modifications
E01	13th February 2015	DH and MT	First Draft
E02	16th June 2015	DH, MT, NVE, PVG, CBM, ML, ZD, CB, MH, JLM,BC,WB,PP,TH	Document updated for internal review
E03	29th June 2015	DH, MT, ML, ZD, KG, MD	Document revised according to internal reviewers' comments.
E04	07th July 2015	DH & MT	Final version. Document revised according to further comments from TU—Delft.

Document Name: Quantification of single-mode risks and impacts

Work Package: 6

Task: 6.1, 6.2, 6.4

Deliverable: 6.1

Deliverable scheduled date (12th Month) 30th April 2015

Responsible Partner: Roughan & O'Donovan

Table of Contents

Introduction

Extreme weather such as heavy and prolonged rainfall, floods, heavy snowfall, extreme heat or cold weather are increasing and causing extensive damage to the European Union's (EU) transportation and energy infrastructure. Previous experiences have shown that around 10% of all costs for road maintenance in the EU are devoted to repairing damage caused primarily by heavy rainfall and floods. Extreme weather events also have a strong impact on energy infrastructure, such as power grids, which when damaged, can lead to disruption to the entire generation and distribution systems. Consequently, adopting adaptive measures to increase resilience is becoming more important as the severity of extreme weather events, and their effect on society, security and the economy, increases.

The objective of work package 6 is twofold, namely a) to assess the societal, security and economic impacts of critical infrastructure (CI) failures based on single-mode and multi-mode failures and b) to identify the quantifiable benefits, from a societal security and economic standpoint, of providing resilient infrastructure.

In this report, Deliverable D6.1, single-mode risks and impacts are addressed. Multi-mode impacts and risks will be addressed in Deliverable D6.2. In addressing the issues associated with single-mode risks, this document describes the advanced risk assessment procedure developed to quantify single-mode risks and the variables required to implement this approach. In addition the methodology for computation of societal, security and economic impacts will be presented.

In Deliverable D6.3 (Month 30), the contents of Deliverable D6.1 and Deliverable D6.2 will be applied to pre-selected case studies to benchmark the methodologies developed and to provide a measurable indicator of the benefits to providing resilient infrastructure.

An Objective Ranking Tool (ORT) which will be used to assess and evaluate the criteria of the impacts of single-mode failures on the various markers is described. These criteria will be evaluated for their respective contribution to the failure and will be classified in order of importance.

The current report begins with a summary of probabilistic risk assessment techniques and an overview of the risk assessment framework developed in WP5. Subsequently the critical infrastructures introduced in WP3 and WP4 are reviewed and the resulting societal, security and economic risks of CI failure are listed and a measurable indicator for each is introduced. In the last section ORT and its application in the RAIN project is summarised.

1. Probabilistic Risk Assessment

Based on the United Nations Office for Disaster Risk Reduction (UN-ISDR) definition, risk is the probability of harmful consequences, or expected losses from death, injuries, property, livelihoods, economic activity disrupted security or environment damaged resulting from interactions between (natural, human-induced or man-made) hazards and vulnerable conditions (Van Westen et. Al 2011). In short, risk is the probability of losses.

Based on this definition of risk, Risk Assessment is a methodology to determine the nature and extent of risk by analyzing potential hazards and evaluating existing conditions of vulnerability that could pose a potential threat or harm to people, livelihoods and the environment on which they depend. Risk assessment encompasses the identification, quantification, risk analysis (qualitative, semi-quantitative, and quantitative) and evaluation of risks associated with a given system. Overall, the risk assessment aims to support rational decision-making regarding risk-bearing activities (Apostolakis, 2004).

In the risk assessment procedure, three questions need to be answered: 1. what can go wrong? 2. How likely is that to happen? and 3. what are the consequences if it does happen? The first question will form a set of scenarios called the “risk scenarios”. The likelihood then refers to the likelihood of each risk scenario individually and collectively. The end states of the scenarios are the consequences such as injury or loss of life, reconstruction costs, loss of economic activity, environmental losses, etc.

WP5 of RAIN project has developed a risk assessment framework, Figure 1, in which these three questions are addressed within a Bayesian Network approach to quantify both single-mode and ultimately multi-mode risks and the impacts of extreme weather events on interconnected critical infrastructure systems.

In summary, the framework starts with *establishing the context.* The system being analyzed is defined in terms of its elements and what constitutes normal operation to serve as a baseline reference point. In the next step, *the risks are identified.* The source of hazard will be identified and characterised and then the scenarios of risk are established and consequences and vulnerability elements will be defined. *Mitigation measures* will subsequently be introduced for each vulnerable element of interest. At the *risk inference* stage (for which further detail is provided in Figure 2), the likelihood of the different scenarios and their attendant levels of damage will be estimated considering the level of mitigation actions and the scenarios according to damage level will be assembled and results will be presented into the appropriate risk curves and priorities. In the final step*, risk evaluation* (for which further detail is provided in Figure 3)*,* the results will be evaluated and interpreted to guide the risk manager or infrastructure owner on strategies to be adopted to reduce risk to an acceptable level. There are many intermediate steps in the five step process when assessing extreme weather risks but the principles are fundamental and in line with the three questions posed for implementing a general risk assessment framework. Detailed description of each step is given in Deliverable D5.1 (Van Gelder & Van Erp 2015) of the RAIN project.

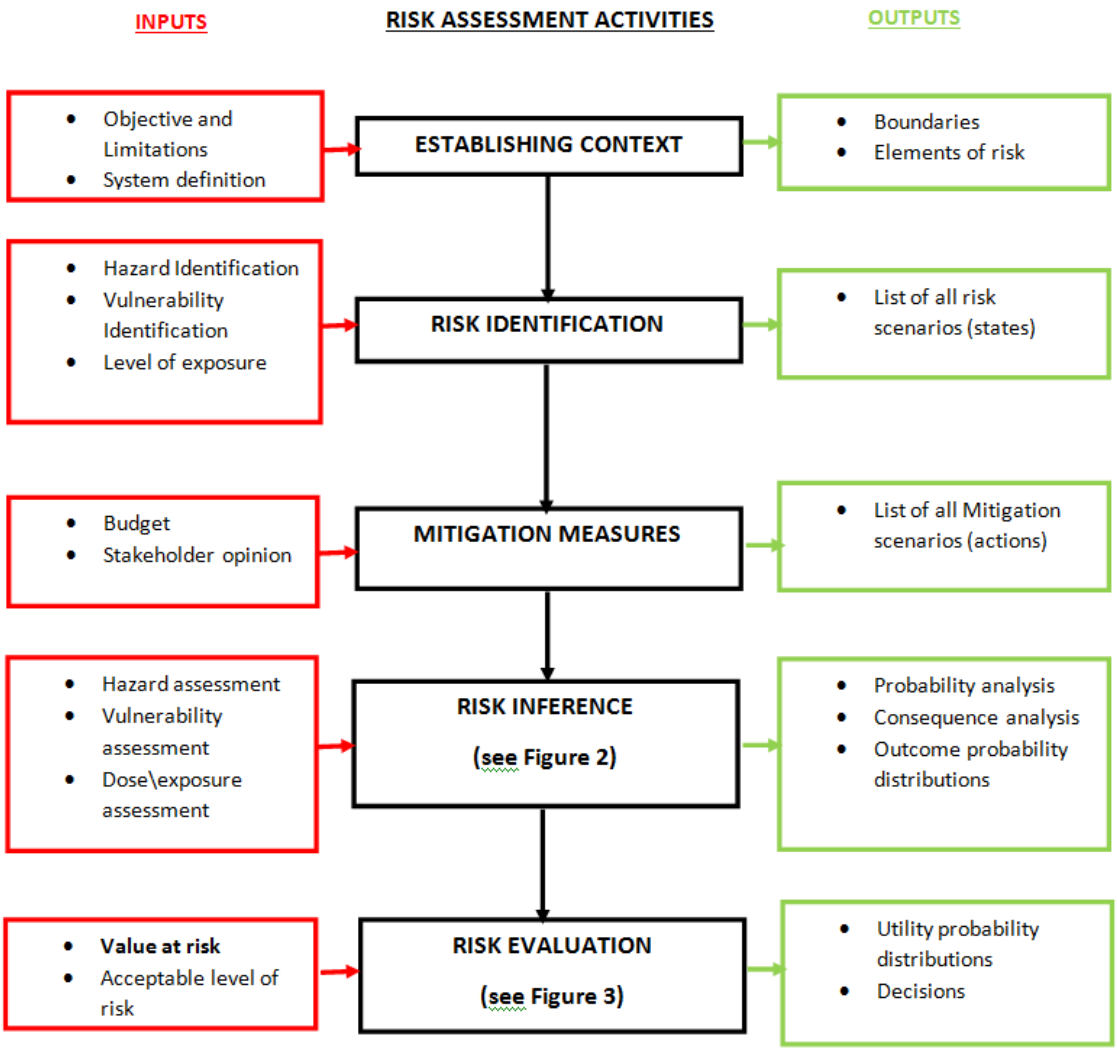


Figure 1- Bayesian Risk Analysis Framework

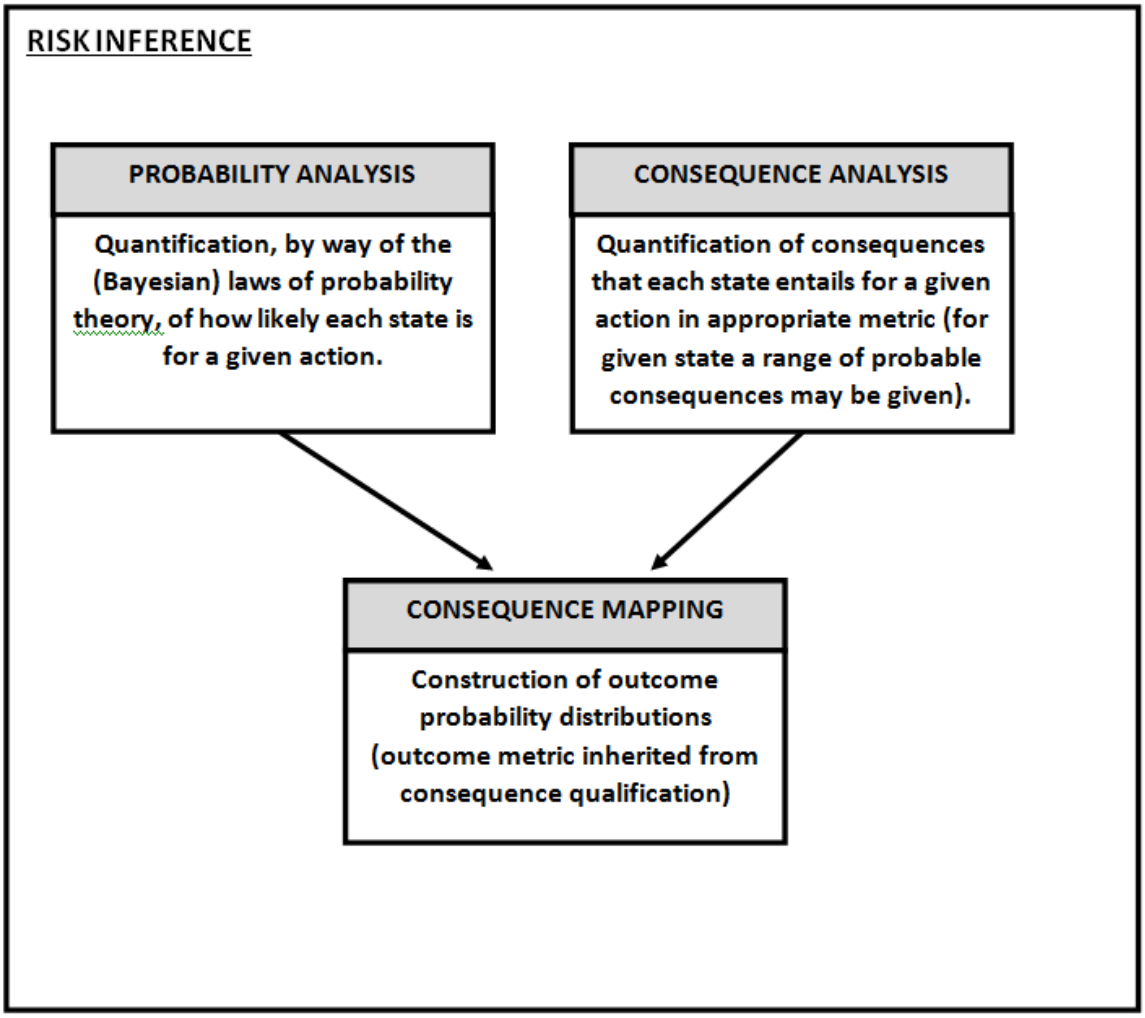


Figure 2-Detail of the risk inference framework

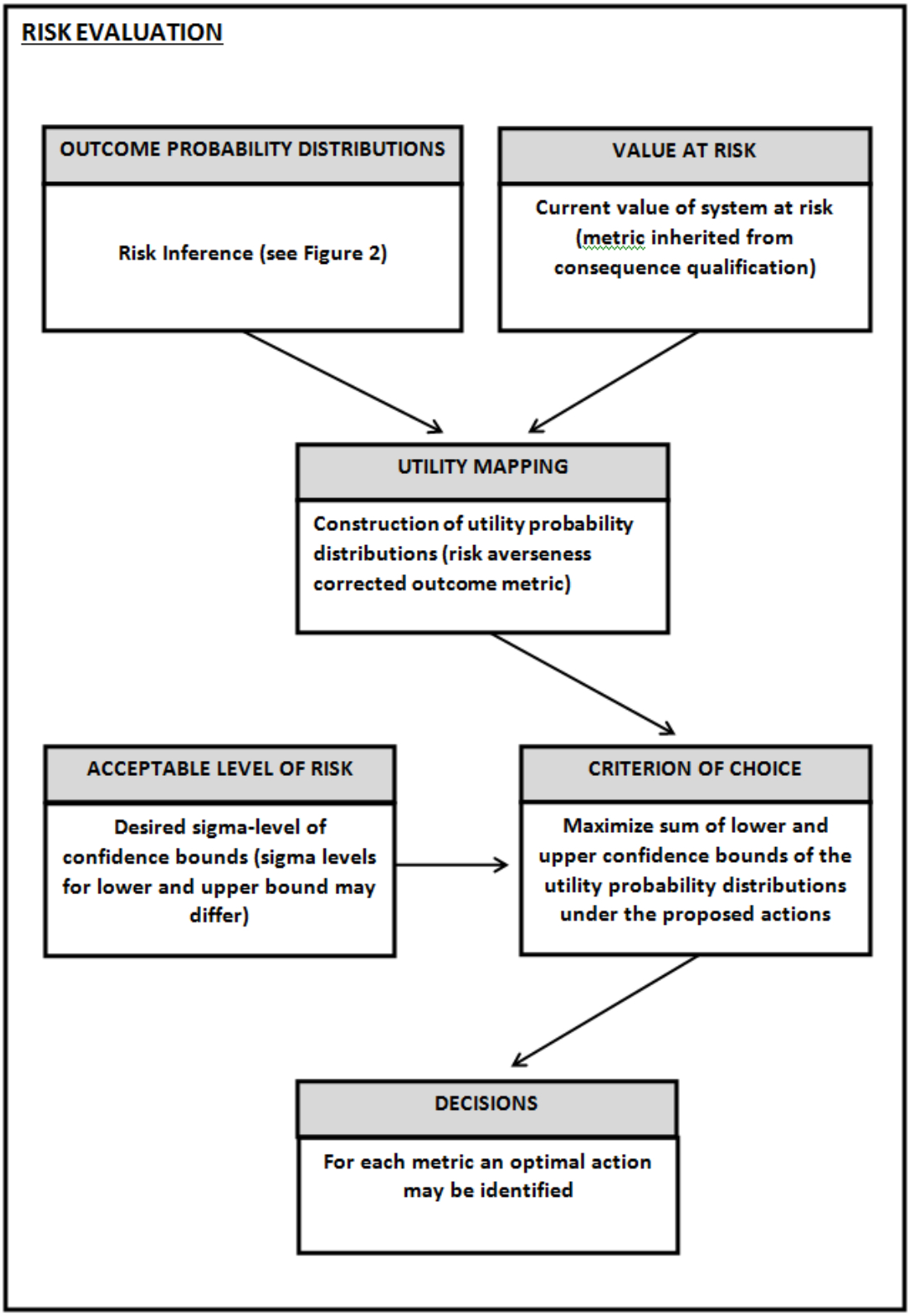


Figure 3- Detail of the risk evaluation framework

The current study aims to provide a measurable indicator of societal, security and economic risks due to critical infrastructure failures using Probabilistic Risk Assessment (PRA) techniques, for which there are four accepted calculation methods:

- Event Tree Analysis (ETA)
- Fault Tree Analysis (FTA)
- Risk Matrix
- Bayesian Network (BN)
- Inference network and Bayesian Probability Theory

Fault and event trees are two of the basic tools in system risk assessment. ***Event trees*** use 'forward logic'. They begin with a triggering event and 'propagate' this event through the system under study by considering all possible ways in which it can affect the behaviour of the (sub) system. The nodes of an event tree represent the possible functioning or malfunctioning of a (sub) system. If a sufficient set of such systems functions normally then the system will return to normal operating conditions. A path through an event tree resulting in a risk is called a risk scenario.

An example of schematic event tree developed for a system of one hazard and two subsystems is shown in Figure 4. The results of the Event Tree are generally presented in the form of outcome event frequencies (probabilities) per year.

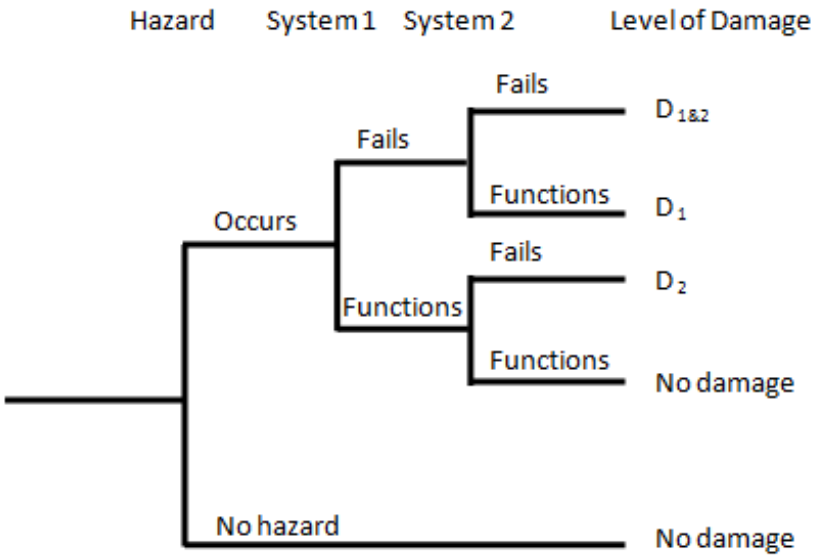


Figure 4- An example of Event Tree

A ***fault tree*** works with 'backward logic'. Given a particular failure of a system, the top event, one seeks the component failures which contribute to the system failure. Fault trees can result in the probability of the top event by ascribing probabilities to each basic event, Figure 5.

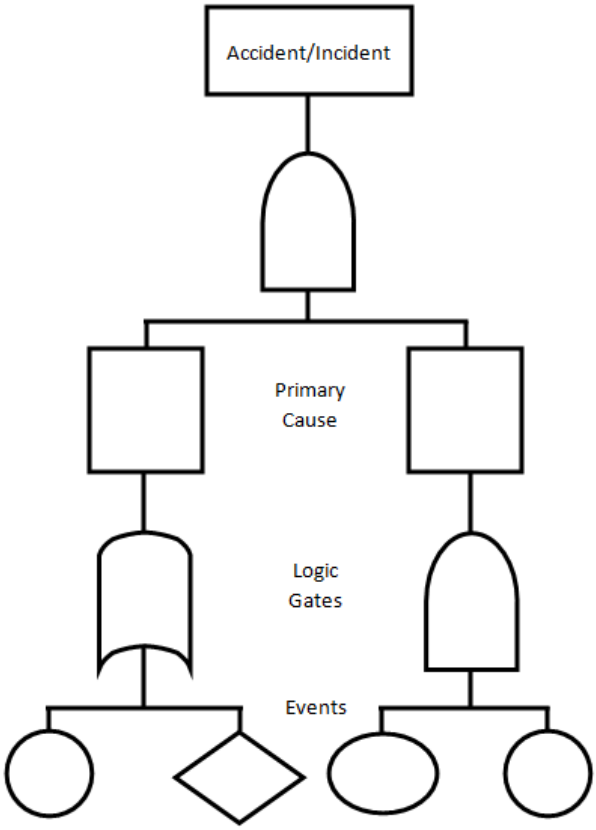


Figure 5- An example of Fault Tree

The third method of undertaking a probabilistic risk assessment is using a **Risk Matrix** (Figure 6). The arrangement of accident/incident probability and corresponding consequence in a Risk Matrix can be a suitable expression of risk in cases where many accidental events are involved or where single value calculation is difficult.

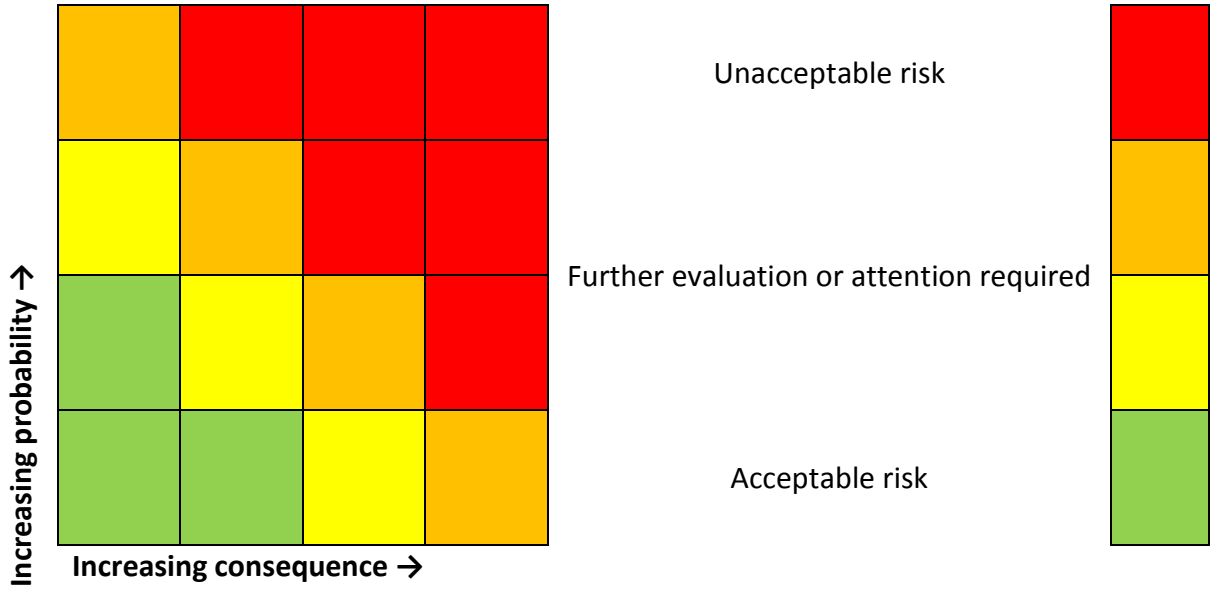


Figure 6- An example of Risk Matrix

One of the main drawbacks of these three methods is that they will rapidly grow to large sizes, even for systems with a few elements. In addition, event trees and fault trees do not provide insight into functional relationships between system components. Therefore an alternative representation that is often used is ***Bayesian Networks*** (equivalent terms are Bayesian Belief Networks or belief network). A Bayesian Network (BN) is a probabilistic graphical model that represents a set of random variables and their conditional dependencies via a directed acyclic graph (DAG) or arrow. Nodes represent random variables and arrows represent conditional dependencies. As part of the Bayesian network the conditional probability of a failure event, given a set of conditions and/or failure of another system can be included to come to an overall risk estimate.

WP5 of RAIN project has developed a risk assessment framework using inference network and Bayesian probability theory which is the inference instrument of choice. In Bayesian probability theory chains of inference are connected by the product and sum rule. This method is capable of evaluating large-scale inference problems which is considered to be the most suitable method for risk assessment framework developed in WP5.

Figure 7 illustrates the inference network developed in WP5 by Van Gelder & Erp (2015), according to the RAIN project objectives. The developed inference network starts with triggering events of hazardous events such as heavy precipitation which may result in fluvial/pluvial/coastal flooding or landslides. Each hazardous event results in critical infrastructure failure and consequently will lead to societal, security and economic risks. Since an output of WP6 is to assess the effect of providing resilient infrastructure on economic, societal and security risk, a 'Mitigation strategies' node is also added to the inference network. For each node of the inference framework, three levels of low, medium and high are considered (shown by red, yellow and green respectively). In the probability and consequence analysis (Risk Inference step in the framework, Figure 1) each level and node is assigned with a magnitude and probability which can be varied in order to carry out a sensitivity analysis.

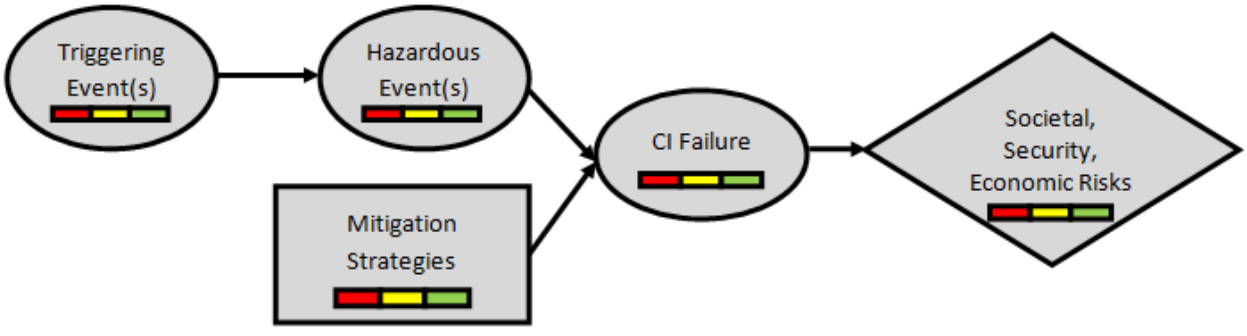


Figure 7-Generic Bayesian network framework developed for RAIN risk assessment framework

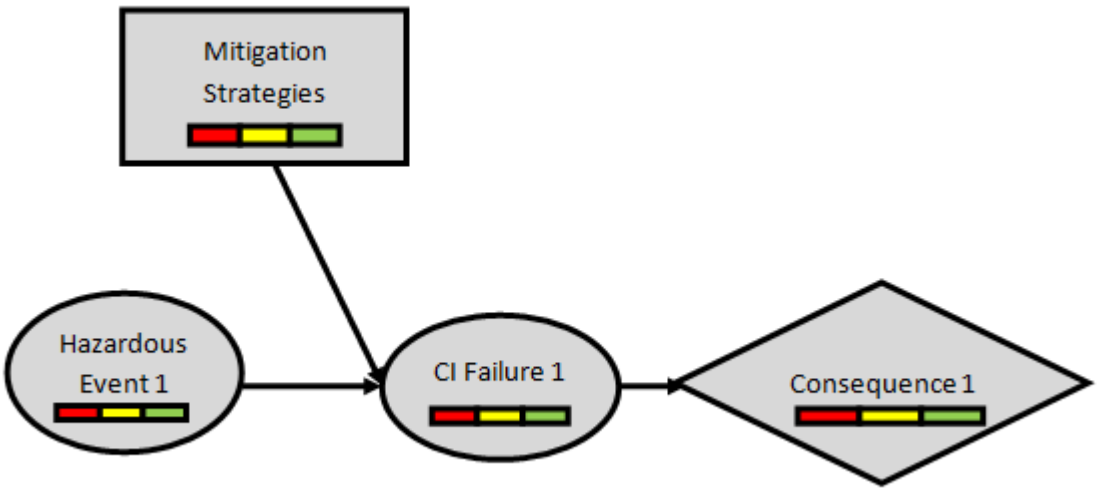
1.1. Single-mode Risks vs. Multi-mode Risks

The multi-risk concept refers to various combinations of hazards and various combinations of vulnerabilities so it requires a review of existing concepts of risk, hazard, exposure and vulnerability,

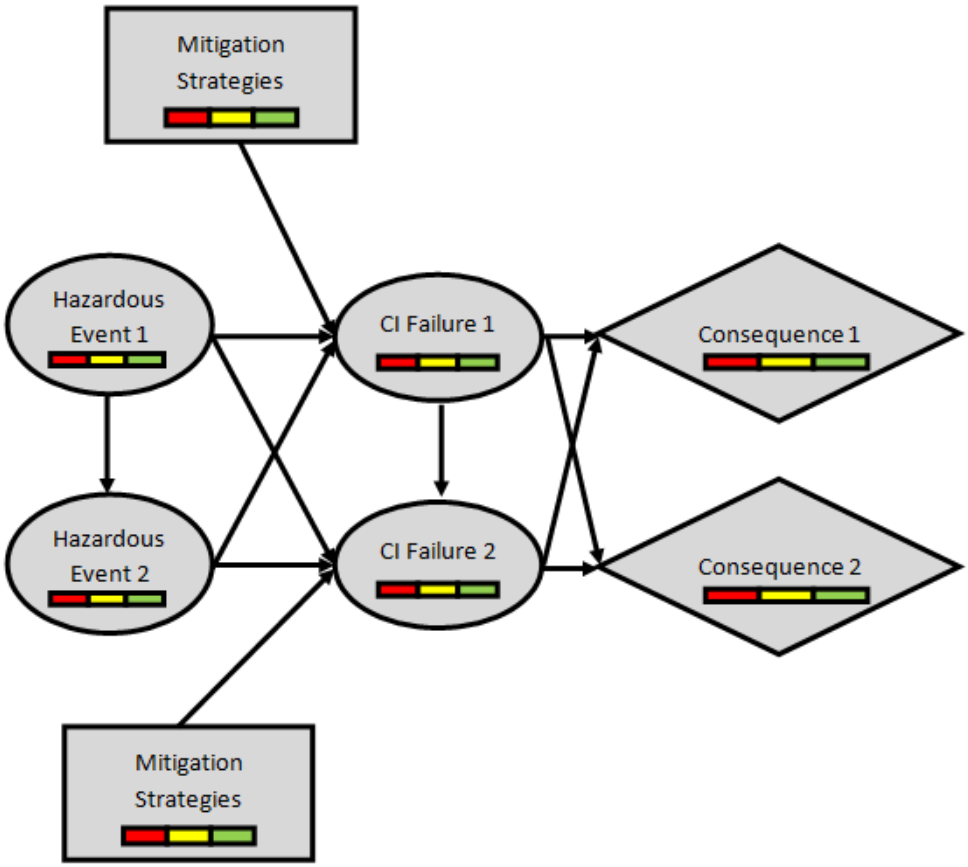
within a multi-risk perspective. Therefore a multi-risk approach requires a multi-hazard and a multi-vulnerability perspective.

According to D5.1 of the MATRIX project (Garcia-Aristizabal& Marzocchi, 2011) the multi-hazard concept may refer to (a) the fact that different sources of hazard might threaten the same exposed elements (with or without temporal coincidence), or (b) one hazardous event can trigger other hazardous events (cascade effects). On the other hand, the multi-vulnerability perspective may refer to (a) a variety of exposed sensitive targets (e.g. population, infrastructure, cultural heritage, etc.) with possible different vulnerability degree against the various hazards, or (b) time-dependent vulnerabilities, in which the vulnerability of a specific class of exposed elements may change with time as a consequence of different factors (e.g., the occurrence of other hazardous events, etc.).

In contrast, the single risk assessment is a risk of particular hazard occurring in a particular geographical area during a given period of time. Hence the single risk assessment ignores the interdependency between hazardous events. In this assessment it is also assumed that there is no connection between infrastructure failures. The difference between a single-risk and multi-risk assessment for a system of two hazardous events and two critical infrastructures is shown in Figure 8. Figure 8(a) illustrates an example of single mode risk scenario of one critical infrastructure failure due to one hazardous event. Figure 8(b) shows a Multi risk scenario, in which there is a possibility of more than one hazardous event with correlation between them and also multi CI failure with possibility of interdependency between failures. Since D6.1 is focused on single-risk assessment the methodology described from hereafter is only applicable for single-risk assessment. Figure 9 illustrates two examples of possible single-risk scenarios. As illustrated, the single-risk scenarios in this study can include multi-infrastructure failure events. Figure 9(a) shows an example of single infrastructure failure due to a hazardous event while Figure 9(b) shows a single-mode risk scenario in which multi-infrastructure failure events occurred due to one hazardous event. It has to be noted that in the case of multi-infrastructure case the failure of CIs is limited to one category (i.e., Railway, Road, Energy or Telecommunication).

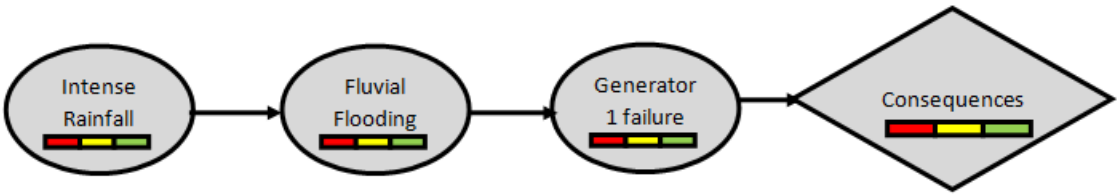


(a)

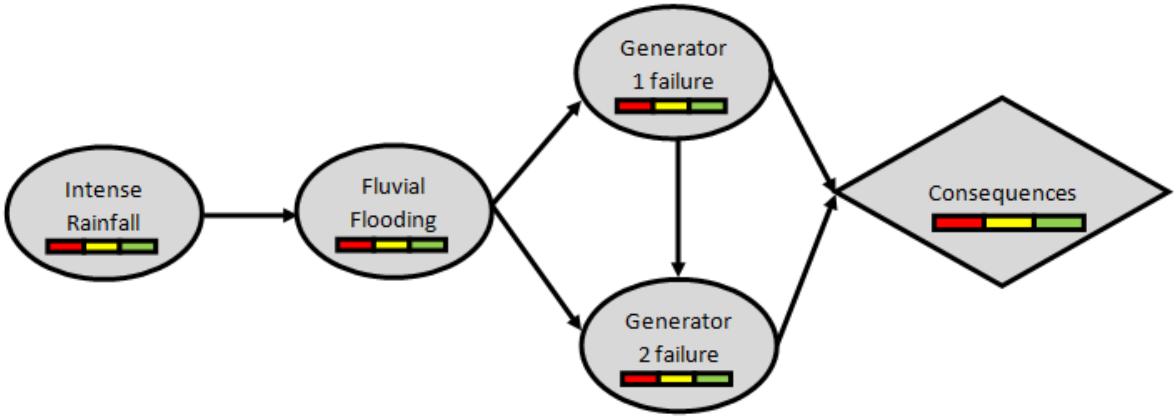


(b)

Figure 8- Single-risk and Multi-risk example for a system of two hazardous events and two critical infrastructures



(a)



(b)

Figure 9- Single-risk scenario examples

2. Critical Infrastructures

A methodology has been developed in WP3 and WP4 to identify critical infrastructure for land, energy and telecommunication networks. The proposed methodology is summarised in the following sections. Further information can be found in RAIN deliverables D3.1 (Dvorak & Luskova, 2015) and D4.1 (Marin & Halat, 2015).

2.1. Critical Land Transport Infrastructure

Due to the absence of a complex model to identify and then assess the criticality of particular elements of transport infrastructure, a general methodology, Figure 10, for identification of potential critical infrastructure elements in transport was developed within WP3 by Dvorak & Luskova, in 2015. This methodology is based on the existing Slovak (Act No. 45, 2011) and European legislation (Council Directive 2008/114/EC) regulating critical infrastructure protection. Within this methodology, the potential critical infrastructure elements are analyzed to determine whether they have a unique/irreplaceable position in the transport network. Based upon an assessment of the elements by the sector and cross-cutting criteria, it is possible to determine which objects are the potential critical infrastructure elements

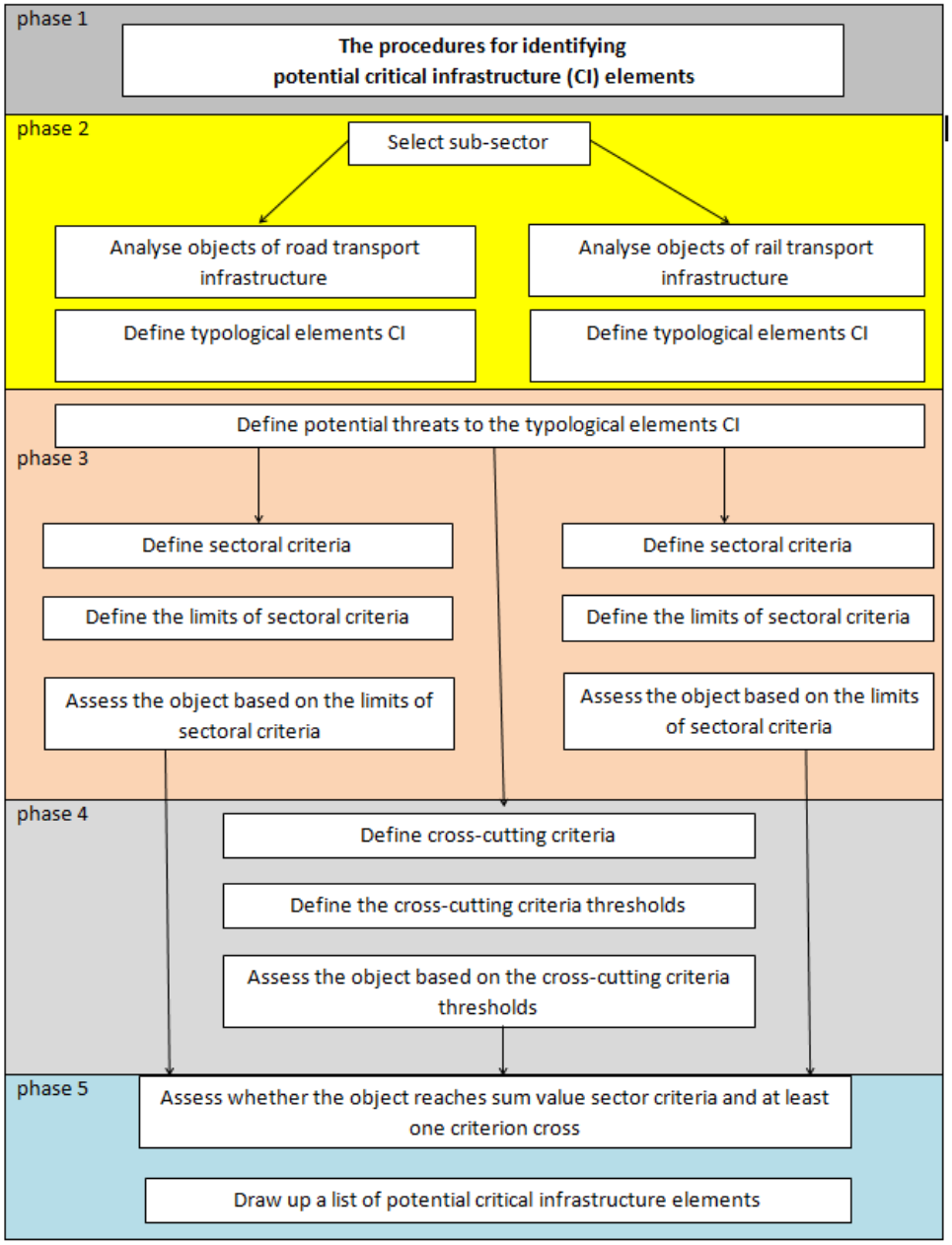


Figure 10- The procedures for identifying potential critical infrastructure elements

Each transport system is made of specific elements which enable the operation of the network. In RAIN, individual typological elements of the road infrastructure were identified as follows. A definition of each element is provided in deliverable 3.1 of RAIN project (Dvorak & Luskova, 2015).

- Roads;
- Intersections;
- Stations of public transport;
- Bridges;
- Tunnels;
- Intersection control systems;

- Systems of variable traffic signs.

In a similar manner as for road infrastructure, it is possible to establish hierarchy structure of typological elements for rail infrastructure. In RAIN, individual typological element of rail infrastructure was identified as follows. For more detail please refer to deliverable 3.1 of RAIN project (Dvorak & Luskova, 2015).

- Railway tracks;
- Railway stations;
- Railway bridges;
- Railway tunnels;
- Terminals of intermodal transport;
- ETCS (European Train Control System);
- Electronic signal boxes;
- Train control;
- Remote operation management;
- Security systems of railway crossings.

Based on the application of the methodology outlined in Figure 10, the elements of road and rail transport infrastructure identified as critical were as follows; terminals of intermodal transport (rail), motorway junctions (road), bus (road) and railway stations (rail), bridges and tunnels (road and railway).

2.2. Critical Energy Infrastructure

The Energy network brings electricity from power plants (nuclear, thermal, hydro, wind, etc.) to consumers, over large distances with remarkably small losses. Figure 11 shows a schematic view of the entire power grid infrastructure, from generation (e.g from power stations), transmission lines (transmission grid), distribution lines (distribution grid) and to the final customers (commonly referred to as *loads)*. Transmission-level voltages are generally considered those above 110 kV. Voltages between 110 kV and 33 kV are typically considered sub-transmission voltages, but are occasionally used for transmission systems with light loads. Voltages of less than 33 kV are representative of distribution. The so-called *substations* are the nodes of the network, where several lines join and where voltage transformation takes place. The transmission section of the grid is ‘mesh’ or ‘graph’ like for redundancy, while the distribution section is more ‘tree’ like. Most countries, mainly due to the cost of building redundancy, build their transmission power grids according to the N-1 security principle which does limit the resilience of the system.

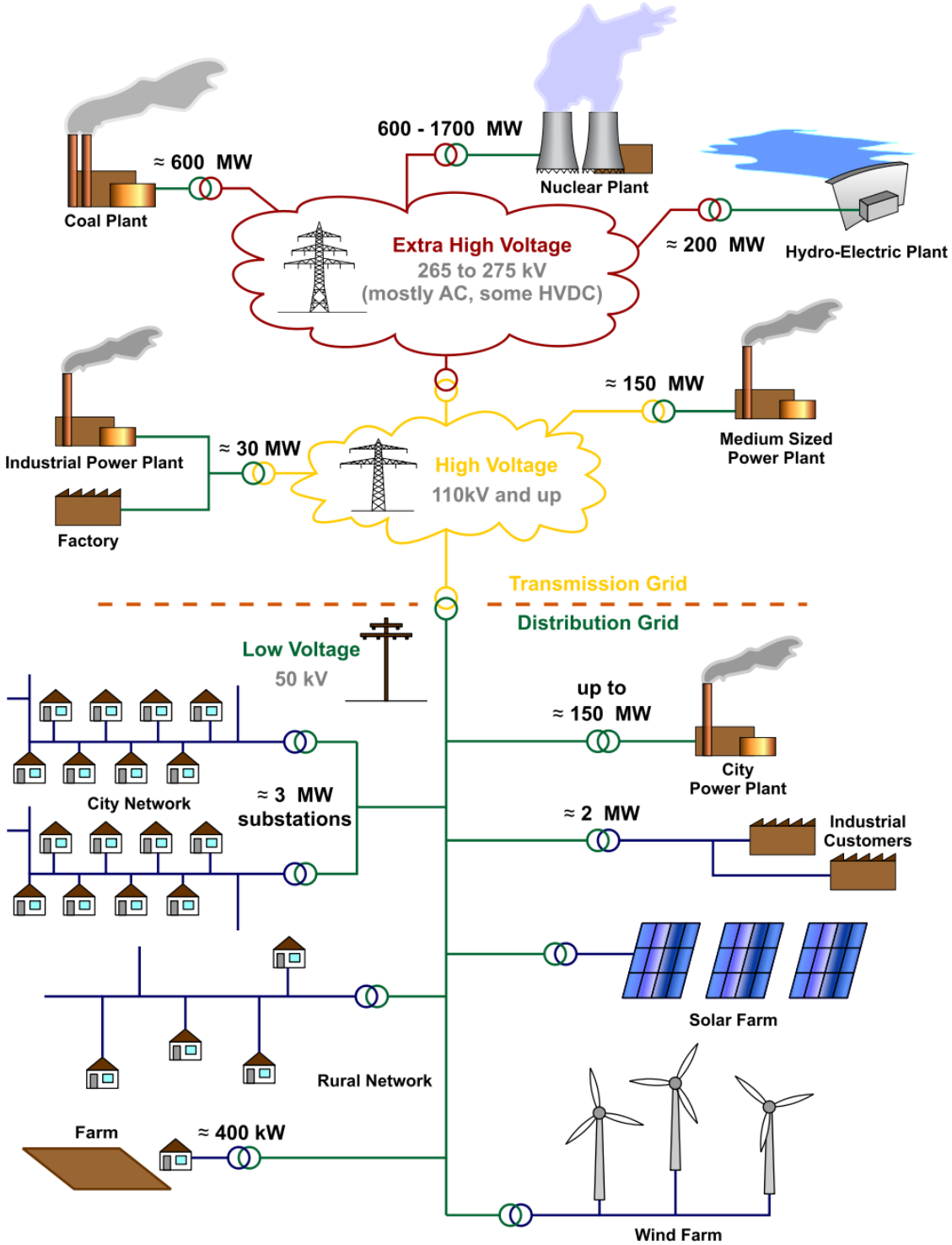


Figure 11- Schematic view of the electric power network infrastructure (source: Wikipedia). The two "clouds" depicting transmission are really a meshed network, which gives the power grid its name.

One characteristic of power networks is that there is currently no means of storing electrical energy at the scale needed by power utilities. Consequently electricity has to be generated in sync with the real-time demand i.e. a balance has to be reached between sources and sinks. This imposes a great deal of burden on the operation of power grids, as the production has to be carefully scheduled in advance (according to forecasts of aggregate demand), and then carefully monitored and regulated to account for real-time deviations. Events that alter this delicate balance, such as the sudden loss of

a generator, or a rapid and unexpected increase in demand, may upset the operation with potentially widespread effects. In particular, local weather disasters have the potential to disrupt the entire electric system, creating problems far beyond the loss of local power supply.
The main components of the electrical power infrastructure, according to the simplified modelling assumptions described in D4.1 (Marin & Halat, 2015) are:

- Generators and their auxiliary power systems;
- Transmission lines (including HVDC links);
- Transmission transformers (including feeders to distribution);
- Switches and breakers;
- Protection relays;
- SCADA and associated Telecoms;
- Other Voltage-management devices.

Note that the developed model does not consider *loads* as a critical component of the infrastructure. A *load* is a modelling abstraction representing thousands or more customer endpoints, in other words, *aggregate demand.* Therefore it is usually just the expression of the active and reactive power draw (P, Q) at the output end of a "feeder" transformer. As such, the actual critical components sitting at the end of the infrastructure are therefore the transformers - the loads that they serve are just a measure of the amount of "service" that could get lost. As to the question of granularity in the model, it is of course necessary to decide at which level of the distribution network hierarchy one wants to stop the analysis.

2.3. Critical Telecommunication Infrastructure

Telecom networks have a structure similar to that of power grids, in that there is a transmission section for long distance, having a graph-like structure for redundancy, and a distribution section, which is more tree-like, Figure 12. However, there are very significant differences in terms of operations: telecom networks are mostly self-rate-limiting, so that there is no risk of collapse in case the demand is not met. This behaviour is even more graceful in modern networks, as most communications are now driven by packet-switching technologies and TCP/IP. Additionally, there is no need to keep a delicate balance between sources and sinks, as for power networks as in this case the users are both sources and sinks of traffic flow. And finally, the resilience of the transmission section is typically much higher in telecom networks than in power networks, as telecom networks based on IP routing can typically withstand the loss of several nodes.

While currently there is limited interdependency between energy and telecommunication networks, this situation will change due to the advent of 'Smart Cities'. As such resilience of these networks will become even more critical.

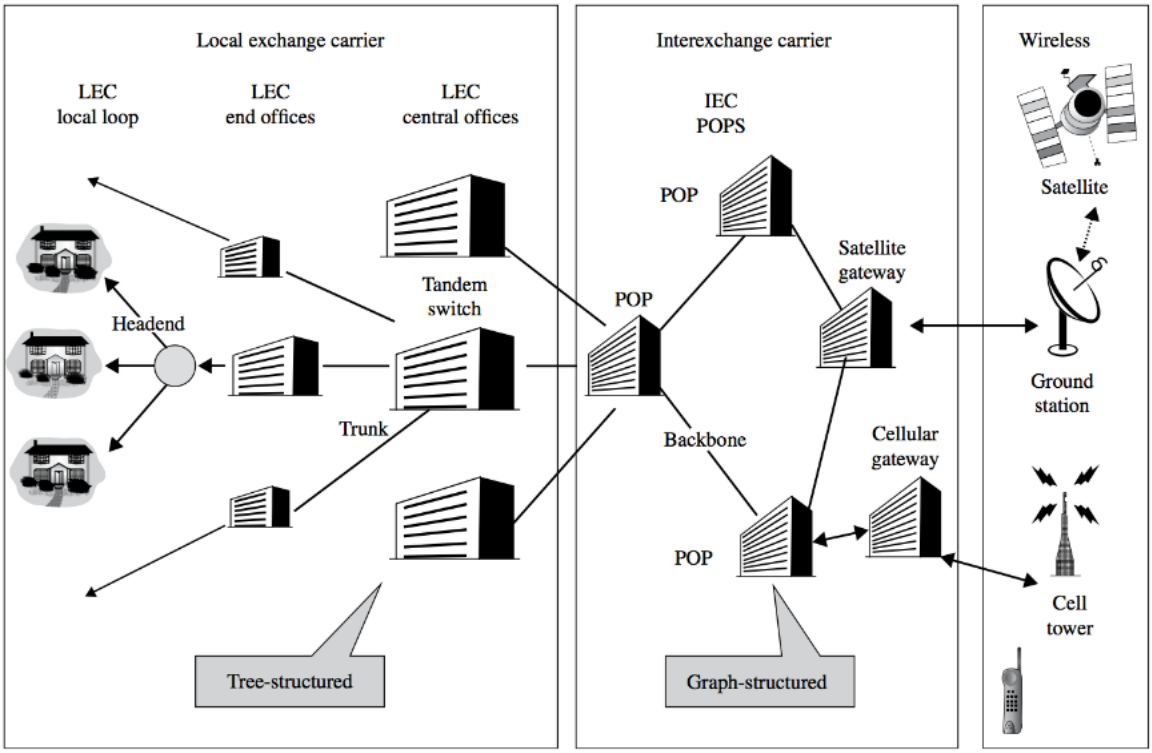


Figure 12- schematic structure of the telecom infrastructure

The critical elements of the telecom network infrastructure, according to the simplified modelling assumptions described in D4.1 on *distribution level*, operated by the Local Exchange Carriers (LEC) companies are (Marin & Halat, 2015):

- Outside Plant equipment;
- The End Offices;
- The Central Offices;
- Aerial trunk lines;
- Underground trunk lines;
- RF link trunk lines.

And at the *transmission section*, operated by Interexchange Carrier (IEC) companies are:

- Class 1, 2, and 3 centres;
- Aerial backbone lines;
- Underground and submarine backbone lines;
- RF and Satellite Backbone lines;

Additionally, we should also consider the following key elements of the *mobile network* world (we omit trunk lines, as they are the same as above):

- Base Stations (BS);
- Base Station Controllers (BSC);
- Mobile Switching Centre (MSC);

- Gateway MSC;
- Home Location Register (HLR);
- Visitor Location Register (VLR).

It has to be noted that in this framework, none of the specific router/switch component are singled out. It is assumed that they all integral part of the abstract elements “Central Office” or “Primary Centre” etc., as that is the main role that these nodes play in the networked infrastructure, i.e. switching traffic. Given the level of risk analysis needed in the RAIN project, it is assumed that it is not necessary make these fine-grained distinctions.

3. Societal Risks

3.1. Qualitative Analysis of Societal Risks

While 'society' as such is composed of a set of people and by relations and institutions that link them together and regulate their interaction, for the purpose of this study, the societal impacts are limited to civil society (i.e. citizens) only. The other aspects of society such as, economic and organizational risks (i.e., security) are explained in separate sections.

The Impacts of failure of an element of critical transportation infrastructure on society can vary greatly and depend on several factors, including: geographical position, adaptive capacity, economic conditions of the area,; and the transportation mode which fails. The impacts will also be related to the severity of the consequences - for example, a road blockage could delay traffic flow, while a bridge collapse could result in complete road closure which, for example, can lead to limited access to first aid and hence will increase the number of injuries and fatalities. Equally the disruption to an energy network can lead to power outages and the impact on society with the resulting impacts dependant on the duration of the power outages. While impacts can be assessed in general terms, no single definitive conclusion on the specific impact of weather events on infrastructure failure can be reached since too many variables have to be taken into account, such as for example severity, preparedness, personal conditions, etc. and the potential for loss in the face of a natural hazard changes across history and geography but also between different societies living in the same time and space (Cutter et. al, 2003). According to the literature, the following are the main direct societal impacts of critical infrastructure failure due to extreme weather event.

- Injury;
- Loss of life;

The failure of CI due to extreme weather events also has indirect societal impacts such as; Injury/Loss of human life as a result of increased amount of accidents, traffic jams, and undesirable effects on traffic interoperability; Psychological effects such as increased stress/depression as a result of poverty, ill health etc; one of the factors in youth migration whereby insufficient infrastructure services can limit employment opportunities, increased health risks etc. and loss of trust in community which can reduce social capital (support networks, social participation, community engagement, social cohesion).

In the long-term due to the poverty created a result of reoccurring extreme weather events and the reputation of an areas susceptibility to extreme weather events the rate of tourism will be affected.

It should be noted that the current study only considers measurable indicators of direct societal risks and the risk assessment of indirect societal impact of CI failure is considered to be beyond the scope of this work.

3.2. Quantitative Analysis of Societal Risks

Societal risk can be defined as the relationship between frequency and the number of people suffering from a specific level of harm in a given population from the realization of a specified extreme event. The societal risk quantifies cumulative risk over the whole area of interest (i.e., risk of multiple incidents in the society as a whole where society has to carry the burden of a hazard). This can be a function of individual risk which is the risk of harm to any identifiable individual who lives within the zone impacted by hazard.

In the risk assessment studies, societal risks are limited to fatalities and injuries. Fatalities risk is generally expressed by f-N or F-N curves. When the frequency of events which causes at least N fatalities is plotted against the number N on double log scales, the result is called an F-N curve. The lower an FN-curve is located on the FN-graph, the safer is the system it represents, because lower FN-curves represent lower frequencies of fatal events than higher curves. Figure 13 illustrates an example of F-N in the Netherlands showing the number of fatalities of various hazardous activities. Note that in this figure installation refers to fatalities in the nuclear industry installation.

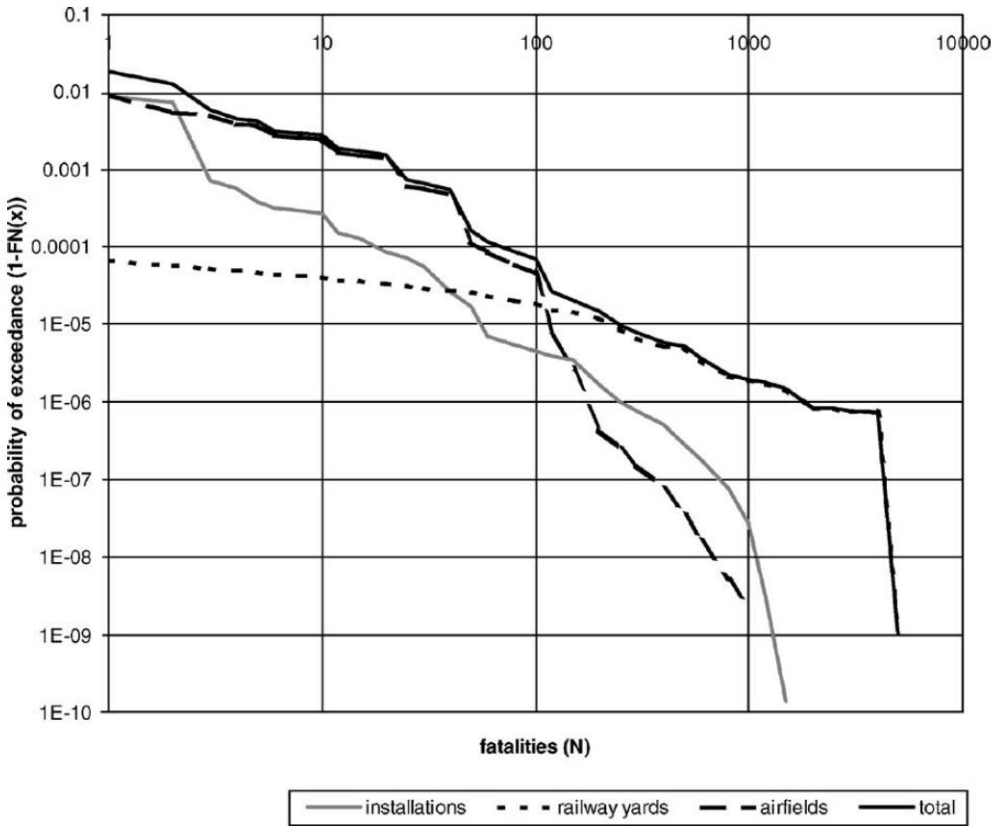


Figure 13-F-N curve for the risks of various activities in The Netherlands in 1999 (Jonkman et. al, 2003)

If the frequency scale is replaced by annual probability, then the resultant curve is called f-N curve. F-N curves can be constructed based on historical data in the form of number of events (floods, landslides, etc) and related fatalities. They can also be based on different future risk scenarios, in

which for a number of events with different magnitudes the number of casualties is estimated using the methods that will be explained in this chapter. Then the F-N curve displays the future risk.

Individual risk (IR) of an average unprotected person can be defined as the probability of certain risk due to an accident resulting from infrastructure failure. For example in the case of loss of life due to infrastructure failure, IR can be calculated as following:

$$IR = P_f P_{d|f} \quad \text{Eq. 1.}$$

where: P_f is the probability of failure, and $P_{d|f}$ probability of fatality for an individual in the case of failure, assuming the permanent unprotected presence of the individual. The aggregated weighted risk (AWR) can then be calculated by following equation:

$$AWR = \iint IR(x,y)h(x,y)dxdy \quad \text{Eq. 2.}$$

where: $IR(x,y)$ refers to individual risk at location(x,y) and $h(x,y)$ number of individuals on location (x,y) and A is the area for which the AWR is determined. By integrating the individual risk levels and the population density, the expected value of the number of for example fatalities can be determined:

$$E(N) = \iint IR(x,y)m(x,y)dxdy \quad \text{Eq. 3.}$$

where $E(N)$ is the expected value of the number of fatalities per year and $m(x,y)$ is the population density on location (x,y). Given the definition of individual risk, the F-N curve can be obtained by following equation:

$$1 - F_N(x) = P(N > x) = \int_x^\infty f_N(x)dx \quad \text{Eq. 4.}$$

where $f_N(x)$ is the probability density function of the number of fatalities per year and $F_N(x)$ is the cumulative function of the number fatalities per year. Then the expected value of the number of fatalities per year, $E(N)$, is:

$$E(N) = \int_x^\infty x f_N(x)dx \quad \text{Eq. 5.}$$

This will lead to the area under the F-N curve, that is a common measure of societal risks in the literature (Vrijling & Van Gelder, 1997, Ale et. al, 1996). The British Health and Safety (HSE) defines a risk integral (RI) as a measure of societal risk in which (Cutter, 2003):

$$RI = \int_x^\infty x\big(1 - F_N(x)\big)dx \quad \text{Eq. 6.}$$

The weighted risk integral parameter is calculated by following equation, in which α is the coefficient representing the aversion to accidents with many fatalities.

$$RI = \int_x^\infty x^\alpha f_N(x)dx \quad \text{Eq. 7.}$$

The number of people at risk (PAR) is also used as another measure of societal risk which can be expressed by following equation (Jonkman et. al, 2003):

$$PAR = \iint_A m(x,y)dxdy \quad \text{Eq. 8.}$$

F-PAR is a similar concept to the F-N curves which displays the probability of exceedance as a function of the people at risk instead of number of fatalities for the FN curve, which is capable of giving a better impression of societal disruption that the F-N curve.

The proposed methodology does not consider a standardized approach for determining *a priori* the impact of a critical infrastructure failure on society (civil society). It starts from the premise that different impacts rely heavily on the level of resilience of the system and cannot thus be standardized which leads to difficulties in obtaining a measurable indicator of risk. A resilient system reacts quickly with the result that citizens using for example, the motorway following an extreme weather event do not feel the impact of that event. On the contrary, a vulnerable system can result in a high level of distress for the users of the motorway (e.g. drivers), as it is not able to respond to the threats posed by the extreme weather event. In synthesis, a vulnerable system results in a negative and more serious impact on its users.

The probability of each societal risk (i.e., fatalities, injuries) given the failure of critical infrastructure is a function of several key factors. In order to turn an essentially qualitative self-assessment into a quantitative datum for the development of resilience of society (i.e., improvement strategies), the Institute of International Sociology of Gorizia (ISIG) (within ECOSTRESS DG ECHO project) is piloting a tool devoted to this purpose. This is to be done through a SWOT analysis (a structured planning method used to evaluate the strengths, weaknesses, opportunities and threats), in which identified theoretical indicators (Figure 14) are turned into dimensions and variables. Once described, each variable is assigned a value (ranging from “-2 extremely negative” to “+2 extremely positive”, passing also through “0 not relevant”).

The final score per Strength, Weakness, Opportunity and Threat gives an overall view of the system. Where Threats/Weaknesses dominate, the system (according to the self assessment of its managers/operators, etc.) tends to be (more) vulnerable and where Strengths/Opportunities score higher the system tends to be (more) resilient.

Starting from this analysis and in a comparative perspective it might be possible to weight the possible impacts of certain events on different systems (comparative analysis) and flexibility of that system to respond to extreme future events, impacting in different degrees on the users of the transport infrastructures (citizens). In the RAIN project we will investigate this methodology in benchmarking the case study regions.

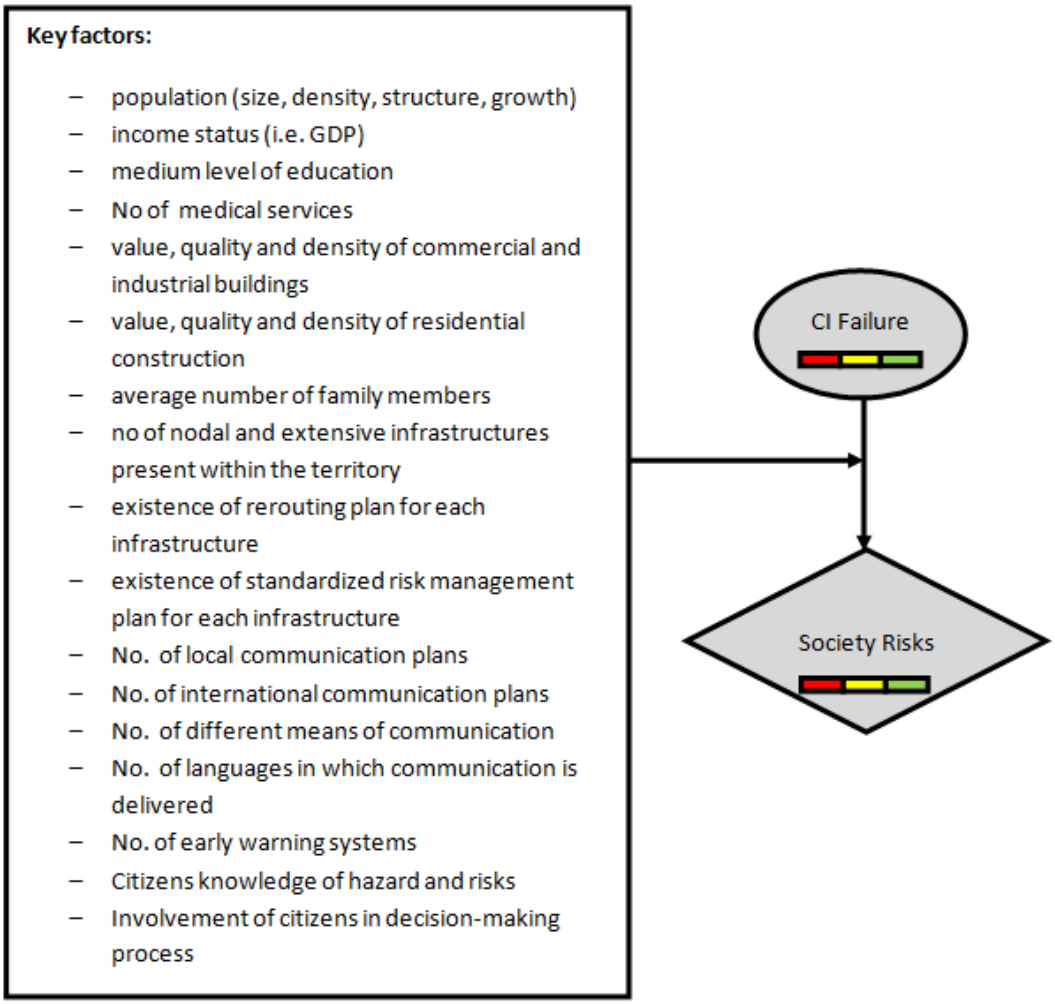


Figure 14- Key factors to be considered in societal risks

4. Economic Risks

Calculating the precise economic impact of a given failure event of even a single piece of critical transport, energy, or telecommunications infrastructure can present a very difficult task to the analyst. This section will outline some of the economic impacts worth considering and highlights some of the issues relating to their assessment.

It is also necessary to determine whether there are infrastructure interdependences that should be considered. For example, electricity needs communication system to run its operations whilst communications needs electricity to run its networks. A flood can affect infrastructure with geographical dependencies, such as water treatment, energy (sub-stations inundated) and transport (local roads and railway flooded), causing more significant consequences, as people can be without piped water supplies, without power and stranded on disrupted roads.

4.1. Qualitative Analysis of Economic Risks

Direct economic impacts arising from the failure of an element of critical infrastructure are as below. Note, not all these factors are independent or each other:

- Cost of Repair or Replacement:

  When an element of critical infrastructure fails, unless it is already redundant, it will have to be either repaired or replaced to ensure the same level of service can be provided as before the failure. While it is possible to produce estimates based upon the cost of similar projects in the region, there are a number of issues that must be considered.

- Cost of Labour:

  Depending on the magnitude of the event that caused the failure there may be issues regarding the availability of individuals with the required skills to repair or replace the element. For example if a single electricity pylon is damaged due to its proximity to a flooding river there is likely to be no issue, however if the entire network has been severely affected by a hurricane there may be a considerable supply and demand issue.

- Availability of Materials:

  Depending on the extent of the damage suffered by other elements of CI during an event there may be shortages of the required materials which results in either increased construction costs or a delay in restoring the element causing additional indirect impacts.

- Age of the Existing Infrastructure

  When estimating the economic impact of the destruction or disablement of an element of CI it is important to consider the age of the element and how soon it was going to be replaced as the value of an element depreciates over time. For example the economic impact of replacing or reconstructing a new rail section will be much greater than if the element was due to be replaced in the near future and a replacement budget already existed.

- Impact on Alternative Routes

  In the case that an element of CI fails, there may often be alternative routes onto which existing demand can be replaced. If for example a road tunnel fails, there may be an alternative road that road users may take advantage of. However, as these users switch to the alternative they may increase congestion on this route and create an economic loss for both the existing users and the economy as a whole.

Failure of critical infrastructure can also results in indirect impacts such as opportunity costs where a disruption in critical infrastructure network can have a knock-on economic effect on the wider community. For example loss of power supply to a business may mean that it may not be able to open resulting in a loss of potential revenue. Similarly the disablement of a vital road to a remote area in peak tourist season may curtail the amount of income that may be generated by the region in a vital economic period.

Similar to societal impacts, quantifying indirect economic risks are beyond scope of the current study.

4.2. Quantitative Analysis of Economic Risks

There are several ways to express economic risks due to CI failure. The Probable Maximum Losses (PML) is the largest loss believed to be possible in a defined return period, such as 1 in 100 years, or 1 in 250 years. The risk can also be represented as a curve, in which all scenarios are plotted with their return periods or probability and associated losses. Such a risk curve is also called the Loss Exceedance Curve (LEC) (Figure 15).

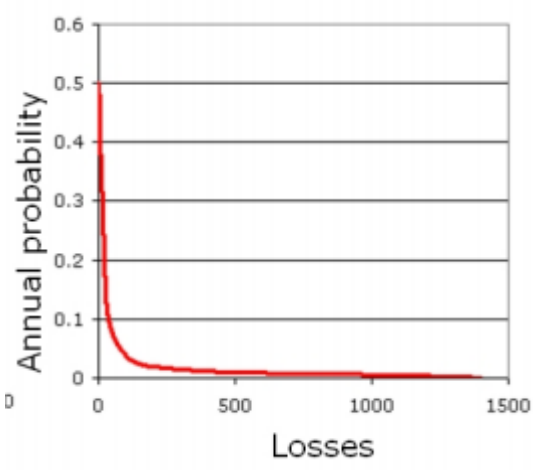


Figure 15-An example of LEC curve (Van Westen et. Al 2011)

An F-D curve is the most common measure of economic risk which displays the probability of exceedance as a function of the economic damage. The F-D curve can be obtained by following equation:

$$1 - F_D(x) = P(D > x) = \int_x^{\infty} f_D(x)dx \qquad \text{Eq. 9.}$$

where $F_D(x)$ is the probability distribution function of the economic damage. Similar to F-N curves, the area below the F-D curve equals the expected value of economic damage, $E(D)$. The total costs in a system, C_{tot}, can be defined by the sum of the expenditure for a safety system, I and the expected value of the economic damage. In the economic optimization process, the total costs ina system is minimized by the following equation which determines the optimal probability of failure of a system provided system investment and the expected economic damage as a function of probability of failure (Jonkman et. al, 2003):

$$min(C_{tot}) = min\ (I + E(D)) \quad \text{Eq. 10.}$$

$$E(D) = \int_x^{\infty} x.f_D(x)\,.dx \quad \text{Eq. 11.}$$

In order to quantify the probability of economic impacts due to infrastructure failure caused by extreme weather, the main key aspects to be assessed have been divided into three different parts: infrastructure descriptive data, infrastructure environment descriptive data and infrastructure use and exploitation data. Figure 16 shows all the main key factors required to be considered in economic risks due to CI failure.

Similar to societal risks, each factor will be weighted and the economic risk probability function given the CI failure will be a function of weighted key variables.

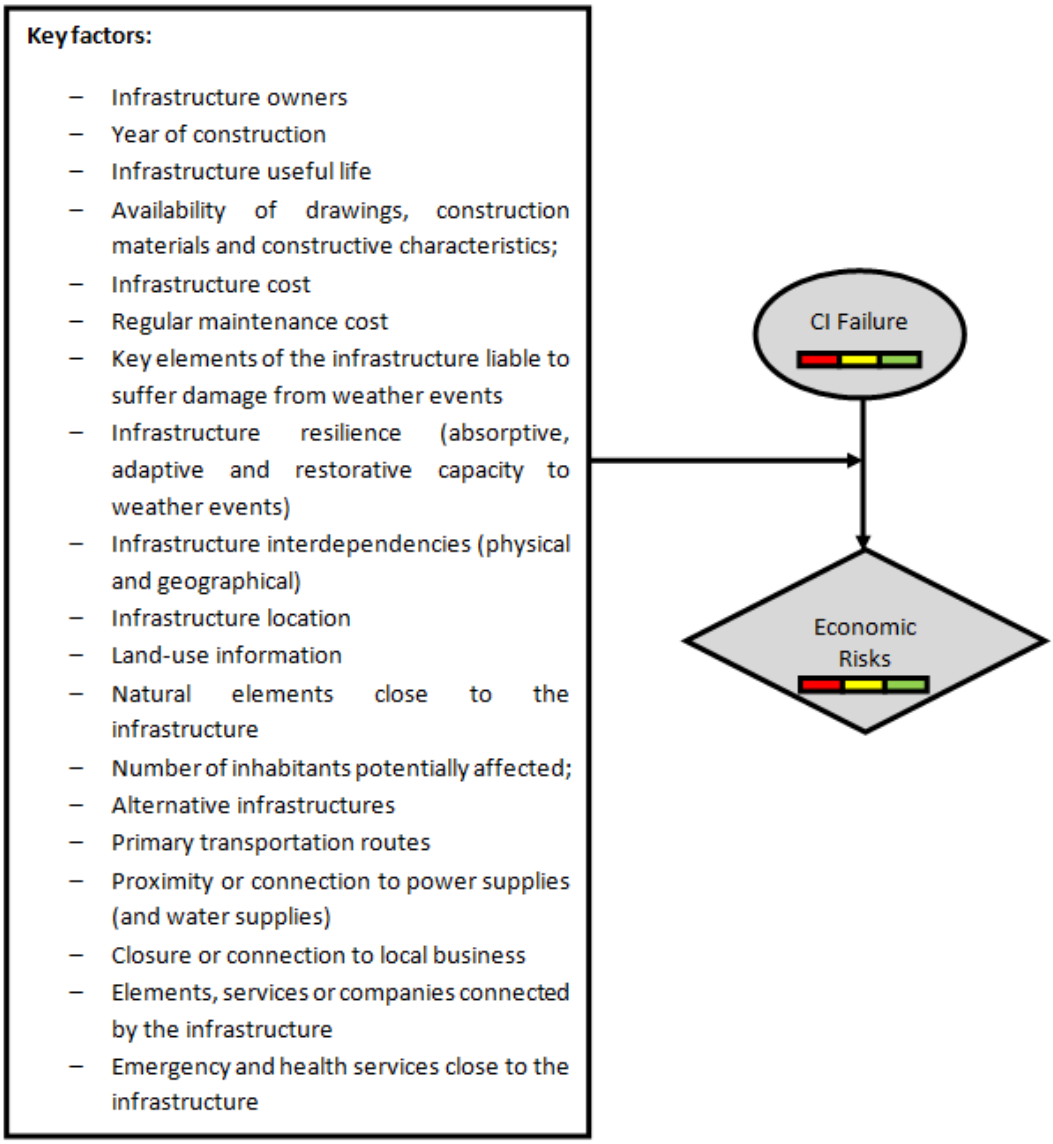


Figure 16- Key factors to be considered in Economic risks

5. Security Risks

Security is an accentuated discourse on vulnerability (Barnett, 2001). Like vulnerability, its assessment requires considering the risk of exposure, susceptibility to loss, and capacity to recover. However, like vulnerability and risk, it is more socially constructed than objectively determined. The distinction is that security is attached to the most important of vulnerable entities – for example the nation (national security), basic needs (human security), income (financial security) and property (home security). In this study security risks are limited to human basic needs including food, energy, and water supply security. Other means of security such as terrorist attacks by misusing the failure of infrastructure due to an extreme weather event is considered beyond the scope of the RAIN project.

Critical infrastructure failure due to extreme weather events could have little to no security impact, but in severe cases with longer recovery time, it can affect water supplies, transport networks, communication, finance and government services. For example extended power outages were found to have severe consequences such as: loss of food and refrigeration, inability to pump fuel, difficulties in carrying out activities and coordinating them for emergency services, due to failed communication systems. Moreover, electricity infrastructures are affected by extreme weather indirectly as extreme cold weather for prolonged periods of time increases electricity demands possibly causing a grid overload.

5.1. Qualitative Analysis of Security Risks

Direct Impacts of security risks are mainly:

- Degradation of fresh water supply

  Failure of critical infrastructures effect water supply security (from highly managed systems with multiple sources to a single rural well) to supply water to users. This may be due to a surplus of water which affects the operation of systems or a shortage of water relative to demands, the latter being triggered by a failure in water supply infrastructure or deterioration in water quality.

- Food systems security

  Food production, storage and delivery systems involve complex interdependent supply chains exposed to multiple hazards which can be affected by critical infrastructure failure. In the long term, impacts transmitted through an increase in the price of food can be especially challenging for the poor communities in developing countries.

- Energy Supply Security

  The energy production infrastructure is often located in regions susceptible to flood, and damaging storms. It is, therefore, highly vulnerable to disruption due to extreme weather events.

The other means of security risks, such as Human Security, undermining of livelihoods, compromising cultures and individual identities and increased migration or increased food prices due to reduced access to and production of food that affects both consumers and food producers, increased rate of looting and theft and an increase in border tension due to rise in migration which can substantially rise because of decrease in life quality, are not considered in the current study. Disruption of transport networks can cause significant effects to the economy and quality of life of regular users.

5.2. Quantitative Analysis of Security Risks

To the best knowledge of the authors, there has been no publications which consider quantitative analysis of security related risks due to critical infrastructure failure. Therefore, in this study the recovery time of a damaged system that is deemed to be essential to the operation of civic society is used as a measure for security risk:

$$1 - F_T(x) = P(T > x) = \int_x^{\infty} f_T(x)dx \qquad \text{Eq. 12.}$$

where, $F_T(x)$ is probability distribution function of the recovery time and $f_T(x)$ represents probability density function of the recovery time of the supply system.

The main factors need to be considered in probability of security risk assessment are shown in Figure 17.

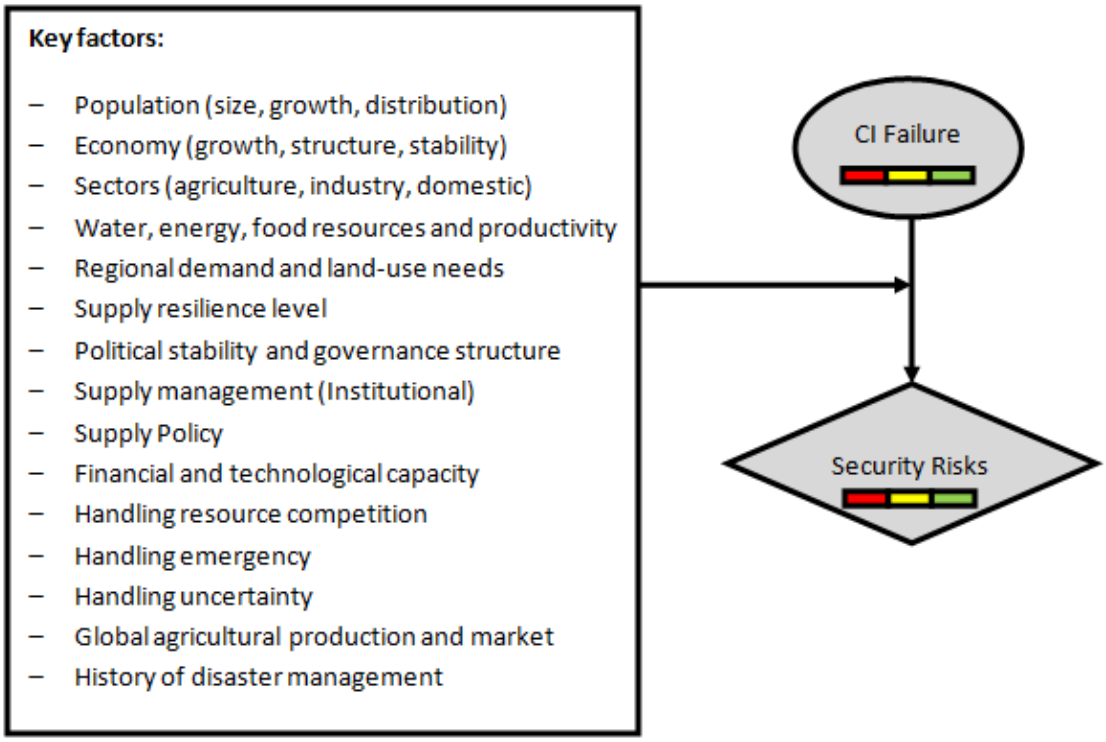


Figure 17- key factors to be considered in security risks

6. Objective Ranking Tool

The Objective Ranking Tool (ORT), which is presented in detail in Deliverable D5.1 (Van Gelder & Van Erp, 2015) is based on three scientific principles: Similarity Judgment, Analytic Hierarchy Processing (AHP) and the use of a Delphi-panel. The RAIN partner PSJ developed ORT as a dedicated application that can be used in any form of decision-support, decision-making and prioritization of alternatives. ORT provides a unified process and structured support tool.

The principle of 'equality' - hereinafter referred to as similarity - supposes that people make judgments and reviews about ‘phenomena’ by comparing the agreement and differences between these objects. The use of a structured group of experts in the form of a Delphi panel is required in order to achieve the most accurate possible results. This has benefits for both the determination of the characteristics, determining the weighting factors as well as in assessing whether an item meets the characteristics, thus providing reliability to the decision making process. The results of the ORT process indicate a ranking in the extent to which objects has a certain degree of equivalence thus facilitating the decision-making process. In other words, the ORT analysis considers the relative ordering between objects.

In the RAIN project, the ORT-application will be used to evaluate the key factors affecting each aspect of risks due to CI failure (i.e., criteria impacting societal, security and economic risks). For this purpose the key factors will be evaluated for their respective contribution to the each risk (societal, security or economic) and the Delphi panel of experts will assign a weighing factor to each key factor based on their field of expertise. Then with the use of ORT, all key factors will be classified in order of importance. Figure 18 illustrates a schematic view of ORT procedure in which the Analytic Hierarchy Processing of key factors is preceded by assigning a weighting factor to each key parameter of risk based on the Delphi panel and similarity judgment principle.

ORT will also be used to asses and evaluates the criteria that the impacts of single-mode failures have on the various impact markers.

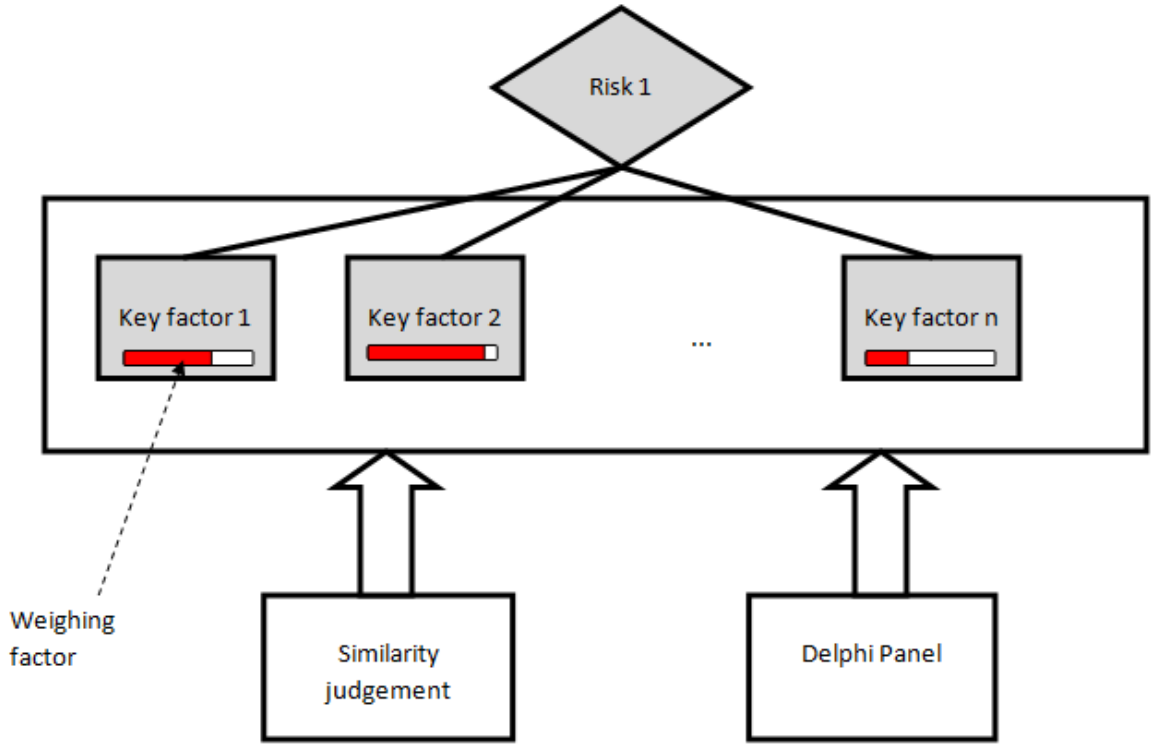


Figure 18- schematic illustration of ORT procedure

7. Conclusion

This document presents a summary of probabilistic risk assessment techniques of societal, security and economic impacts of critical infrastructure failure due to extreme weather events.

First an overview of critical infrastructure is provided according to the methodologies provided in D3.1 and D4.1 of RAIN project. Then the impacts of CI failure due to an extreme weather event is detailed from three aspects; society, economy and security. For societal risks, fatalities and injuries are considered as the main single-mode societal risks due to infrastructure failure. In the case of economic risks, the cost of repair or replacement, cost of labour, availability of materials, age of the existing Infrastructure and impact on alternative routes are listed as the main impacts of CI failure from economy point of view. Security supply of basic human needs such as water, food and energy are assumed to be the main security risks (single-mode) due to CI failure. The key variables required to quantify each aspect of risk is provided.

In the last section an overview of the ORT technique is given which will be used as a tool in the further studies for evaluating the criteria that impacts of the single-mode failures will have on the various impact markers of case studies.

8. References

Act No. 45., 2011. Act No. 45 from 8th February 2011 about critical infrastructure.

Ale, B.J.M., Laheij, G.M.H. & Uijt de Haag, P.A.M., 1996. Zoning instruments for major accident prevention, Probabilistic Safety Assessment and Management 96, '96; Proceedings of ESREL 96 - PSAM-III, Crete.

Andreassen, S., Jensen F.V., & Olesen K.G., 1991. Medical Expert Systems Based on Causal Probabilistic Networks. International journal of *Biomedical Computing*. 28(1-2), pp: 1-30.

Apostolakis, G.E., 2004. How useful is quantitative risk assessment? Journal of *Risk Analysis*, 24(3), pp: 515-520.

Barnett, J. 2001. Security and climate change. Tyndall Centre for Climate Change Research. Working paper 7.

Carter, D. A., 2002. A worst case methodology for obtaining a rough but rapid indication of the . societal risk from a major accident hazard installation, Journal of *Hazardous Material*. A92, pp: 223–237

Council Directive., 2008, Council directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. L 345/75 Official Journal of the European Union; Published 23.12.2008.

Cutter, S.L., B. Boruff, & W. L. Shirley., 2003. Social Vulnerability to Environmental Hazards. Social Science Quarterly 84, no. 2 -June 2003.

Dvorak, D. & Luskova, M. 2015. Report on the list of critical land transport infrastructure elements and the most probable threats t critical land transport. Deliverable D3.1, EU funded RAIN project (Risk Analysis of Infrastructure Networks in response to extreme weather), 2014 - 2017, GA no. 608166.

Dower, N., 1995. Peace and security: some conceptual notes. Essays on Peace: Paradigms or Global Order. Central Queensland University Press, Rockhampton, pp: 18-23.

Garcia-Aristizabal, A. & Marzocchi, W., 2011. State-of-the-art in multi-risk assessment. Deliverable 5.1, EU funded MATRIX project (New Methodologies for Multi-Hazard and Multi-Risk Assessment Methods in Europe), 2010-2013, GA no. 265138.

Jonkman, S. N., van Gelder, P. H. A. J. M. & Vrijling, J. K., 2003. An overview of quantitative risk measures for loss of life and economic damage. Journal of *Hazardous Material*. A99, pp: 1–30.

Marin, J & Halat, M., 2015. Report on energy and telecommunication infrastructure description and identification of critical energy and telecommunication infrastructures at a European Level. Deliverable D4.1, EU funded RAIN project (Risk Analysis of Infrastructure Networks in response to extreme weather), 2014 - 2017, GA no. 608166. *pending publication*

Prak, P., 2009. Research into the application of similarity judgment in determining alert locations within the railway sector. Master Thesis, School of Executive Education of the Technical University Delft.

Soroos, M., 1997. The Endangered atmosphere: Preserving a global commons. University of South Carolina Press, Columbia.

Tversky, A., 1984. Features of similarity. Psychological Review, 3, pp: 327-352.

Van Gelder, P & Erp, N., 2015. Report on risk analysis framework for single and multiple hazards. Deliverable D5.1, EU funded RAIN Project (Risk Analysis of Infrastructure Networks in response to extreme weather) , 2014 - 2017, GA no. 608166 - *pending publication*

Van Westen, C.J., Alkema, D., Damen, M.C.J., Kerle, N. & Kingma, N.C., 2011. Multi-hazard risk assessment guide book. United Nations university-ITC school of Disaster Geo-information Management (UNU-ITC DGIM)

Vrijling, J.k., Van Hengel, W. & Houben, R.J., 1995. A framework for risk evaluation, Journal of *Hazardous Material*. 43, pp: 245–261.

Vrijling, J.K. & Van Gelder, P.H.A.J.M., 1997. Societal risk and the concept of risk aversion, Proceedings of *Advances in Safety and Reliability*, vol. 1, Lissabon, pp: 45–52