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 6.2 E0.2**
Deliverable Name	**Quantification of multi-mode risks and impacts**
Contributing Partners	**ROD**
Date of Submission	**December 2015**

The 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**
- **The content does not add new information on vulnerabilities, sensitivities or incident scenarios on specific objects or transport systems or in general**
- **There are no uncertainties that might need to contact the NSA**

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	**Signed by the chairman**
Date of Evaluation	**2016-01-15**

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

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 6.2-Quantification of multi-mode risks and impacts

Authors

Donya Hajializadeh* (Roughan & O'Donovan)
Ciaran Carey (Roughan & O'Donovan)
Mark Tucker (Roughan & O'Donovan)

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

Date: 31/12/2015

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	14/12/2015	DH, CC and MT	First Draft
E02	06/01/2016	DH, CC, MT,ML and KG	Document revised according to internal reviewers' comments.

Document Name: Quantification of multi-mode risks and impacts

Work Package: 6

Task: 6.3

Deliverable: 6.2

Deliverable scheduled date: (20th Month) 31th December 2015

Responsible Partner: Roughan & O'Donovan

Table of Contents

1. Introduction

Changes in the likelihood and severity of extreme weather events and climate-related disasters can result in the failure of critical infrastructure (CI) elements and networks. A Quantitative risk assessment of such failures is a core part of risk management protocols. In Work Package 5 (WP5) of the RAIN project, a systematic risk analysis framework is being developed which quantifies risks due to extreme events by explicitly considering the impacts of extreme weather events on critical infrastructure. In conjunction with the risk assessment framework being developed in WP5, the activities in WP6 seek to benchmark the framework against case studies by assessing the societal, security and economic impacts of critical infrastructure failures based on single-mode and multi-mode failure (i.e., scenarios which involve the failure of either a single hazardous event resulting in critical infrastructure failures without considering the interaction between infrastructure network elements and scenarios with multi hazardous event resulting in propagation of failure in infrastructure network due to their location or functionality interaction). Furthermore, in WP6 the quantifiable benefits of providing resilient infrastructure will be estimated from a societal, security and economic standpoint.

The first deliverable of WP6, Deliverable D6.1 (Hajializadeh and Tucker, 2015), addresses single-mode risks and the impacts of extreme weather events on CI and provides the methodology for computation of societal, security and economic impacts. In this report, Deliverable D6.2, multi-mode risks and impacts are addressed. As such, this document gives an overview of an advanced risk assessment procedure which has been developed to quantify multi-mode risks and the techniques required to assess the interaction between different hazardous event and various critical infrastructure systems. A review of the single mode and multi-mode risk assessment technique being developed in work package 5 is presented initially followed by a description of multi-mode scenarios and components. In this study it is assumed that multi-risk scenarios refer to two main components: a. multi-hazard (i.e. the potential for one or more than one hazard triggered by primary hazard event) and b. multi-vulnerability (i.e., potential for failure propagation in critical infrastructure network(s)) scenarios. Descriptions of various multi-hazard and multi-vulnerability scenarios are provided and the approach required to quantify risk arising from each scenario is outlined.

In Deliverable D6.3 (due in Month 30), the contents of Deliverable D6.1 (Hajializadeh and Tucker, 2015 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 of providing resilient infrastructure.

2. Review of Multi-risk assessment framework

Deliverable 5.1 (van Erp and van Gelder, 2015) of the RAIN project described the general risk assessment technique. In this section, a summary is provided of the modification made from Bayesian Probability theory to Markovian network to allow for multi-risks assessment.

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 assessment should consider two main components: 1) a multi-hazard and 2) a multi-vulnerability component.

According to D5.1 of the MATRIX project (Garcia-Aristizabal and Marzocchi, 2011) the multi-hazard concept may refer to (a) the fact that different hazard sources might threaten the same exposed elements (either at the same time or at different times), 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 different degrees of vulnerability 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 this report, a multi-hazard event refers to interactions in which the primary hazard triggers or increases the probability of secondary hazards occurring. The multi-vulnerability component represents the dependencies and interdependencies in the infrastructure network. In contrast, single risk assessment concepts consider the risk of a particular hazard occurring in a particular geographical area during a given period of time (Hajializadeh and Tucker, 2015) leading to failure of one or more CI(s) without considering the interactions between the risk components (i.e., Hazards and Vulnerabilities). Figure 1 illustrates the difference between single and multi-mode risk scenarios.

In the following section, the general framework of the risk assessment technique being developed in Work Package 5 of RAIN project is provided, explaining the implementation of the technique for single and multi-mode scenarios.

2.1. Bayesian probability method for multi-risk assessment

In WP5, details of a Bayesian probability theory based risk assessment framework are presented (van Erp and van Gelder, 2015). This framework is a probabilistic graphical model that represents hazardous events and the resulting infrastructure failure by means of a directed acyclic graph (DAG). In Bayesian probability theory, probability distributions are combined by product and sum rules; those being the only admissible operators by which to combine probabilities consistently (Cox, 1946). It is worth noting that Bayesian Networks are a special instance of the more general Bayesian probability theory; in other words, Bayesian probability theory is more general as it (1) applies to both continuous and discrete probability distributions, (2) has a built-in model-selection functionality, and (3) offers several approaches to translate states of uncertainty to probability distributions (van Erp and van Gelder, 2015).

Since modelling of multi-mode risks requires an undirected and possibly cyclic relationship, Markov networks should be implemented in the Bayesian approach to allow for bi-directional link between nodes. In the work being conducted in Work Package 5, Markovian probability models will be developed in order to come up with a generic class of probability models in order to model both interdependencies in hazards and infrastructure networks.

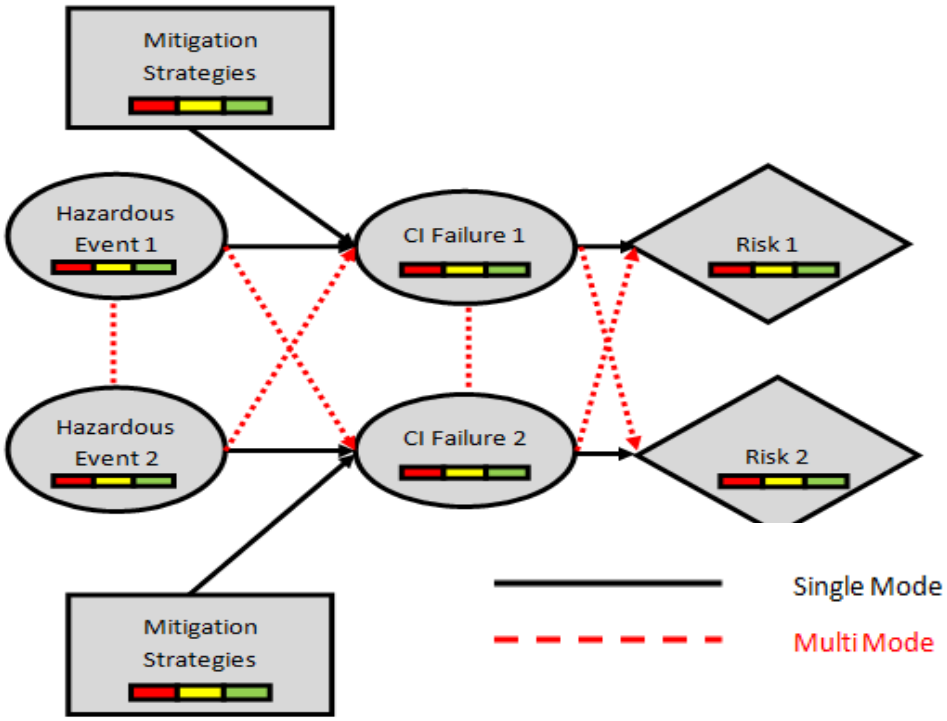


Figure 1-Single-risk and Multi-risk example for a system of two hazardous events and two critical infrastructures

The initial inputs in a Markovian risk assessment framework are the various multi-mode scenarios which could potentially occur. The different hazard and vulnerability components are represented by nodes, with corresponding probability distributions. As explained in the previous section, each multi-mode scenario has two main components: the multi-hazard element, considering the interaction between hazardous events, and the multi-vulnerability component, which accounts for infrastructure typology and their corresponding functionality dependencies and interdependencies (i.e., potential failure propagation from one system to another system). In the multi-vulnerability component a “system” can refer to either an individual infrastructure with corresponding elements or a network of infrastructures as illustrated by Figure 2. Figure 3 illustrates an example of system interdependency between different networks.

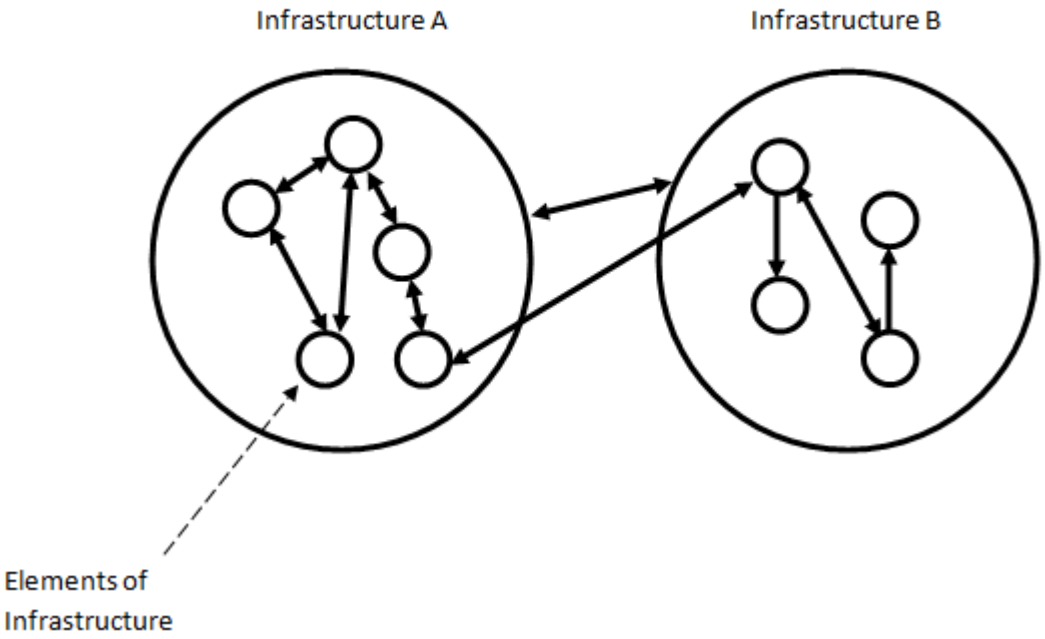


Figure 2-Dependencies and Interdependencies in Infrastructure system(s)

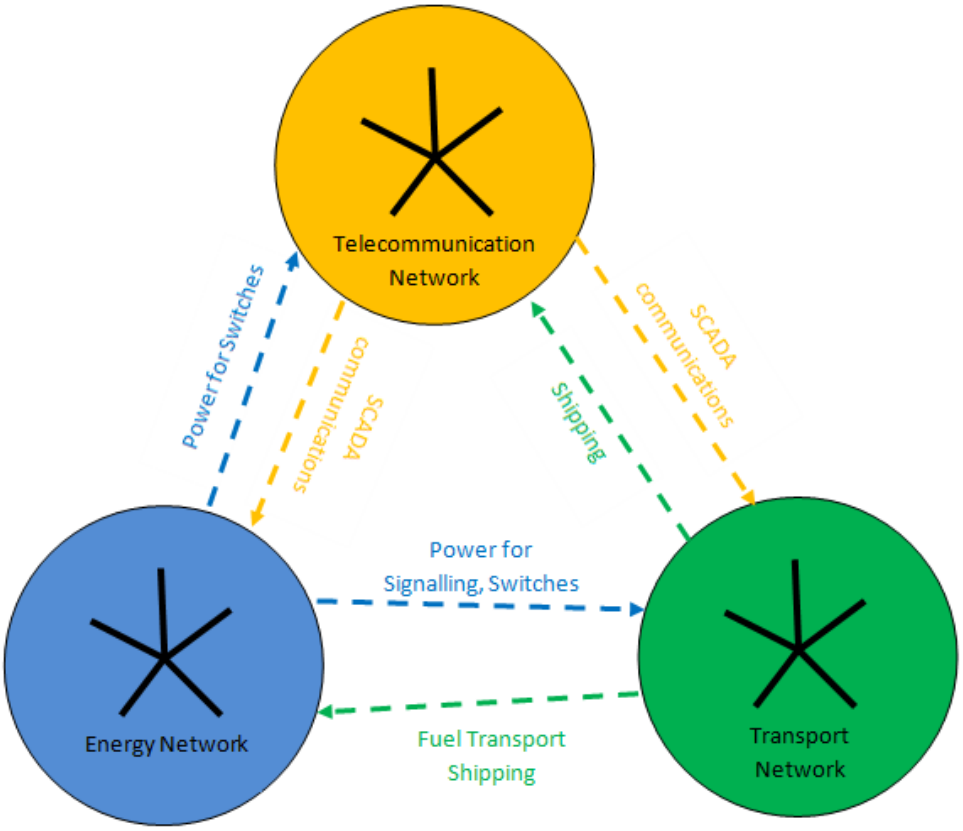


Figure 3- Interdependencies between networks

Figure 4 illustrates the summary of different type of single and multi-mode risk assessment components and description. As can be seen from the figure, in summary, both single and multi-mode risk assessments consist of two main component hazard and vulnerability assessment. For single-mode assessment, the single hazard corresponds to the single triggering event resulting in extreme hazardous event. The single vulnerability then refers to one or more infrastructure failure purely due to extreme weather hazards without considering the interactions between different elements in an infrastructure or different infrastructures in a network. The potential interaction between primary and secondary hazardous events and also possible failure propagation due to interaction between in infrastructure elements and between different systems of infrastructure will be quantified in multi-risk assessment in the form of multi-hazard and multi vulnerability components respectively. The current deliverable provides an overview of each multi-risk scenario component, details on selected multi-hazard and multi-vulnerability scenarios and their implementation in the risk assessment framework.

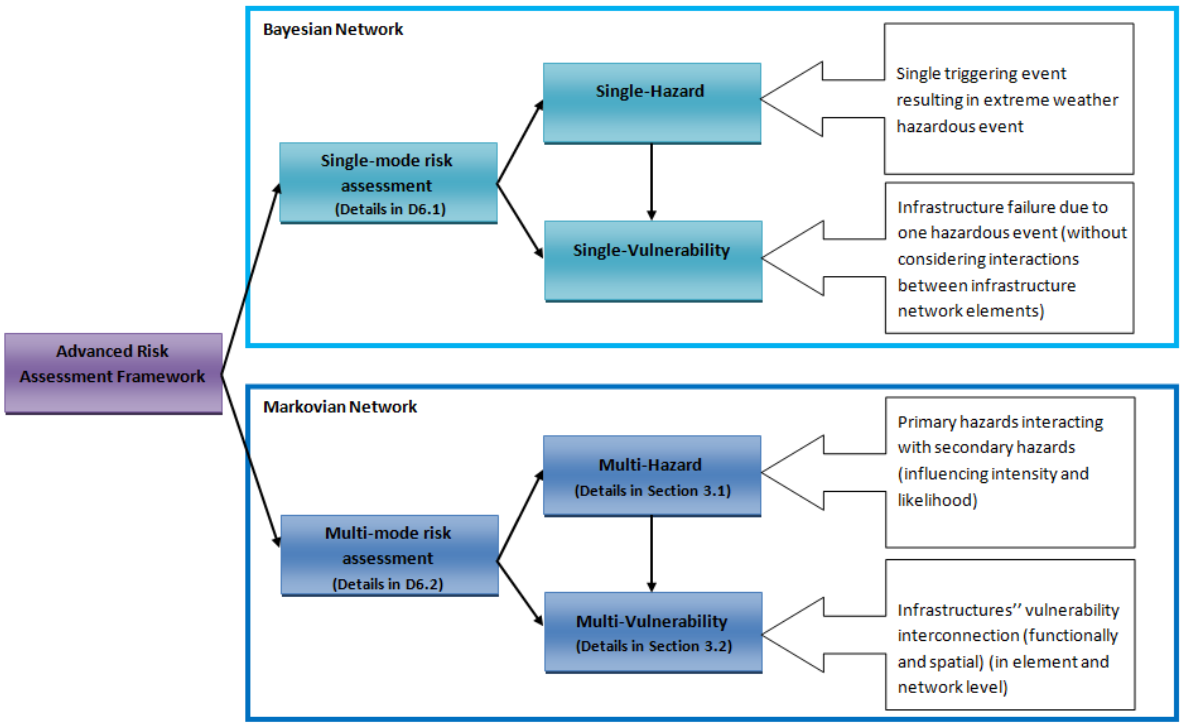


Figure 4- components of single-mode and multi-mode risk assessment

3. Multi Risk Scenarios

3.1. Multi Hazardous scenarios

Two or more hazards may affect the same region at the same time without any interaction and with their simultaneous occurrence happening purely by coincidence. Where interaction does take place the term 'cascade' or 'domino' is often used in the literature (Kumasaki et al. 2015). Kappes et.al (2012) gives an outline of terms used to describe the interaction between hazards and group 'knock-on effect' and 'follow-on event' as well as 'triggering effect' along with 'cascade' etc.

In this study, 'interactions' are considered to be those where a primary hazard triggers or increases the probability of secondary hazards occurring. In other words, primary hazards (those which occur first) interact with secondary hazards by (a) triggering the secondary hazards (b) increasing the probability of the secondary hazard or (c) both triggering and increasing the probability of the secondary hazard. Kappes et al. (2012) note that in using the term 'interaction' the impression can be created that there is bidirectional influence between the hazards which may or may not be the case.

3.1.1. Selected scenarios

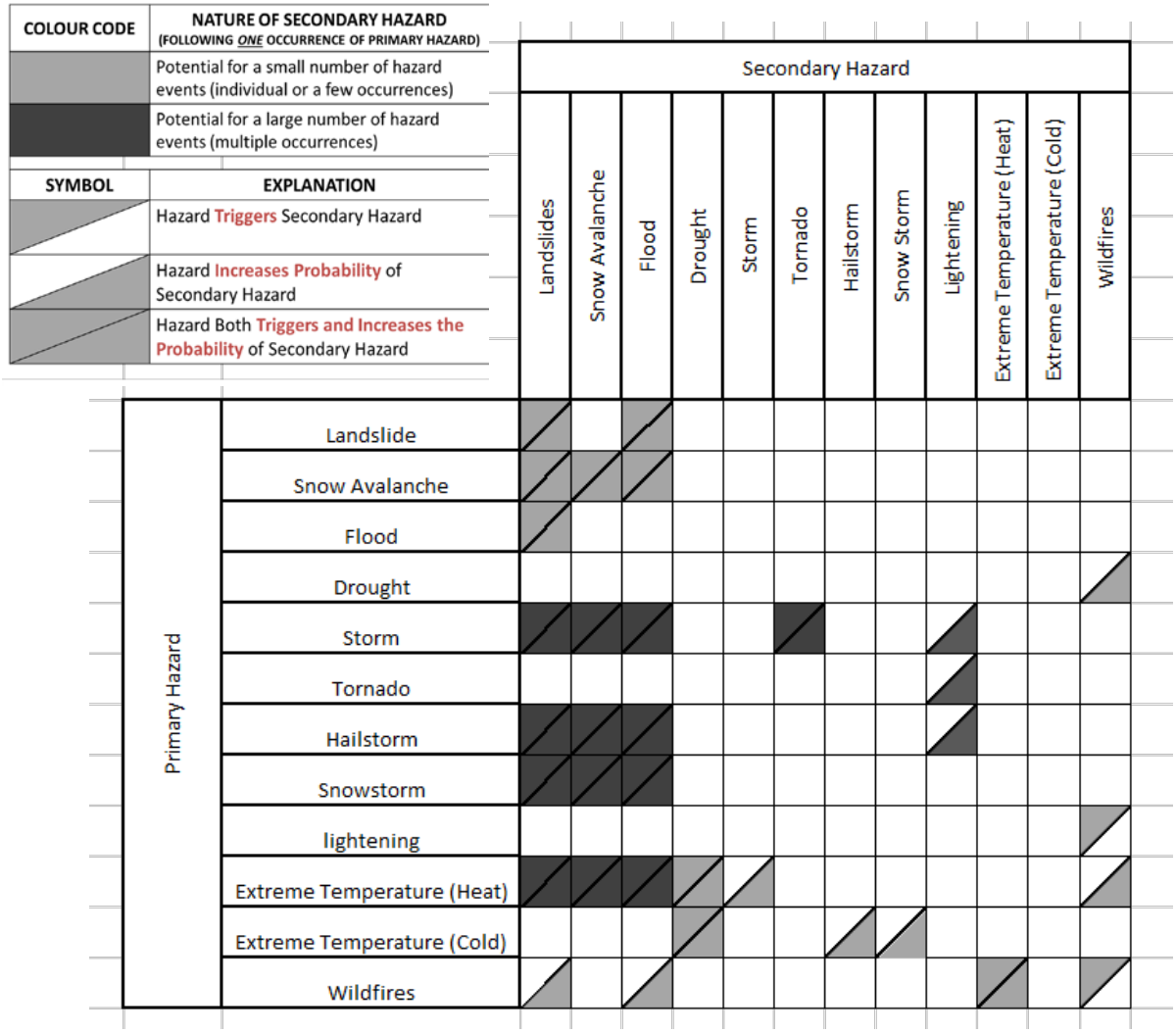
There are distinct and broad ranges, spatially and temporally, over which each of the different extreme weather events have an impact. Generally, the assessment of spatial and temporal scales does not consider interactions between different hazards, instead focusing on single hazards. Such approaches often treat hazards as isolated or independent phenomena. An Earth system sciences approach, however, indicates significant interactions between various component systems (such as the lithosphere, atmosphere, hydrosphere, and biosphere) and thus highlights the inadequacy of always treating hazards as independent. Such an assumption can lead to the distortion of management priorities, increased vulnerability to other spatially relevant hazards, or an underestimation of risk (Gill and Malamud, 2014). The same authors have conducted an extensive review of the hazard interaction of 21 natural hazards drawn from six hazard groups (geophysical, hydrological, shallow Earth, atmospheric, biophysical and space hazards) (Gill and Malamud, 2014). As the RAIN project is focused on extreme weather events, the interactions between hydrological, Atmospheric, biophysical groups from Gill and Malamud's (2014) study are used in the current report as multi-hazardous scenarios which will be considered further in developing multi-mode scenarios. These multi-hazardous scenarios are summarised in Table 1 below. The table also outlines the forecasting potential of the location, timing and magnitude of each secondary hazard, given information about the primary hazard. Each forecasting factor is given a classification from N (value 0) to H (value 3) depending on what information is available to help constrain the factor. In this Table N refers to None, L to Low, M to Medium and H to High contributing factor. These three values are totalled to give a rating from 0-9, and colour coded in terms of the ability to characterise the secondary hazard, with poor (0-3, light shading), semi (4-6, medium shading) or excellent (7-9, dark shading).

Table 1- Ability to characterize triggered and increased probability secondary hazards given information from the primary hazard. (Gill and Malamud, 2014).

PRIMARY HAZARD	SECONDARY HAZARD	FORECASTING FACTORS			OVERALL RATING
		LOCATION	TIME	MAGNITUDE	
Landslide	Landslide	N – L – **M** – H	N – L – **M** – H	N – L – **M** – H	6/9
	Flood	N – L – **M** – H	N – L – **M** – H	N – L – **M** – H	6/9
Snow Avalanche	Landslide	N – L – **M** – H	N – L – **M** – H	N – **L** – M – H	5/9
	Snow Avalanche	N – L – **M** – H	N – L – **M** – H	N – **L** – M – H	5/9
	Flood	N – L – **M** – H	N – **L** – M – H	N – L – **M** – H	5/9
Flood	Landslide	N – L – **M** – H	N – L – **M** – H	N – **L** – M – H	5/9
Drought	Wildfire	N – **L** – M – H	N – **L** – M – H	N – **L** – M – H	3/9
Storms	Landslide	N – L – **M** – H	N – L – M – **H**	N – L – **M** – H	7/9
	Snow Avalanche	N – L – **M** – H	N – L – **M** – H	N – **L** – M – H	5/9
	Flood	N – L – M – **H**	N – L – **M** – H	N – L – **M** – H	7/9
	Tornado	N – **L** – M – H	N – **L** – M – H	N – **L** – M – H	3/9
	Lightning	N – **L** – M – H	N – L – **M** – H	N – **L** – M – H	4/9
Tornadoes	Lightning	N – **L** – M – H	N – L – **M** – H	N – **L** – M – H	4/9
Hailstorm	Landslide	N – L – **M** – H	N – L – **M** – H	N – L – **M** – H	6/9
	Snow Avalanche	N – L – **M** – H	N – L – **M** – H	N – **L** – M – H	5/9
	Flood	N – L – M – **H**	N – L – **M** – H	N – L – **M** – H	7/9
	Lightning	N – **L** – M – H	N – L – **M** – H	N – **L** – M – H	4/9
Snowstorm	Volcanic Eruption	N – L – **M** – H	**N** – L – M – H	N – **L** – M – H	3/9
	Landslide	N – L – **M** – H	N – L – **M** – H	N – L – **M** – H	6/9
	Snow Avalanche	N – L – **M** – H	N – L – **M** – H	N – **L** – M – H	5/9
	Flood	N – L – M – **H**	N – L – **M** – H	N – L – **M** – H	7/9
	Ground Collapse	N – **L** – M – H	N – **L** – M – H	N – **L** – M – H	3/9
	Ground Heave	N – L – **M** – H	N – L – **M** – H	N – L – **M** – H	6/9
Lightning	Wildfire	N – L – **M** – H	N – L – M – **H**	N – **L** – M – H	6/9
Extreme Temperature (Heat)	Landslide	N – L – **M** – H	N – **L** – M – H	N – **L** – M – H	4/9
	Snow Avalanche	N – L – **M** – H	N – **L** – M – H	N – **L** – M – H	4/9
	Flood	N – L – **M** – H	N – **L** – M – H	N – L – **M** – H	5/9
	Drought	N – L – **M** – H	N – L – **M** – H	N – **L** – M – H	5/9
	Storm	N – **L** – M – H	N – **L** – M – H	**N** – L – M – H	2/9
	Wildfire	N – **L** – M – H	N – **L** – M – H	N – **L** – M – H	3/9
Extreme Temperature (Cold)	Drought	N – L – **M** – H	N – L – **M** – H	N – **L** – M – H	5/9
	Hailstorm	N – L – **M** – H	N – L – **M** – H	N – L – **M** – H	6/9
	Snowstorm	N – L – **M** – H	N – L – **M** – H	N – L – **M** – H	6/9
Wildfires	Landslide	N – L – M – **H**	N – **L** – M – H	N – **L** – M – H	5/9
	Flood	N – L – M – **H**	N – **L** – M – H	N – **L** – M – H	5/9
	Wildfire	N – L – **M** – H	N – L – **M** – H	N – L – **M** – H	6/9
	Extreme Temp. (Heat)	N – L – **M** – H	N – L – **M** – H	N – L – **M** – H	6/9

According to Gill and Malamud's (2014) study, there are four types of hazard interaction: 1) interactions where a hazard is triggered, 2) interaction where the probability of a hazard is increased, 3) interactions where the probability of a hazard is decreased, 4) events involving the spatial and temporal coincidence of natural hazards. Table 2 indicates the secondary hazardous events resulting from primary events and the type of interaction.

Table 2- Hazard interactions and their types (Gill and Malamud, 2014).



3.1.2. Implementation in Risk Assessment Framework

In this study, hazard interaction will be accounted for by considering an increase in the secondary hazard intensity and likelihood as a function of primary hazard intensity and probability of occurrence. Gill and Malamud's (2014) have identified six possible relationships between the primary and triggered secondary hazard intensities which represent the majority of the case studies examined:

A. Threshold alone, where the secondary hazard will only occur if the intensity of the primary hazard is at or exceed a minimum threshold. In this type the intensity of the secondary hazard does not change unless the intensity of the primary hazard increases;

B. Continuous alone: the intensity of the secondary hazard can be mapped in a proportional way to the intensity of the primary hazard;
C. Threshold and Continuous: the secondary hazard will only occur if the intensity of the primary hazard is at or exceeds a minimum threshold and after this minimum value, the intensity of the secondary hazard will increase proportional to the intensity of the primary hazard;
D. Continuous and cut off: the intensity of the secondary hazard can be mapped in a proportional way to the intensity of the primary hazard. Beyond a certain primary hazard intensity, the intensity of secondary hazard will not increase further;
E. Threshold, continuous and cut off: The secondary hazard will only occur if the intensity of the primary hazard is at or exceeds a minimum threshold. After the threshold value, the intensity of the secondary hazard will then increase proportional to the intensity of the primary hazard. Beyond a certain primary hazard intensity, one or more limiting factors means the intensity of the secondary hazard will not increase any further;
F. Complex: The intensity of the secondary hazard is very difficult to relate to the intensity of the primary hazard. This could be because of it being very specific to the particular location.

Figure 5 illustrate the differences between each type schematically.

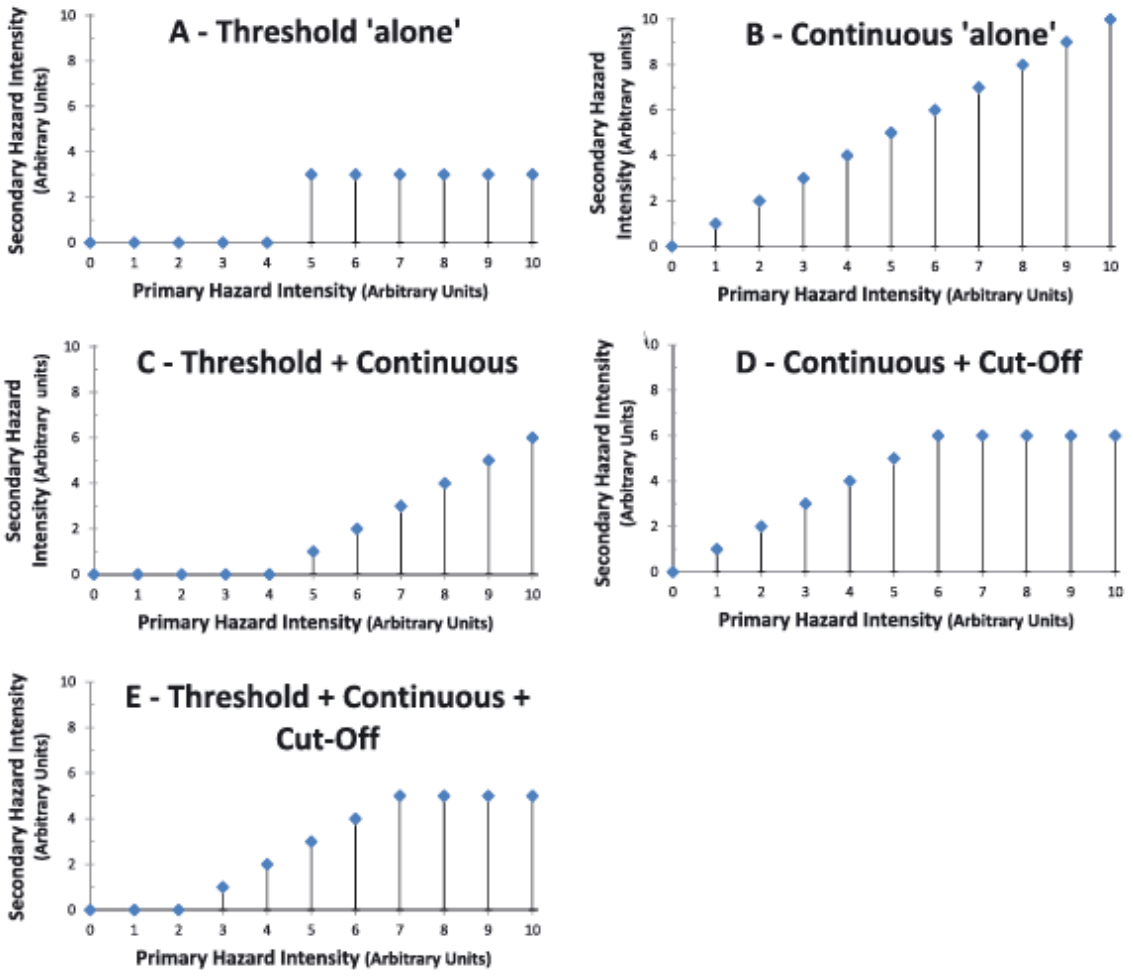


Figure 5: Possible triggering intensity relationships (Gill and Malamud, 2014)

In any case where the likelihood a triggered event is increased, the focus is on quantifying the relationship between the intensity of the primary hazard and the likelihood (in the form of potential intensity) of the secondary hazard. Gill and Malamud (2014) have introduced three forms of relationship between the primary and potential secondary hazard intensity:

a. Threshold alone: where the primary hazard changes the natural environment in such a way as to change certain parameters that influence the occurrence of a secondary hazard, moving these parameters closer to the minimum triggering threshold;
b. Continuous alone: as the intensity of a primary hazard increases, it changes the natural environment so as to increase the likely intensity (in terms of spatial extent affected, the temporal duration) of any future occurrences of the secondary hazard and
c. Complex: where there is a high level of dependency on a specific location, making it difficult to represent the relationship clearly.

The combination of the first 5 intensity relationships and the first two intensity-probability relationships will be included in the hazardous nodes of the multi-mode risk framework. This will allow hazard interaction to be accounted for and will be benchmarked against specific case studies in Deliverable D6.3.

3.2. Multi vulnerability scenarios

Infrastructure networks do not exist in isolation. Rather they are interconnected to other infrastructures and, as technological development increases, so too does the linkage between networks (Wang, Hong, and Chen 2012). The term interdependency is used to describe the relationship between infrastructures (Rinaldi, Peerenboom, and Kelly 2001) where each infrastructure influences the other(s). This bi-directional relationship can increase the complexity in the system of systems significantly.

According to Zimmerman (2001), infrastructures can be interconnected functionally and spatially – An example of a functional interconnectedness failure between infrastructures would be a fault in power supply causing issues with train lines. An example of a spatial interconnectedness failure would be a burst water main flooding a road etc.

In general, infrastructure interdependencies can be categorized according to various dimensions in order to facilitate their identification, understanding and analysis. According to the literature (Rinaldi et al., 2001), there are typically six dimensions to characterise the interdependencies:

1. The type of interdependencies (physical, cyber, geographic, and logical),
2. The infrastructure environment (technical, business, political, legal, etc.),
3. The couplings among the infrastructures and their effects on their response behaviour (loose or tight, inflexible or adaptive),
4. The infrastructure characteristics (organisational, operational, temporal, spatial),
5. The state of operation (normal, stressed, emergency, repair), the degree to which the infrastructures are coupled,
6. The type of failure affecting the infrastructures (common- cause, cascading, escalating).

Rinaldi et al. (2001) categorise interdependency into four types: 1) Physical Interdependency: refers to the cases where physical output of one infrastructure is the physical input to another infrastructure. In this type of interdependency, perturbations in one infrastructure will impact the other. A simple example of this type of relationship is illustrated when a tree falls on a power line during a thunderstorm resulting in a loss of power to an office building and all the computers inside. 2) Cyber Interdependency: occurs due to infrastructures being connected via information links. For example, a supervisory control and data acquisition (SCADA) system which monitors and controls elements on the electrical power grid is an example of this type of relationship between the SCADA system and the power grid. While a loss of the SCADA system will not necessarily lead to gird shut down, the ability to remotely monitor and operation breakers will be lost. 3) Geographical Interdependency: means that two infrastructures impact one another because of physical proximity. Examples include flooding or fire affecting all the assets located in one area. 4) Logical Interdependency: refers to the interdependencies which the state of one infrastructure depends on the state of another infrastructure, usually via human decisions and actions. For example, a lower gas price increases the flow of gasoline and traffic congestion.

The interdependencies of a network of infrastructures depending on the scale of modelling can be established through either a 1) Holistic Perspective – Infrastructure Level, where each infrastructure is viewed as a single, monolithic entity with well-defined boundaries and a (possibly reduced) set of functional properties; or 2) Reductionist Perspective – Component Level, where it identifies "elementary" components within an infrastructure and then describes the evolution of the entire system based on the "aggregated" behaviour of these components. In the reductionist perspective, the boundaries of each infrastructure tend to fade, but the interactions between components can be detected.

The RAIN project is focused on three main infrastructure networks: (i) Land Transport Infrastructure, (ii) Energy Infrastructure and (iii) Telecommunications Infrastructure. In WP3 of the RAIN project a methodology was developed to identify critical components for land transport infrastructure. The details can be found in RAIN Deliverable D3.1 (Dvorak and Luskova, 2015) and are summarised in the first column of Table 3 below, while the identified components are in the first column of Table 3. Table 3 also shows the critical components for both the Energy and Telecommunications networks that were identified in RAIN WP4. Further details are provided in D4.1 (Marin and Halat, 2015).

Table 3 Critical Infrastructure Components

Land Transport Infrastructure	Energy Infrastructure	Telecommunication Infrastructure
• Roads; • Intersections; • Stations of public transport; • Bridges; • Tunnels; • Intersection control systems; • 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.	• 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.	• Outside Plant equipment; • The End Offices; • The Central Offices; • Aerial trunk lines; • Underground trunk lines; • RF link trunk lines. • Class 1, 2, and 3 centres; • Aerial backbone lines; • Underground and submarine backbone lines; • RF and Satellite Backbone lines; • Base Stations (BS); • Base Station Controllers (BSC); • Mobile Switching Centre (MSC); • Gateway MSC; • Home Location Register (HLR); • Visitor Location Register (VLR).

3.2.1. Selected Scenarios

3.2.1.1 Interdependencies (Element Level)

Land Transport Infrastructure

Land transport infrastructure is highly connected within the road or rail network, therefore failure in one section of the network would cause closure in the route passing through the failed section of infrastructure. Closures in sections of transport networks results in traffic flow redistribution which, depending on traffic flow, could result in failure of the network if the alternative routes are incapable of catering for the increased levels of traffic flow.

The following section summarises the most likely triggering scenarios causing closure in road and rail networks, which will be used to select the multi-vulnerability scenarios for the multi-mode risk assessment.

- Windstorms and tornadoes effecting roads and railways due to falling trees and overturned high-sided vehicles and causing long queues of traffic due to closed bridges and roads. They can also lead to disruption in train traffic timetables due to adjusted train speeds.
- Heavy rainfall, flash floods and coastal flood affecting the roadways and rail lines due to water mass and debris flow which can lead to the closure of road and rail infrastructure. These events can also erode bridges and rail embankments or even wash them away. Heavy rainfall can also initiate landslides which can result in road and rail infrastructure closure.
- Accumulated hail can result in the closure of the road and rail network.

- Lightening can cause fire in rail networks and consequently stops the functionality of the network, fully or partially depending on the extent and severity of the event.
- Snow and snow storms, blizzards and freezing rain can result in the closure of roads due to low visibility, which can lead to an increase in congestion in rail and road infrastructure which can also become blocked due to fallen trees with increased likelihood of accidents.
- Wildfires causing closure in road and railway infrastructure.

Energy Infrastructure

Since power and telecom infrastructures are closely linked, local failures have the potential to cause significant effects in the network at far away locations, and with nearly instant propagation (Marin and Halat, 2015). It should be noted that Telecom networks degrade more gracefully in the event of local failures (except in the case of cyber-security events, which can quickly spread globally). Power grids, on the other hand, degrade more abruptly, and are more likely to result in a widespread blackout. However, in both cases it is quite likely that a single failure has the potential to immediately change the physical state of large parts or even the whole network (e.g. increasing flows at stressed paths, or rerouting traffic and overflowing routers) and, as a consequence, immediately increase the likelihood of further network failures both locally and globally. Therefore, in the case of Energy and Telecoms, in contrast to Transport infrastructure networks, the effects of local failures have two equally important components: (a) the local impacts derived from the single-mode failure (e.g. the loss of power by a whole neighbourhood due to a flooded substation) and b) the impact on the rest of the network. It is true that some failures in transport (e.g. a critical junction) may impact the rest of the network, but this does not happen with the degree of pervasiveness, long range, and instantaneous effects that we encounter in Energy and Telecom networks. This implies an increase in the likelihood of cascading failures, not just locally but potentially at far away distances. Measuring this impact is not easy in general, because it depends on the current operational state of the network.

Figure 6 shows a schematic view of the dependencies and interdependencies in 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) (Marin and Halat, 2015).

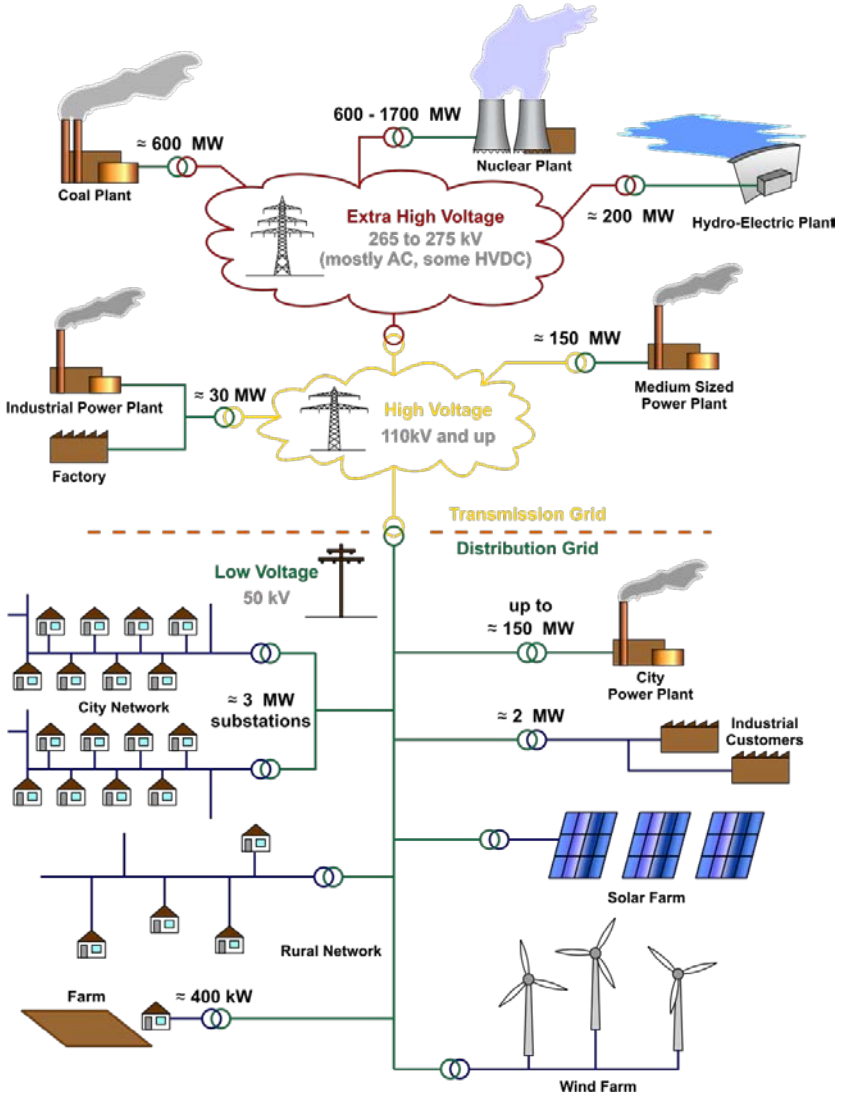


Figure 6- Schematic view of the electric power network infrastructure (source: Wikipedia). The two "clouds" depicting transmission are really a meshed network, which gives the power grid its name.

Extreme weather events can significantly affect energy production and delivery facilities, causing supply disruptions of varying lengths and magnitudes and affecting other infrastructure that depends on energy supply. The impacts in terms of loss of service depend a lot on the section of the network being affected. If the assets belong to the transmission part and the incidents are not very widespread geographically, chances are the service can continue uninterrupted, depending on redundancy level. If the incidents affect distribution equipment, the impact will depend on how far down the distribution this happens. Higher upstream, distribution networks typically have some degree of "reconfiguration" in order to isolate faulted sections. But moving to the distribution levels and the consumer end, supply becomes purely radial (i.e. tree-like). There, a loss of a transformer or a line means that all the associated customers become disconnected.

The selected triggering multi-vulnerability scenarios to be considered in RAIN are chosen according to an extensive study conducted in Work Package 4 of the project (Marin and Halat, 2015):

- Lightening affecting overhead lines and unsheltered transformers.

- Wind storms affecting overhead lines and unsheltered transformers, typically bending or toppling power line towers and causing electrical faults. The damage to towers (pylons), either directly or indirectly by fallen trees, can be permanent.
- Ice/snow storms affecting overhead lines and unsheltered transformers which also can cause sagging in power lines under its weight, or whip violently when the wind blows large chunks of ice off the line.
- Flash floods affecting generator plants which could also affect ground-level and underground transformers, often causing permanent damage. Due to debris flow, they can also affect power pylons.
- Extreme cold spells affecting generator plants due to inadequate winterization of the power plant equipment, and straining the grid due to peak loads.
- Extreme heat waves causing strain on the grid due to peak demand, also increasing likelihood of congested transmission lines, due to the reduction in capacity (lower thermal limits due to less thermal dissipation) and to line sagging.
- Wild fires affecting mainly unsheltered transformers, sitting on ground level.
- Sand storms affecting power transmission lines severely due to fallen trees.
- Sudden seasonal drought putting stress on the grid due to generation shortage.

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 7 shows the dependencies and interdependencies in the telecommunication network (Marin and Halat, 2015).

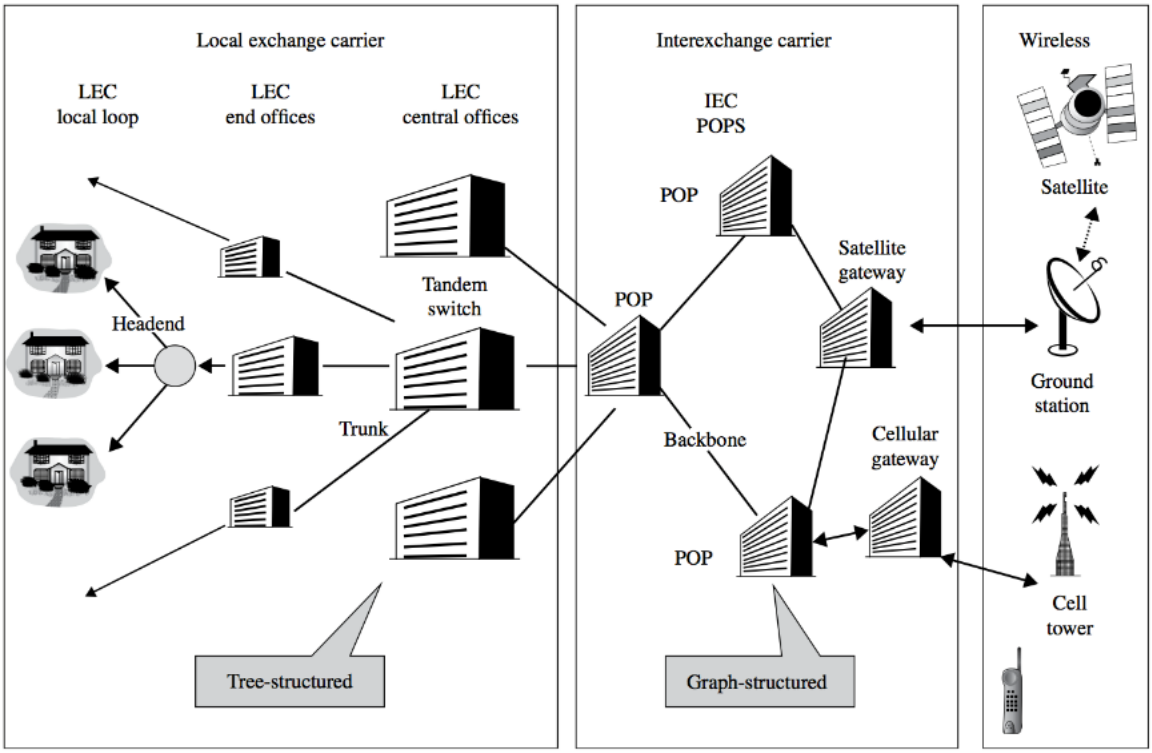


Figure 7- schematic structure of the telecom infrastructure

The following list represents the most likely triggering multi-vulnerability scenarios in telecommunication networks.

- Wind storms affecting mainly aerial, RF, and satellite trunk lines, as well as outside plants and cell towers.
- Ice/snow storms affecting mainly aerial lines and RF links and causing ice to grow on aerial lines, which may crumble under its weight, or whip violently when the wind blows large chunks of ice off the line.
- Flash floods affecting mainly outside plants. The debris flow can affect cell towers and Base Stations.
- Extreme cold waves affecting batteries and the auxiliary generator facilities, outside plant equipment, RF link stations, and in general any switching centre without reliable access to the power grid.
- Extreme heat waves affecting the electronics of outside plants, RF link stations, cell towers, and Base Station Controllers.
- Wild fires affecting aerial trunk lines and RF links, outside plant equipment in residential areas close to forests or dense vegetation.
- Sand storms affecting aerial trunk and backbone lines due to fallen trees.

3.2.1.2 Interdependencies (Network Level)

Land Transport and Energy

According to Deliverable D4.1 (Marin and Halat, 2015) of the RAIN project, the power grid has, for a long time, had quite a low direct dependence on any other critical infrastructure, apart from, of course, that related to the supply of primary sources (mainly oil and gas nuclear plants refuel at 1-2 year intervals). Dependency on transport infrastructure is quite low, and is mainly limited to access for the maintenance crews to distribution equipment. Utility companies have their own special transportation means to reach very remote substations and lines.

Despite the low dependency of energy network on transport infrastructure, transport network, railways in particular, is highly connected to energy network and any disruption in energy supply can result in failure in rail transport network.

Land Transport and Telecommunication

In the event of a long power blackout, the Telecom network becomes interdependent with the Transportation infrastructure, as the diesel generators need to be refuelled.

In cases where there is extensive failure in Road and Rail infrastructures there is consequently an increase in telecommunication congestion as people try to reach emergency services or their relatives. This can eventually result in the collapse of the telecommunication network.

Energy and Telecommunication

According to Deliverable 4.1 (Marin and Halat, 2015) of the RAIN project, the majority of the existing power grids developed in the early 20th century without the benefit of extensive telecommunication networks. This is no longer the case nowadays. Before the 1980s, transmission networks had plenty of transmission capacity margins built in, so that the operation of the system could rely on basic

automatic coordination. In essence, the common frequency of the grid (50Hz in Europe, 60Hz in North America) provided the synchronization and regulation mechanism for all generators, and operators had the time to coordinate further control actions, simply by means of telephone calls to the power plants. The safety margins for operation are now much tighter, and these control decisions must be taken must faster. The operators need to receive their SCADA telemetry via data communications, and their SCADA commands need to actuate immediately. All SCADA systems rely critically on telecommunications. Luckily, the power utilities have always been rather conservative and always preferred to build their own ad-hoc communications lines, in order to be independent of external telecom providers. Many high-voltage lines carry one or more so-called optical ground wire (OPGW) at the top of the pylon, which carries a fibre optic communications line and doubles as grounding wire. Many utilities actually lease these lines to the big telecom companies. However, it is uncertain whether all SCADA systems at power utilities are truly independent from external Telecom providers. It is generally true for transmission-level networks, at least at the highest voltage levels. But as one descends downwards to distribution sections, it becomes more likely to find utilities that lease lines from Telecommunication for SCADA use. Such lines may have guaranteed traffic capacities, but they could be affected by network outages just like the rest of telecom lines.

On the other hand, the telecommunications infrastructure has an intrinsic dependency on the supply of power. All equipment devices consist of electronics, and these need electric power to run. Therefore all switching centres, base stations, satellite downlinks, etc., are retrofitted with backup power. In case the power from the grid goes out, the batteries supply backup power first, with duration that may range from 30 minutes to 8 hours, or even a full day. For long power outages, the diesel backup generator kicks in.

An energy blackout can lead to the saturation of a telecommunications network (Rozel et al., 2008). In fact, the dependence between the electrical and telecommunications networks is increasing (Delamare, Diallo, and Chaudet, 2009) which will then make the emergency services unavailable, increasing the vulnerability of those exposed to hazards (Rozel et al., 2008)

Luiijf et al. (2009) examined a database of failures in 12 Critical Infrastructure sectors and found that, in relation to cascades, the overwhelming majority of them originated in the energy and telecom sectors. A further point of interest in the same research is that 29% of the events in Europe were the result of incidents in other sectors.

Since power grid cuts are a dominant cause of severe network and service outages in the EU's electronic communications sector, all the scenarios affecting energy networks are essentially affecting Telecommunication networks due to close dependencies of Telecommunications to energy infrastructure.

3.2.2. Implementation in risk assessment framework

Much effort is devoted to the development of models and methods capable of analysing interdependent infrastructure systems; Pederson et al. (2006) has conducted a comprehensive overview of methods and models.

An extensive review paper (Ouyang, 2014) groups the infrastructure interaction modelling approaches into six categories

- empirical approaches,
- agent based approaches,
- system dynamics based approaches,
- economic theory based approaches,
- network based approaches, and
- other approaches.

A fundamental characteristic of interdependent networks is that the failure of a node/component in one network may lead to the failure of nodes in another network (Buldyrev et al. 2010). The literature on interdependent infrastructure networks covers a diverse set of networks including transport networks, communication networks, financial transition networks, energy networks, water supply networks, food supply networks and fuel networks.

For infrastructure systems, network theory has been widely used to characterize infrastructure network topology and layout features by taking advantage of closed-form expressions and numerical simulations. For example Wang and Rong (2011) investigate cascading failures induced by the intentional edge attacks in the power grid of the western United States using network modelling techniques. Winkler et al. (2011) also implement this technique and combine power network topology and a component fragility model to study how the network topology affects the reliability of a power system impacted by natural disasters.

In this deliverable, a comprehensive network modelling approach is introduced for modelling different components of vulnerable land, energy and telecommunication networks and their interaction with multi-hazardous events and its implementation into the risk framework which will be applied to specific case studies in Deliverable D6.3. This approach produces a mathematical formalisation of interdependent framework and hence provides a quantitative technique for multi-hazardous and multi-vulnerability risk modes. The outcome of the network modelling will be fed into the risk frameworks in the form of an updated inference network and associated probabilities. In this study, the methodology proposed in Pant et al. (2014) is used to not only model the interdependencies but also take account of system flow redistribution.

The unconditional probability of failure of an individual asset can be calculated by integrating the product of fragility and probability distribution over different intensities of a hazardous event.

$$P[r] = \int_y L(r|y) f_Y(y) dy \qquad \text{Eq.1.}$$

where $f_Y(y)$, is the continuous probability distribution of a hazard, $L(r|y)$, is the fragility function of r, given a hazardous event of y, $(r|y)$, given as $L(r|y) = P[r = 0|y]$, r, representing the state of attributes assigned to an asset, a, which can be a set of attributes such as asset geometry or infrastructure type.

Assuming$D(r,a)$, as the consequence associated with asset failure, the risk is measured as the product of the failure probability of the asset and the consequence incurred due to failure, which is calculated by:

$$R(r) = \int_y L(r|y) f_Y(y) D(r,a) dy = D(r,a) \int_y L(r|y) f_Y(y) dy \quad \text{Eq.2.}$$

An ideal model of a single system of infrastructure assets is a complex network consisting of many sub-systems connected to each other. In this case, the infrastructure network should be defined as a collection of the set of assets given as:

$$A = \{(a_1, r_1), \dots, (a_b, r_b)\} \quad \text{Eq.3.}$$

Then the probability of the infrastructure system in a state of$r^j, j \in \{1, \dots, 2^b\}$, can be calculated as:

$$P[\boldsymbol{r}^j] = \int_y P(\boldsymbol{r}^j|\boldsymbol{y}) f_{\boldsymbol{Y}}(\boldsymbol{y}) dy = \int_y P(r_1^j, \dots, r_b^j|\boldsymbol{y}) f_{\boldsymbol{Y}}(\boldsymbol{y}) dy \quad \text{Eq.4.}$$

Where $P(\boldsymbol{r}^j|\boldsymbol{y})$ is the conditional probability of state $\boldsymbol{r}^j$ given hazard y which captures the product of individual asset state conditional probabilities (i.e., $P(\boldsymbol{r}^j|\boldsymbol{y}) = P(r_1^j, \dots, r_b^j|\boldsymbol{y}) = P[r_1^j|\boldsymbol{y}] \dots P[r_b^j|\boldsymbol{y}]$.

At network level, r^j, will be considered for each individual infrastructure, depending on the scale of modelling, and the effect of interdependencies will be reflected in the form of infrastructure state and associate probability which will eventually feed into the Markovian network.

Failure at asset level and overall network depends upon network attribute assignment, topological characteristics and their mapping to special scales.

Mathematically, a topological network can be represented as a graph with nodes and edges representing their connectivity nature. Given these properties, networks can be represented by $I = \{N, E, M\}$, where N, is the node sets, E, is the edges set and M is a $N \times N$ matrix representing the function of edges to pair-wise nodes. For a network consisting of ν number of nodes and ω number of edges, I is given as:

$$I: \begin{cases} N = \{n_1, \dots, n_v\}, E = \{e_1, \dots, e_\omega\} \\ M = \{e_k \rightarrow (n_i, n_z), \forall\, k \epsilon [1, \omega], i, z \epsilon [1, v]\} \end{cases} \quad \text{Eq.5.}$$

In this network representation, N is a generalised node set that represents a collection of infrastructures that provide and demand different services from each other and subset of N can contain assets having similar characteristics. Different mapping characteristic depending on interdependency function can be captured in the matrix M. In the network mapping, an asset introduced by A can be either presented by N, set of nodes or E, set of edges.

The directional structure of the infrastructure networks provides a set of functional pathways (connecting edges and intermediary nodes) that facilitates service flows from an origin to a destination. Assuming Θ ($\Theta \subset \mathrm{N}$), as all origin nodes and Λ ($\Lambda \subset \mathrm{N}$), as destination, set of functional pathways can be shown by $\xi_{o,d}$, which comprises of unique individual pathways $\xi_{o,id}$ ($\xi_{o,id} \epsilon \xi_{o,d}$) given as:

$$\xi_{o,id} = \{n_o, e_z, \dots, e_l, n_d) \equiv \{a_o, a_z, \dots, a_l, a_d\} \quad \text{Eq.6.}$$

Where n_o is a single origin node and n_d is a single destination node. By assembling all pathways, the redundancy and robustness of the network structure can be explored.

Since the triggering failure state of an infrastructure is either a hazardous event or the interdependencies with another infrastructure, the conditional failure probability can be decomposed as:

$$P\left[r_i^j|\boldsymbol{y}\right] = P\left[r_i^{hi,j} \cup r_i^{in,j}|\boldsymbol{y}\right] = P\left[r_i^{hi,j}|\boldsymbol{y}\right] + P\left[r_i^{in,j}|\boldsymbol{y}\right] - P\left[r_i^{hi,j}\right] \times P\left[r_i^{in,j}|\boldsymbol{y}\right] \quad \text{Eq.7.}$$

Where $r_i^{hi,j}$ denotes the failure state due to hazard and $r_i^{in,j}$ denotes the infrastructure failure state due to connectivity effects. In this equation, $P\left[r_i^{hi,j}|\boldsymbol{y}\right]$ is effectively a measure of fragility when infrastructure is subjected to an extreme weather event. The failure probability due to connectivity, $P\left[r_i^{in,j}|\boldsymbol{y}\right]$, depends upon network topology and the hazard impact and it can be estimated from the failure propagation once network elements fail due to extreme weather event, given as:

$$P\left[r_i^{in,j}|\boldsymbol{y}\right] = P\left[r_i^{in,j} \cap (\boldsymbol{r}^{hi,j}|\boldsymbol{y})\right] = P\left[r_i^{in,j}|\boldsymbol{r}^{hi,j} \cap \boldsymbol{y}\right] P\left[\boldsymbol{r}^{hi,j}|\boldsymbol{y}\right] = P\left[r_i^{in,j}|\boldsymbol{r}^{hi,j}\right] P\left[\boldsymbol{r}^{hi,j}|\boldsymbol{y}\right] \quad \text{Eq.8.}$$

where $P\left[r_i^{in,j}|\boldsymbol{r}_i^{hi,j}\right]$, denotes the conditional dependence of indirect failures on the direct failure mechanism and is derived by considering the number of service paths through the infrastructure a_i in the network before and after direct failure (i.e. failure due to extreme weather event) and can be estimated as:

$$P\left[r_i^{in,j}|\boldsymbol{r}_i^{hi,j}\right] = 1 - \frac{P_i^f(\boldsymbol{r}^{hi,j})}{P_i} \quad \text{Eq.9.}$$

The term $P_i^f(\boldsymbol{r}^{hi,j})$ stands for the number of functional (service) paths through infrastructure a_i after failure set of $\boldsymbol{r}^{hi,j}$ and P_i is the number of paths through the infrastructure before failure. This equation takes account of the bi-directional effect of failure on functionality of infrastructure dependencies and the redistribution of service flow can be incorporated by modifying the functionality matrix.

In the final step, the updated failure state and corresponding probability will be fed into the Markovian risk assessment framework in the vulnerable nodes (critical infrastructure) to quantify the effect of interdependencies.

4. Conclusion

This document presents a summary of multi-mode risk concepts and the main components of multi-mode scenarios and different techniques in implementing risk framework to multi-mode risk scenarios.

First, an overview of multi-mode risk assessment is presented and a comparison is made between single and multi-mode risk frameworks. Then different components (i.e. multi-hazard and multi vulnerability components) of multi-mode risk scenarios are described, and selected scenarios for each component are listed. For each component, the implementation technique in the risk assessment framework is then explained.

It is shown that for multi hazard scenarios there are 9 possible interactions, of which, 7 will be studied as part of the selected case studies. For the multi-vulnerability scenarios, network modelling can be considered as the most appropriate approach to quantify the failure propagation in infrastructure system due to network dependencies and interdependencies.

5. References

Becker, T., Nagel, C., and Kolbe, T. H. 2011. Integrated 3D modeling of multi-utility networks and their interdependencies for critical infrastructure analysis. In *Advances in 3D Geo-Information Sciences, Lecture Notes in Geoinformation and Cartography*.

Buldyrev, S. V, Parshani, R., Paul, G., Stanley, H. E., and Havlin, S. (2010). Catastrophic cascade of failures in interdependent networks. *Nature*, *464*(7291), 1025–8. http://doi.org/10.1038/nature08932.

De Porcellinis, S., Oliva, G., Panzieri, S., and Setola, R. 2009. A HOLISTIC-REDUCTIONISTIC APPROACH FOR MODELING INTERDEPENDENCIES. In *CRITICAL INFRASTRUCTURE PROTECTION III* (pp. 215–227). Springer Berlin.

Delamare, S., Diallo, A.-A., and Chaudet, C. 2009. High-level modelling of critical infrastructures' interdependencies. *Int. J. Critical Infrastructure*, *5*(1/2), 100–119.

Dvorak, D. and 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.

Dudenhoeffer, D. D., Permann, M. R., and Manic, M. 2006. CIMS : A Framework for Infrastructure Interdependency Modeling and Analysis. In L. F. Perrone, F. P. Wieland, J. Liu, B. G. Lawson, D. M. Nicol, and R. M. Fujimoto (Eds.), *Proceedings of the 2006 Winter Simulation Conference*.

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.

Groenemeijer, P. and Becker N. 2015. Past Cases of Extreme Weather Impact on Critical Infrastructure in Europe. Deliverable D2.2, EU funded RAIN project (Risk Analysis of Infrastructure Networks in response to extreme weather), 2014 - 2017, GA no. 608166.

Hajializadeh, D. and Tucker, M. 2015. Quantification of single-mode risks and impacts. Deliverable D6.1, EU funded RAIN project (Risk Analysis of Infrastructure Networks in response to extreme weather), 2014 - 2017, GA no. 608166.

Kappes, M. S., Keiler, M., von Elverfeldt, K., and Glade, T. 2012. Challenges of analyzing multi-hazard risk: a review. *Natural Hazards*, *64*(2), 1925–1958. http://doi.org/10.1007/s11069-012-0294-2

Kumasaki, M., King, M., Arai, M., and Yang, L. 2015. Anatomy of cascading natural disasters in Japan: main modes and linkages. *Natural Hazards*. http://doi.org/10.1007/s11069-015-2028-8

Laprie, J.-C., Kanoun, K., and Kaâniche, M. 2007. Modelling Interdependencies between the Electricity and Information Infrastructures. In F. Saglietti and N. Oster (Eds.), *Computer Safety, Reliability, and Security* (pp. 54–67). Springer Berlin Heidelberg.

Luiijf, E., Nieuwenhuijs, A., Klaver, M., van Eeten, M., and Cruz, E. 2009. Empirical Findings on Critical Infrastructure Dependencies in Europe, 357–365.

Marin, J and 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*

Min, H.-S. J., Beyeler, W., Brown, T., Son, Y. J., and Jones, A. T. 2007. Toward modeling and simulation of critical national infrastructure interdependencies. *IIE Transactions*, *39*, 57–71. http://doi.org/10.1080/07408170600940005

Newman, D. E., Nkei, B., Carreras, B. A., Dobson, I., Lynch, V. E., and Gradney, P. 2005. Risk Assessment in Complex Interacting Infrastructure Systems. In *Proceedings of the 38th Hawaii International Conference on System Sciences* (Vol. 00, pp. 1–10).

Ouyang, M. 2014. Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering and System Safety*, *121*, 43–60. http://doi.org/10.1016/j.ress.2013.06.040

Pant, R., Hall, J., Thacker, S., Barr, S. and D. Alderson. National scale risk analysis of interdependent infrastructure network failure due to extreme hazards, Infrastructure Transitions Research Consortium, EPRS, Engineering and physical #science Research Council.

Peerenboom, J. P., and Fisher, R. E. (2007). Analyzing Cross-Sector Interdependencies. In *Proceedings of the 40th Hawaii International Conference on System Sciences* (pp. 1–9).

Rinaldi, S. M. (2004). Modeling and Simulating Critical Infrastructures and Their Interdependencies. In *Proceedings of the 37th Hawaii International Conference on System Sciences* (pp. 1–8).

Rinaldi, S., Peerenboom, J., and Kelly, T. 2001. Identifying, understanding, and analyzing critical infrastructure interdependencies. *Control Systems, IEEE*, 11–25. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=969131

Rozel, B., Viziteu, M., Caire, R., Hadjsaid, N., and Rognon, J. 2008. Towards a common model for studying critical infrastructure interdependencies. *Power and Energy …*, 1–6. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4596465

van Westen, C. J., Montoya, L., Boerboom, L., and Badilla Coto, E. (n.d.). MULTI-HAZARD RISK ASSESSMENT USING GIS IN URBAN AREAS : A CASE STUDY FOR THE CITY OF TURRIALBA , COSTA RICA. *Hazard Mapping and Risk Assessment*, 53–72.

Wang, J.W. and Rong L.L. 2011 Robustness of the western United States power grid under edge attack strategies due to cascading failures, Saf. Sci. 49, 807–812

Wang, S., Hong, L., and Chen, X. 2012. Vulnerability analysis of interdependent infrastructure systems: A methodological framework. *Physica A: Statistical Mechanics and Its Applications*, *391*(11), 3323–3335. http://doi.org/10.1016/j.physa.2011.12.043

Winkler.J., Dueñas-Osorio, L., Stein, R. and Subramanian, D. 2011. Interface network models for complex urban infrastructure systems, J. Infrastruct. Syst. 17 (4) 138–150.

Zimmerman, R. 2001. Social Implications of Infrastructure Network Interactions. *Journal of Urban Technology*, *8*(3), 97–119. http://doi.org/10.1080/106307301753430764

Zimmerman, R. 2004. Decision-making and the vulnerability of interdependent critical infrastructure.

In W. Thissen, P. Wieringa, M. Pantic, and M. Ludema (Eds.), *Proceedings of IEEE International Conference on Systems, Man and Cybernetics*. Delft University of Technology, The Hague, The Neterlands. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1401166

Zimmerman, R., and Restrepo, C. 2006. The next step: quantifying infrastructure interdependencies to improve security. *International Journal of Critical Infrastructures*, *2*(2/3), 215–230. Retrieved from http://www.inderscienceonline.com/doi/abs/10.1504/IJCIS.2006.009439