EU-CIRCLE

A pan-European framework for strengthening Critical Infrastructure resilience to climate change

D3.4 Holistic CI Climate Hazard Risk Assessment Framework

Contractual Delivery Date: 31/05/2016	**Actual Delivery Date**: 07/10/2016
Type: Document	**Version**: V1.0

Dissemination Level [Public] Deliverable

Statement

EU-CIRCLE advances the state-of-the art through a general risk assessment framework that can be used to examine the risk of damage to critical infrastructure under the increasing stress of climate change and associated climate hazards. The holistic approach consideres also secondary impacts to society, economy and environment that emerge as consequences of critical infrastructure disruptions.

EU-CIRCLE is a project that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653824. Please see http://www.eu-circle.eu/for more information.

Preparation Slip			
	Name	Partner	Date
From	Ralf Hedel	Fraunhofer	24/06/2016
Reviewer	Round 1 of open review from the consortium	All	12-22/07/2016
Reviewer	Round 2 of open reviews from the consortium	All	19-28/09/2016
For delivery	Thanasis Sfetsos	NCSRD	4/10/2016

Document Log			
Issue	Date	Comment	Author / Organization
V0.1	10/11/2015	ToC changed after comments by EU-CIRCLE partners, harmonisation with WP 1	R. Hedel (Fraunhofer)
V0.2	05/01/2016	ToC modified	Ralf Hedel
	20/04/2016	Inclusion of impact assessment models, Introduction of approach to infrastructure registry	L. Shakou (EUC) K. Kołowrocki (GMU)
	26/04/2016	Re-organisation of chapters after discussion with EUC	R. Hedel (Fraunhofer)
V0.3	20/05/2016	Risk management steps described	R. Hedel (Fraunhofer)
V0.4	15/06/2016	Extension of ToC, New chapters integrated based on Consolidation workshop result	T. Sfetsos and A.Eleftheriadou (NCSRD)
V0.45	07/07/2016	Content extended, pre-final draft send out	R. Hedel and T. Sfetsos
V0.5	18/07/2016	Integration of changes from EUC, EXETER and GMU	R. Hedel
V0.7	19/07/2016	Integration of changes through NCSRD (Chapter 3)	T. Sfetsos
V1.0	29/09/2016	Finalisation after second open review round	R. Hedel and T. Sfetsos

Executive Summary

This deliverable presents approaches for risk assessment and risk management as they have been developed and established in European Countries and beyond.

On the base of that, it develops a general framework for the assessment of the risks of failures in critical infrastructures as a result of climate hazards. This general framework includes a selection of approaches for describing and modelling of:

- assets,
- dependencies and interconnections between them,
- assessment of failure impacts,
- propagation of risks through networks,
- uncertainties.

On the base of scientifically validated and well established approaches, we suggest a sequence of the following steps for the holistic risk assessment:

1) Scenario development,
2) Critical infrastructure network topology and description,
3) Structural and Operational analysis,
4) Network analysis, taking into account interconnectivity and resilience characteristics and
5) Holistic impact analysis

For each step, the deliverable provides general guidance. Also, this deliverable describes the relevant categories of impacts, approaches to handle and process scenario data and to deal with uncertainty.

The selected approaches are suitable to conduct the case study analysis foreseen within EU-CIRCLE but also, they are considered to be of relevance to many other assessment challenges.

The approaches are described in a more generic format. A more detailed documentation is subject to following deliverables, especially D3.5, taking into consideration the recommendations of the EU-CIRCLE case studies and the interactions / recommendations of the end-user community.

This deliverable recaps the case studies and describes the analytical questions which are in the focus, discussing how the proposed framework is flexible and adaptable and therefore suitable for the specificities and characteristics of each.

Finally, the deliverable discusses aspects of data exchange and data transformation in preparation of conduction of the case studies and development of the EU-CIRCLE CIRP platform.

Contents

List of domain specific, frequently used abbreviations

AAL	Average Annual Loss
CC	Climate Change
CI	Critical Infrastructure
CI/KR	Critical Infrastucture / Key Resource
CIP	Critical Infrastructure Protection
ECI	European Critical Infrastructure
GIS	Geographic Information Systems
LP-HC	Low Probability-High Consequence
NRA	National Risk Assessment
PML	Probable Maximum Loss
RA	Risk Assessment
RVA	Risk and Vulnerability Analysis

1 Introduction

Within the EU-CIRCLE project, a framework and platform for analysis, design and modelling scenarios for any kind of climate hazards and CI will be developed. It will allow users to define and examine their individual infrastructure‘s resilience.

One objective of the deliverable is to provide a general description on the steps and thus the entire process to assess and manage the risk for any critical infrastructure and climate hazard.

Risk assessment is one of the procedural step within the overarching risk management concept. An explanation of risk management and risk assessment - is of highest relevance at this early stage of the project since these steps must be facilitated by the EU-CIRCLE CIRP and SimICI. These software platforms will be developed in subsequent stages of the EU-CIRCLE project and will support end-users to examine the risks within their critical infrastructures and evaluate strategies.

Work package 3 provides the basis for this implementation, namely to describe the methodological approaches for:

- Modelling of CIs, connections and interdependencies,
- Handling of uncertainties
- Assessing likelihoods of failures
- Modelling risks and risk propagation
- Assessing the consequences

In this first version of the deliverable, a generic framework is proposed that will be valid throughout the project. As the present deliverable D3.4 has to be developed at an early stage of the project, the explanation will focus on the fundamental concept and is rather genderic. Deliverable D3.4 amends the traditional understanding of risk management and risk assessment with the aspects associated to the concept of resilience.

Within the second version of this deliverable (D3.5, M33), a more detailed description on the aspects introduced within D3.4 will be provided and additional topics will be covered as well, such as: explicit handling of uncertainties, translation of risk metrics. More details on specific topics introduced in D3.4 will be reported in deliverables of WP 3, namely:

- D3.1: Registry with CI assets (M22)
- D3.2: Report of climate related critical event parameters (M31)
- D3.3: Inventory of CI impact assessment models (M32)
- D3.6. Risk model metadata (M33)

1.1 Working methodology

This deliverable is a joint effort of multiple partners working mainly in WP 3, with contributions from colleagues working on further work packages. The workings steps undertaken to develop this deliverable are the following:

- literature study on frameworks for risk assessment, mainly from the following sources:
    - International standards
    - Description of programmes implemented by cities, regions, nations
    - Meta studies on risk assessment and risk management approaches
- extensive discussion among the WP 3 partners on the suitability, pros and cons of framework approaches

- distillation of most common approach deployed for risk management and preparation of draft framework description
- amendment of classical risk management procedure by aspects introduced with resilience
- extensive discussion with partners involved in WP 5 and 6
- presentation of risk management approach during the consolidation workshop (May 2016, Milano)
- rework, review and finalization of framework description.

This deliverable (D3.4) provides the general background, explains and suggests possible solutions to the end-users. Though, throughout the project, especially in the validation activities (case studies etc.) the approaches will be further discussed, developed and evaluated.

In the 2nd version of this deliverable, D3.5 “Holistic CI Climate Hazard Risk Assessment Framework V2.0”, any possible changes that will be proposed by the EU-CIRCLE stakeholders and also a detailed description of the network analysis models that will be introduced in the CIRP. Additionally, as this Deliverable will be ready after the execution of the 2nd case study, recommendations and suggestions for determining the risk components from the different impact categories will be introduced.

This Deliverable, as a focal one within the project, has been subject to **two open reviews from the entire consortium** which delayed the submission. This enabled partners to meaningfully contribute to its development through numerous suggestions and recommendations. As EU-CIRCLE deals with a research domain that is very broad, specific elements from the nature, characteristics and properties of each CI and the climatology domain where introduced into the proposed generic approach, and required several interactions with the entire consortium to reach the final version.

1.2 Links to other WP

This development takes into consideration the first findings of the work within other work packages, especially from WP 1:

- D1.1:introduces a definition for “risk assessment” as “a methodology to determine the nature and extent of risk by analysing potential hazards and evaluating existing conditions of vulnerability that together could potentially harm exposed people, property, services, livelihoods and the environment on which they depend.” (M3)
- D1.2: introduces into objectives of risk assessment and approaches from various countries. This deliverable provides also a state of the art review and taxonomy of existing knowledge (M12 - this deliverable had to be submitted at exactly the same project months as D3.4, therefore a final version was not available during the writing of D3.4)
- D1.3 introduces to the strategic context which needs to be considered in assessment of risks (M6)
- D1.4, which reports on the methodological framework (M11)

Furthermore, this deliverable is linked with D4.1 in WP4, which defines resilience, provides a resilience framework, defines its constitutent parts and furthermore explains the relation between risk management and resilience. The adaptation framework (D4.5) is also related to the development of D3.4 to reduce the risk and to improve resilience.

Partners involved in WP 5 and 6 were consulted to discuss the appropriateness of the proposed generic framework to the development of the EU-CIRCLE technologies CIRP and SimICI and the Case studies.

1.3 Structure of the deliverable

After a short introduction in section 1, we introduce in Chapter 2 approaches for risk management and risk asssemment, established in Europe and abroad. In Chapter 3 we describe the current understanding of risk management and components of risk assessment within the EU-CIRCLE consortium which will serve as the baseline for further developments. Chapter 4 updates on the case studies. For their conductin, data preparation are needed. Therefore, Chapter 5 introduces briefly ways of data exchange and transformation. Chapter 5 concludes this deliverable with final remarks.

2 State-of-the-art risk management and risk assessment

2.1 CI Risk assessment in the context of climate change

Climate change amplifies existing risks and create new risks for natural and human systems. Risk of climate-related impacts results from the interaction of climate-related hazards (including hazardous events and trends) with the vulnerability and exposure of human and natural systems, including their ability to adapt. Some risks are particularly relevant for individual regions, while others are global.

Risk management is considered as a fundamental strategies. One of the key strategic activities of risk management is the risk assessment which requires the use of reliable methodologies to allow for an adequate calculation of probabilistic losses of exposed elements.

Risk assessment constitutes an essential path for identifying threats, assessing vulnerabilities and evaluaing the impact(s) on assets, infrastructures or systems whilst concurrently taking into account the probability of the occurrence of these threats. Numerous risk assessment methodologies exist for critical infrastructures.

Risk is often defined as the likelihood of provoking harm, or the probability that some type of injury or loss would result from the hazard event. Several expressions have been proposed in order to define risk such as:

Jones & Boer (2003)*:* *Risk = probability x consequense*
UNDP 2004 (Wisener, et al., 2003): *Risk = hazard × vulnerability*
Crichton (1999): *Risk = hazard × exposure ×vulnerability*
Davidson (1997): *Risk = hazard × exposure × vulnerability × capacity measures*
Villagran de Leon (2004)*:* *Risk = hazard ×vulnerability × deficiency in preparedeness*

The probability and severity of the hazard are obviously not the only factors that affect risk. Risk also depends on the exposure to the hazard and how vulnerable it is to damage (Fedeski & Gwilliam (2007), Crichton (2001)). Risk is assessed as a combination of threat (expressed as the probability that a given action, attack, or incident will occur), vulnerability (expressed as the probability that a given attack, or vulnerability will succeed, given that the action, attack or incident occurs), and consequence (expressed as some measure of loss, such as dollar cost, resources loss, programmatic impact, etc.).

The overall risks of future climate change impacts can be reduced by limiting the rate and magnitude of climate change. The exact levels of climate change that will result in irreversible change remain uncertain, but the risk associated with crossing such thresholds increases with rising temperatures. For risk assessment, it is important to evaluate the widest possible range of impacts, including low-probability outcomes with large consequences.

There is a significant number of risk assessment methodologies for critical infrastructures basically based the scope of the methodology, the audience to which it is addressed and their domain of applicability. A complete Risk Assessment Framework for Critical Infrastructures climate includes typically:

1. Hazard characterization (type, extent, intensity, probability, thresholds, time period),
2. Vulnerability Assessment (Exposure – extent and value, identification of CI, identification

of interdependencies, how prone CI are to the specific hazard thus definition of damage states & probability of exceedance),

3. Impact Analysis (Type of impacts: *Societal*: Fatalities, Injuries; *Security*: Fresh Water Supply, Food Supply, Energy Supply; *Economic*: Cost of Repair/Replacement, Cost of Labour, Availability of Materials Age of the Existing Infrastructure, Weighted indexes for each impact, Interconnections, Cascading effects) and
4. Risk Assessment (Risk scenarios, probability methods, direct/indirect outputs for specified CI, time response: micro/macro scale, recovery and resilience).

Assessments are either qualitative in their approach or they are quantitative providing numerical estimates of population exposures and rankings of vulnerability. They can be single hazard or multi-hazard and they can range from local place-specific analyses to more regionally based patterns.

Most quantitative climate change risk assessments developed at the urban and sub-urban scales rely on the availability of accurate information on potential climate change hazards, information usually derived from General Circulation Models (GCM). These models are regionalised by means of dynamic or statistical downscaling techniques. Hazard information at the local level can be expressed as probabilistic distributions of climate events characterised in terms of return periods and intensities of occurrence. The underlying data needed to produce probabilistic distributions of climatic events under climate change scenarios are not always available at the local level. Even if hazard information is available, accurate cost estimates linked to specific clima te change threats are difficult to assess in the face of social and economic vulnerability factors.

The vulnerability assessment deals mainly with the quantification of damage of each element at risk, using appropriate fragility functions. Given the spatial distribution of the characteristics of hazard, loss scenarios for buildings, utility and transportation systems, critical facilities and strategic buildings are produced, using inventory data and adequate fragility relationships.

Potential losses are frequently communicated as ‘damage’ or ‘vulnerability functions’. Loss estimates including direct and indirect losses, depend on the inventory and typology classification of the elements at risk, the vulnerability models and the existing interactions between lifeline components. The creation of an inventory is an essential step to identify, characterize and classify all types of lifeline elements, according to their specific typology and their distinctive geometric, structural and functional features.

For probabilistic disaster risk assessment, the vulnerability of exposed elements is assessed using functions that relate the intensity of the phenomenon that the hazard represents to the mean damage ratio or relative direct physical impact. Vulnerability functions and they must be estimated for each one of the construction classes, so that a particular vulnerability function can be assigned to each one of the components in the exposure database. Each vulnerability function is characterized by a value known as the mean damage ratio (MDR) and its corresponding variance for each level of hazard intensity. That enables estimating the loss probability function at each level of intensity for the hazards under study (CIMNE, 2013).

Although some works provide solid estimates on the potential impacts of climate-driven events, most of them rely on a limited number of dimensions that are directly linked to the physical characteristics of the events themselves, such as e.g. flood extension, depth and velocity in the case of floods, as well as to the structural characteristics of the building stock, like e.g. houses with lowest floor below ground level retrieved from remote sensing data or similar tools. Still, damage cost assessments derived from these calculations can also be quite context-specific, undermining comparability across spatial units.

The impact of the disaster caused by a natural hazard on a system evolves with time elapsed from the event and in space. In the aftermath of the event, the damaged infrastructure operates in a state of emergency, and only progressively returns to the previous or a different state of normal functionality. Correspondingly, the spatial extent of interest to the study of the infrastructure response increases, involving adjacent regions in the economic recovery phase and multiple interactions between systems and with the built environment (Kyriazis, et al., 2011).

A Single-risk assessment refers to the single risk (i.e. likelihood and consequences) of a singular hazard (e.g. flood) occurring in a particular geographic area during a given period of time. Multi-risk assessments refers to the total risk from several hazards either occurring at the same time or following each other because they are dependent from one another or because they are caused by the same triggering event or hazard; or merely threatening the same elements at risk (vulnerable/ exposed elements) without chronological coincidence (European Commission, 2010).

CI risk assessment methodologies can be divided in these major categories:

- Sectoral methodologies, whereby each sector is treated separately with its own risks and ranking; and methodologies taking a systems
- Systems approaches, that assess the critical infrastructures as an interconnected network. Methodologies belonging to the second category are rather limited.

The vast majority of the existing work has been sectoral and mostly at asset level. Some methodologies have then been extended to cope with networked systems.

Methodologies developed for certain assets are well defined. However, methodologies that aim at assessing risks at a higher level e.g. networked systems require further refinement (Giannopoulos, et al., 2012). Not only direct impacts on infrastructure must be considered, instead, also "second order" impacts within one infrastructural sector or to connected infrastructure. In this respect, we also introduce to the concept of "domino" or"cascading" effects. Cascading impacts are "second order" impacts that appear as a consequence of dependent (such as tree-like) structures

2.2 European and international frameworks

2.2.1 European Directive 114/2008

The European Programme for Critical Infrastructure Protection (EPCIP) is the main tool to implement the Directive 114/2008 on "the identification and designation of European Critical Infrastructures and assessment of the need to improve their protection" in the member states (MS) of the EU (European Commission, 2008). It encompasses several instruments for the protection of critical infrastructures in Europe. First of all a definition of **Critical Infrastructure** (CI) as an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions. Furthermore, the directive aims to identify and designate **European Critical Infrastructures** (ECI). In a first step, the priority is on energy (electricity, oil, gas) and transport sector. The identification of European Critical Infrastructures has to be carried out taking account of the following impact criteria (Theocharidou & Giannopoulos, 2015):
1) casualties criterion (assessed in terms of potential number of fatalities or injuries),

2) economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects),
3) public effects criterion (assessed in terms of the impact of public confidence, public health and disruption of daily life; including the loss of essential services).

The identification and designation process follows a 4-step procedure that is based on the sectoral and the cross-cutting criteria (CCC).

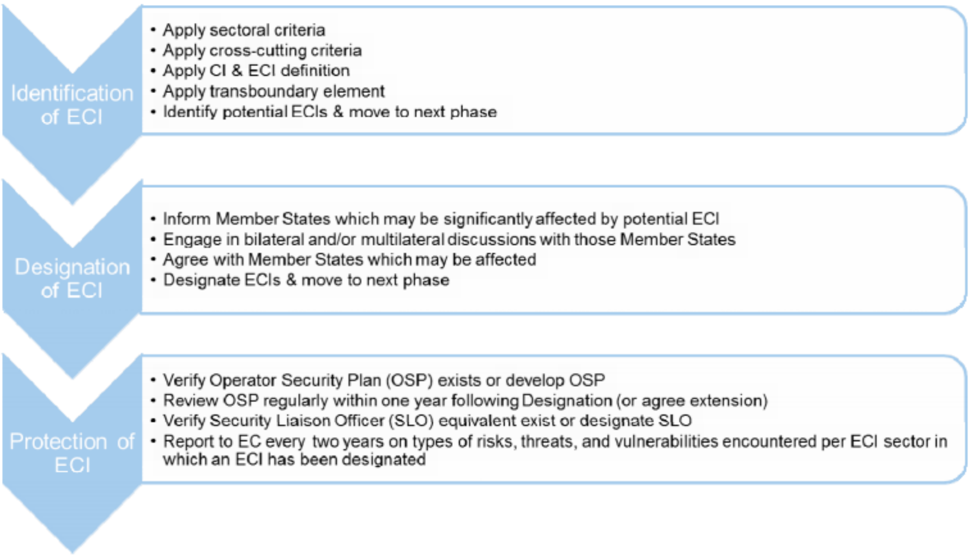


Figure 1: Phases concept of Directive 114/2008.

All Member States must adopt a four-step process according to Annex III to the Directive (EC, 2012) and apply sectoral criteria to identify ECIs in the two sectors. The next step is to confirm that the identified CIs meet the definition of ‘critical infrastructure’ in Article 2(a) of the Directive. The Directive then suggests evaluating the impact of any disruption to the identified CIs on other Member States. This can be done by applying either the CCC, which specify thresholds to assess the general effects of CI disruption, such as the number of casualties, economic effects or public effects, or the national equivalent of such criteria. This impact evaluation should factor in alternatives and disruption/recovery time. The Directive also requires the relevant Member States to engage in negotiations leading to the designation of ECIs. Once an ECI is identified, the Directive requires a specific set of actions to be taken by its owners/operators in order to develop an Operator Security Plan (OSP) documenting critical assets and security measures. The Directive makes the Member State authorities responsible for ensuring that ECIs comply with its requirements. Most Member States have applied the sectoral criteria, with a few making adjustments and adaptations to align them with an existing national approach. Some Member States have assigned responsibility for determining the sectoral criteria to the ministries or sectoral regulators concerned.

According to Article 7(2) of the Directive Member States must regularly report to the Commission on the types of risks, threats and vulnerabilities for those sectors where ECIs have been designated. Member States have delivered first assessments for such sectors. In addition, risk assessment must be conducted within the context of an Operator Security Plan for a designated ECI.

For more complex systems, including the interaction of cyber and physical layers, the boundaries of the sectors are not clearly defined, so it is often rather difficult to classify a certain infrastructure within sectoral limits. This reflects the complex interconnectivity of infrastructures for the delivery of vital societal services.

2.2.2 European strategy on Climate Adaptation

Adaptation and mitigation are complementary actions that contribute to resilience, and both constitute EU priority areas for tackling climate change. Adaptation has the ability to support policy objectives, such as the 'Europe 2020 — Europe's growth strategy' (European Commission, 2013). According to the European Environmental Agency (EEA) report 2013:

- Adaptation of both natural and human systems is already taking place across Europe.
- Sixteen EEA member countries have developed national adaptation strategies and some of these countries already have action plans in place. National adaptation strategies address primarily the water, agriculture and forestry, biodiversity, and human health sectors. Twelve additional EEA member countries are currently preparing a national adaptation strategy, and 15 in total have already established web portals. Some transnational regions (such as the Danube, the Baltic, the Alps and the Pyrenees) and cities have developed adaptation strategies or are currently developing them.
- At EU level, instruments for implementing adaptation policy include key mechanisms such as cohesion funds, agriculture funds, and infrastructure funds, as well as funds from the LIFE+ programme. These are critical to integrate adaptation into EU policy — a process known as 'mainstreaming' of adaptation.
- The European Climate Adaptation Platform (Climate-ADAPT, http://climate-adapt. eea.europa.eu) is an important source of information on adaptation in Europe. It supports stakeholders at all levels of governance by sharing a broad set of information on climate change risks, EU sector policies, adaptation practices, national initiatives, and decision support tools. Climate ADAPT includes key results of EU research, INTERREG and ESPON projects that have strengthened the EU's knowledge base on adaptation.
- The assessment of the costs and benefits of adaptation actions — at European, member country, and local levels — is an emerging field of work. Limited information on costs and benefits is available at present, and this information has to be considered with care as there is still much work to be done on improving assessment methods.

Implementation of the EU Adaptation Strategy is based on eight actions (European Commission, 2013):

- Encourage all Member States to adopt comprehensive adaptation strategies:
  - As part of the Adaptation Strategy package the Commission has provided guidelines to help Member States formulate adaptation strategies.
  - The Commission will develop an ‘adaptation preparedness scoreboard’, identifying key indicators for measuring MS’ level of readiness.
  - In 2017, the Commission will assess whether action being taken in MS is sufficient. If progress deems insufficient, the Commission will consider proposing a legally binding instrument.
- Provide LIFE funding to support capacity building and step up adaptation action in Europe (2014-2020):
  - A climate-action sub-programme will be created under the 2014-2020 LIFE funding programme for the environment. This will substantially increase the LIFE funds available to combat climate change.

    - Priority vulnerable areas have been identified to steer discussions with Member States on the 2014-2020 LIFE work programme.
- Introduce adaptation in the Covenant of Mayors framework (2013/2014):
    - The Commission, supports adaptation in cities. It will do this in particular by launching an initiative, based on the model of the Covenant of Mayors, through which local authorities can make a voluntary commitment to adopt local adaptation strategies and awareness-raising activities.
- Bridge the knowledge gap:
    - The Commission will work further with Member States and stakeholders to identify adaptation knowledge gaps and the relevant tools and methodologies to address them. The findings will be fed into the programming of Horizon 2020 and will address the need for better interfaces between science, policy making and business.
    - The Commission will promote EU-wide vulnerability assessments, taking into account, inter alia, the cross-sectoral EU overview of natural and manmade risks that it will produce in 2013. It will in particular support the Joint Research Centre in its work on estimating the implications of climate change and undertake a comprehensive review of what global climate change will mean for the EU.
- Further develop Climate-ADAPT:
    - as the ‘one-stop shop’ for adaptation information in Europe.
    - The Commission and the European Environment Agency will improve access to information and develop interaction between Climate-ADAPT and other relevant platforms, including national and local adaptation portals.
    - Special attention will be given to cost-benefit assessments of different policy experiences and to innovative funding, through closer interaction with regional and local authorities and financial institutions.
    - Work on the inclusion of the future Copernicus climate services (GMES – Global Monitoring for Environment and Security).
- Facilitate the climate-proofing of the Common Agricultural Policy (CAP), the Cohesion Policy and the Common Fisheries Policy (CFP):
    - As part of the Adaptation Strategy package the Commission has provided guidance on how to further integrate adaptation into the CAP, the Cohesion Policy and the CFP. This guidance aims to help managing authorities and other stakeholders involved in programme design, development and implementation during the 2014-2020 budget period.
    - Member States and regions can also use funding under the 2014-2020 Cohesion Policy and CAP to address knowledge gaps, to invest in the necessary analyses, risk assessments and tools, and to build up capacities for adaptation.
- Ensuring more resilient infrastructure:
    - In 2013 the Commission launched a mandate for European standardisation organisations to start mapping industry-relevant standards in the area of energy, transport and buildings and to identify standards that need to be revised to achieve better inclusion of adaptation considerations.
    - The Adaptation Strategy package provides guidelines to help project developers working on infrastructure and physical assets to climate-proof vulnerable investments.
    - Drawing on the results of its Communication on Green Infrastructure, adopted in May 2013, the Commission will explore the need to provide additional guidance for

authorities and decision makers, civil society, private business and conservation practitioners to ensure the full mobilisation of ecosystem based approaches to adaptation.

- Promote insurance and other financial products for resilient investment and business decisions:
  - The Green Paper on the insurance of natural and man-made disasters, adopted as part of the Adaptation Strategy package, is a first step towards encouraging insurers to improve the way they help to manage climate change risks. A report on the results of the public consultation associated with the Green Paper has been published.
  - The Commission’s aim is to improve the market penetration of natural disaster insurance and to unleash the full potential of insurance pricing and other financial products for risk-awareness prevention and mitigation and for long-term resilience in investment and business decisions (2014-2015). A process has been launched to increase involvement of the insurance and financial sector. The results of this exercise will be disseminated via Climate-ADAPT in particular.

2.2.3 Intergovernmental Panel on Climate Change

The conceptual framework proposed by the Intergovernmental Panel on Climate Change (IPCC) on the WGII AR5 (IPCC, 2014) identifies three core components of climate change –driven *risk*, namely *hazard*, *exposure* and *vulnerability*: “risk results from the interaction of vulnerability, exposure, and hazard” (IPCC, 2014, glossary). Further, ‘risk’ refers to the potential for adverse effects on lives, livelihoods, health status, economic, social and cultural assets, services (including environmental), and infrastructure due to uncertain states of the world.

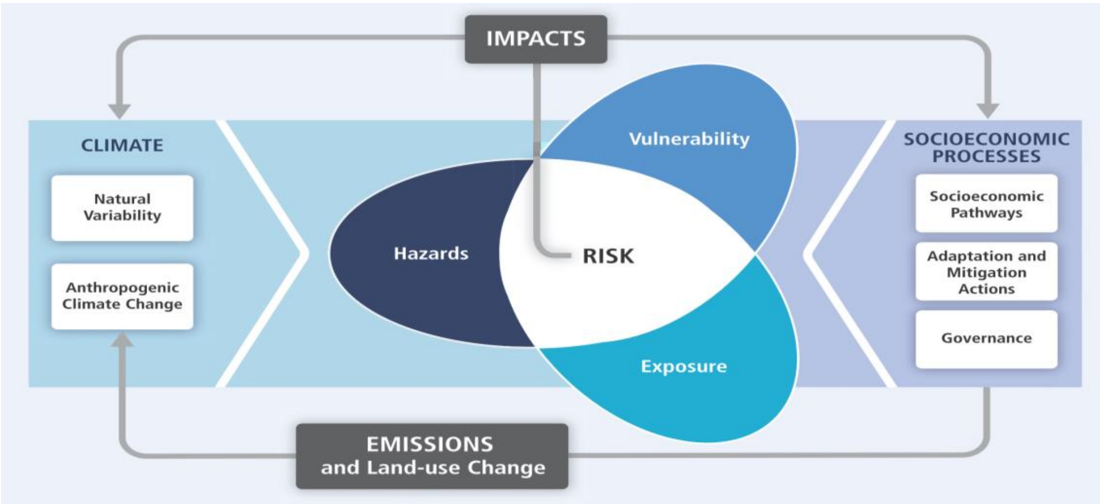


Figure 2: Conceptual framework of IPCC.

Estimates of the likelihood of its occurrence and its resulting consequences will be evaluated by experts after the analysis and understanding of the characteristics of a specific event. Defining risk and uncertainty and their relevant metrics is the first step. The next step is defining the choices with respect to climate change policy options regarding risk and uncertainty. The action and plans undertaken by individuals in relation to climate change policy options under conditions of risk and uncertainty differ and range from long-term global temperature targets to lifestyle choices (IPCC, 2014).

Key risks that span sectors and regions include the following (high confidence): 1. Risk of severe ill-health and disrupted livelihoods resulting from storm surges, sea level rise and coastal flooding; inland flooding in some urban regions; and periods of extreme heat. 2. Systemic risks due to extreme weather events leading to breakdown of infrastructure networks and critical services. 3. Risk of food and water insecurity and loss of rural livelihoods and income, particularly for poorer populations. 4. Risk of loss of ecosystems, biodiversity and ecosystem goods, functions and services.

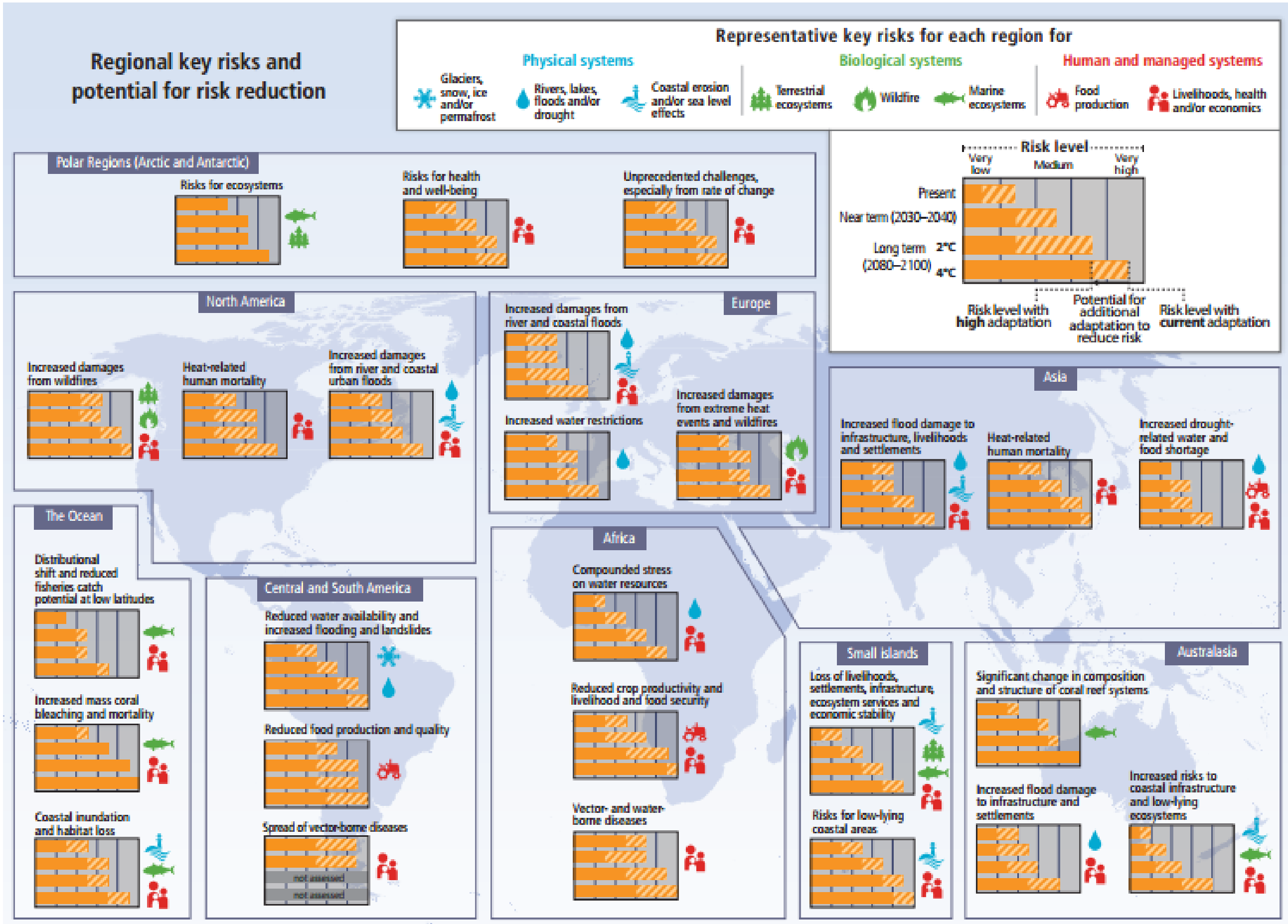


Figure 3: IPCC Regional key risks and potential for risk reduction (*WGII* SPM Assessment Box SPM.2 Table 1).

IPCC recommends the following process for decision making: 1) Define a set of possible decision. 2) Quantify uncertainties on possible states of the world. 3) Value possible outcomes of the decision alternatives as utilities. 4) Choose the alternative with the highest expected utility.

Uncertainty is explecitely addressed. The Guidance Note for Lead Authors of the IPCC Fifth Assessment Report on Consistent Treatment of Uncertainties summarizes alternative ways of representing uncertainty (IPCC, 2014), among them probability density functions and parameter intervals.

The natural hazard framework conceptualizes vulnerability as the response relationship between an exogenous hazard to a system and its adverse effects. This terminology of vulnerability corresponds most closely to the element “sensitivity” in the IPCC terminology. The principal difference between the natural hazards risk-based approach and the IPCC biophysical vulnerability approach is that risk is generally described in terms of probability, whereas the IPCC and the climate change community in general tend to describe (biophysical) vulnerability as a function of certain variables. However, the core of both biophysical vulnerability and risk are essentially the same - hazard and social vulnerability. The element “hazard” is described by as having “varying degrees of intensity and severity” and refers to statistical likelihoods of hazards obtained from long records. These represent a probabilistic view of the uncertain future. On the other hand, probabilities of climate projections are almost absent in the climate change community where the description of impact uncertainty is considered more important.

2.2.4 United Nations International Strategy for Disaster Reduction

UNISDR has spearheaded since 2011 a multi-hazard Global Risk Assessment in partnership with leading scientific and technical organizations in order to provide comparable open-access disaster risk metrics across countries and hazard categories. In the UNISDR assessment, probabilistic hazard models have been developed for earthquake, tropical cyclone wind and storm surge, tsunami and river flooding worldwide, for volcanic ash in the Asia-Pacific region and for drought in parts of Africa.

A global exposure model for the built environment has been developed at a 1km x 1km resolution along coastlines and 5km x 5km elsewhere. On the base of expert knowledge, vulnerability functions have been developed for each region.

The open-source multi-hazard risk platform CAPRA is used to calculate risk. Average annual loss (AAL) is often used in order to describe the results of probabilistic risk models (UNISDR, 2015). The AAL is the average expected loss annualized over a long time frame representing the amount that countries would have to set aside each year to cover the cost of future disasters in the disaster risk management field. The AAL has been calculated as part of the new Global Risk Assessment providing worldwide coverage for multiple hazards.

An increasing number of risk assessments are now being produced for specific hazards and portfolios of exposed assets. However, up to now it has been difficult to estimate global disaster risk due to major geographical gaps and the fact that global assessments for single hazards use different data sets and methodologies. The application of a harmonized risk assessment methodology would facilitate comparisons of risk levels between countries and regions and across hazard types and would enable for a better understanding of the order of magnitude of losses in each country.

The global AAL data illustrates how disaster risk is distributed across countries, income groups, geographical regions and hazard types. Thus, it is appropriate for ranking and comparing country risk levels. However, it is not appropriate for the development of detailed national or local disaster risk management strategies, including risk financing subjects. The AAL can be used by governments and policy makers to provide an initial risk profile for a country motivating the development of detailed assessments in specific sectors and territories as a basis for public and private investment strategies and for the design of risk financing projects.

The global AAL is extremely conservative for three reasons. First, it does not include all hazards and relevant sectors. Furthermore, it only represents direct physical risk to residential and commercial buildings, schools, hospitals and other public and industrial buildings. It does not include risks to infrastructure such as roads and bridges, ports and airports, energy and electrical facilities, telecommunication facilities, dams and mines, or to agriculture. At the same time, it only includes a selection of potential global hazards. If the risk of extra-tropical windstorms, ice and snow, sandstorms and tornadoes were also taken into account, the figure would again be significantly higher. Second, extensive risk, associated with smallscale, high frequency localised events is not considered. The analysis of 85 national disaster loss data sets show that this risk layer may account for up to 40 per cent of economic losses, particularly in low and middle income countries. Third, AAL does not consider indirect losses and impacts. While it is difficult to calculate a global value, evidence from specific countries shows that these indirect losses can surpass the direct costs, particularly if economic resilience is low. When compared to reference income without a disaster, impacts from large disasters can lead to income (GDP) reductions of up to 20 per cent over a number of years following a devastating event.

Unlike historical estimates, AAL takes into account all the disasters that could occur in the future, including very intensive losses over long return periods, and thus overcomes the limitations associated with estimates derived from historical disaster loss data. The other metric presented is probable maximum loss (PML), which represents the maximum loss that could be expected within a given period of time. Typically, PML is relevant to determine the size of reserves that, for example, insurance companies or a government should have available to buffer losses.

In 2015, the Sendai framework was adopted by UNISDR (UNISDR, 2015). It builds upon the Hyogo Framwork for action from 2005 (ISDR, 2005) well as the Yokohama Strategy for a Safer World from 1994 (UNISDR, 1994). It provides a general framwework to increase resilience for disaster risk reduction at all levels (local, regional, national and beyond). The non-binding agreement sees main responsibility for risk reduction at the national states but suggests that other stakeholders should be involved also, such as local goverrments, civil society, volunteers, etc. The framework provides concrete guiding principles to achieve improvements in seven global development objectives within the time period 2015 to 2030. One of the objectives is particularily related to EU-CIRCLE: *"Substantially reduce disaster damage to critical infrastructure and disruption of basic services, among them health and educational facilities, including through developing their resilience by 2030"*. The four top priority actions of the Sendai framework are the following:

- Priority 1: Understanding disaster risk.
- Priority 2: Strengthening disaster risk governance to manage disaster risk.
- Priority 3: Investing in disaster risk reduction for resilience.
- Priority 4: Enhancing disaster preparedness for effective response and to “Build Back Better” in recovery, rehabilitation and reconstruction.

2.3 National risk assessments

As early as 2009, a framework for European Union (EU) cooperation on disaster prevention covering all types of natural and man-made hazards was established within EU Member States (European Council, 2009). A fundamental component within this framework is risk assessment, for which a common set of guidelines on risk assessment was set in 2010 (European Commission, 2010), based on research and good practice examples that could support MS in the preparation of national risk assessments (NRAs). Additionally, MS agreed to prepare or update their own national risk assessments and to share with the Commission and other MS the results of these assessments (European Council, 2011). This document provides an overview of natural and man-made disaster risks the EU may face in the future, based on national risk registers and also focused on hazards with a pre-dominately cross-border dimension and those on a larger scale where impacts would be experienced by more than one Member State

In 2012 the Commission has received contributions on national risk assessments from 12 out of 32 countries participating in the Community Civil Protection Mechanism (Participating States): Czech Republic, Denmark, Estonia, Germany, Hungary, Italy, Netherlands, Norway, Poland, Slovenia, Sweden and UK. Most of these were complete or summary assessments except Denmark, Germany, Hungary and Sweden had sent information on the process to develop risk assessment and lists of hazards to be assessed. Additional information has been gathered through projects, systems, methodologies and datasets managed by the Commission (JRC) and collected through the Global Disaster Alert and Coordination system (GDACS), the European Flood Awareness System (EFAS), the European Forest Fire Information System (EFFIS) and the European Drought Observatory (EDO). The national risk assessments showed that the most wide-spread risks (cited by 75-80% of respondents) are floods and extreme weather events, followed by pandemics, terrorist attacks and cyber-attacks (2/3 of respondents). Other wide-spread risks (50-60% of respondents) are wild or forest fires; Chemical, Biological or Nuclear contamination and industrial accidents. Lower-ranking risks (>25-50%) are loss of critical infrastructure such as transport, energy or water networks; earthquakes; livestock epidemics; nuclear accidents and civil unrest/polarisation of society. Risks that concern 25% or fewer of the countries responding so far are marine pollution and oil spills, volcanic eruptions, landslides and transport accidents. (European Council, 2014)

The most important hazards in the EU as identified by the Member States include the following (European Council, 2014):

- Natural Hazards
  - Floods (number of MS: 17)
  - Severe weather (number of MS: 15)
  - Pandemics/epidemics (number of MS: 14)
  - Livestock epidemics (number of MS: 12)
  - Wild/Forest fires (number of MS: 11)
  - Earthquakes (number of MS: 9)
  - Landslides (number of MS: 7)
  - Droughts (number of MS: 6)
- Man-made hazards
  - Non malicious
    - Industrial accidents (number of MS: 15)
    - Nuclear/radiological accidents (number of MS: 13)
    - Transport accidents (number of MS: 10)
    - Loss of critical infrastructure (number of MS: 7)
  - Malicious
    - Cyber attacks (number of MS: 9)
    - Terrorist attacks (number of MS: 8)

The loss or disruption of critical infrastructure is considered separately as a man-made hazard (unintentional, accident).

Differences in risk assessments of MS exist in: (1) method of scenario building; (2) method of quantitative analysis, (3) number of risks and risk scenarios considered; and (4) temporal horizon (European Commission, 2010).

Both single-risk and multi-risk scenarios are considered in national risk analyses. The analysis must be carried out separately per category of impact. In addition, it should appropriately aggregate the risks from multiple hazards, but keeping available the results of impact categories. While risk assessments in more experienced countries may analyse in depth, quantitatively, with a greater number of scenarios, it may be appropriate to limit the number of analysed scenarios for MS who carry out the national risk assessment process for the first time (European Commission, 2010).

The following listing shows the identified risks for CIs:

Country	Risk Level	Term used
CZ	High	Critical infrastructure disruption
DE	-	Outage of critical infrastructure
IE	High	Loss Critical Infrastructure
PL	Medium	Disruption of electricity supplies, of fuel supplies, of natural gas supplies
SE	Very High	Disruption in food supply due to fuel shortages
UK	High	Attacks on infrastructure
NL	Very High	IP network failure, malicious prolonged electricity failure
	High	National power failure, malicious power supply failure
	Medium	Malicious gas supply failure

2.3.1 Germany

The Baseline protection concept for CI (Schutz Kritischer Infrastrukturen - Basisschutzkonzept) was developed under the authority of the German Federal Office for Civil Protection and Disaster Response and the Centre for the Protection of Critical Infrastructures (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe / Zentrum Schutz Kritischer Infrastrukturen). It was issued in 2005 and intended to be used as a guideline for large and medium size companies within the CI sectors and aims to protect human life by reducing the vulnerability of CI to natural events, incidents resulting from technical failure or human error, terrorist attacks, and criminal acts. The risk assessment method aims at providing a guideline for large and medium size companies within the critical infrastructure sectors, with the objective to protect human life by reducing the vulnerability of CI to natural events, incidents resulting from technical failure or human error and to terrorist attacks or criminal acts. The method does not include cyber threats. This topic is covered by separate guidelines, among which the IT Baseline Protection Manual and the further recommendations from the Federal Office for Information Security (BSI). The method is freely available and includes the following steps:

a. The establishment of danger (threat) categories, differentiated according to the areas of natural disasters, incidents resulting from technical failure or human error, terrorism or criminal acts.
b. Based on the above, definition of the respective protection levels.
c. The development of damage and threat scenarios.
d. The analysis of weak points.
e. The formulation of protection objectives as a basis for the definition of protection measures and countermeasures.
f. Definition of the required scope of action (coordination between public and private-sector measures).
g. Implementation of the defined required scope of action.
h. Regular reviews of this analysis and planning process for the purposes of quality management.

In addition, the method focuses on physical assets and considers nature, human and technical failure and human intent as sources of threats. It focuses more on recognising risk factors than on the scoring of them. Thus the comparison of the results is rather difficult. The method also supports the determination of threats, vulnerabilities and effects in the form of checklists.

2.3.2 Netherlands

The DHM (De Haagse Methodiek – The Hague Method) Security Management method was initially developed as a security management course for students at the The Hague University of Professional Education. The holistic RA method is based on quality assurance principles and is nowadays used by Dutch government (e.g. military bases and correctional institutions), nearly all sectors of the Dutch CI (e.g., nuclear, chemical, drinking water) and private enterprises in the Netherlands. The DHM Security Management method encompasses a RA phase (termed an Internal Security Audit) as well as a risk management (termed a Security Management Package) phase. The Internal Security Audit comprises the following elements:

- security policy,
- risk profile, risk scenarios,
- inventory and characterisation of assets,
- inventory of security measures and their condition,
- security organisation: time based analysis (detect, delay and response) of
- consequences of risk scenarios,
- effectiveness of security measures, linked to the risk scenarios and based upon the level of controllability
- seamless connections between internal and external(response) security organization and
- when necessary, proposals for improvement.

Quality assurance is achieved by means of internal security audits at regular intervals and by keeping the Security Management Package up to date. DHM addresses physical, ICT, organisational and personnel assets. The focus of the RA method is on threat due to human intent and the aim is to set up, run and maintain an effective security management system which prevents and protects against unauthorised influences and security risk against company activities and property. The method provides comparable results between assessments, is applicable at levels ranging from companies to multinational regulators. Strong points of DHM are its methodological background and its maturity.

In 2007, the Dutch Ministry of the Interior and Kingdom Relations (Ministerie vanBinnenlandse Zaken en Koninkrijksrelaties) decided to adopt a new strategy on national safety and security, in which a nationally-coordinated, sector transcending approach is followed (National Coordinator for Security and Counterterrorism, 2009). It encompasses two distinct phases, the first is concerned with the analysis of threats and risk. The second phase builds on the results of phase one and developes policies to manage the identified risk in a balanced way by reinforcing capabilities of preparation, prevention, response and aftercare. In order to support the first phase and identify risk factors in a scientifically justified way, a RA methodology was developed by a multidisciplinary project group. It supports a consistent all-hazards risk analysis over all sectors while ensuring compatible results. This enables comparisons among threats and sectors. The RA method is designed to determine the threats to CI and effects of their failure at a national scale, and to assess societal risk. Threats are described in the form of scenario, comprising the following steps:

- Formulation of a representative and complete set of scenarios to describe the threats under investigation.
- Assessment of the impact of each of the scenarios.
- Assessment of the likelihood of each of the scenarios. The likelihood assessment method distinguishes between threats (non-malicious causes) and hazards (malicious causes) based on the predominant use of statistics or expert opinions.

- Analysis of the resulting risk visualised in a 2-dimensional risk diagram.

This method includes all assets and all threat types. It implements a sound quantitative scoring mechanism, which enables comparison between assessments. It uses an exceptionally large number of 10 weighted impact criteria used for impact assessment), which include both tangible (such as costs, deaths, etc.) and intangible effects (such as social or psychological impact, environmental effects, etc.). The method prescribes which threats and effects are considered.

Strong points of the method are that it provides a comparison of very different threat types in order to facilitate their prioritisation and that threats are formulated into one or more scenarios which make them easy to relate to. This is essential, as the method involves a wide spectrum of stakeholders which assures the wide acceptance of the assessment. Another strong point is that the method incorporates methods to deal with the variations in perception concerning the relative importance of multiple types of effect.

2.3.3 Denmark

The RVA (risk and vulnerability analysis) Model was developed by the Danish Emergency Management Agency (DEMA) and released in 2006. The RVA model is primarily intended as a generally applicable tool for voluntary use among government authorities. However, in principle the model can be used by all interested parties with preparedness responsibility, both public and private entities.

2.3.4 UK

The Climate Change Risk Assessment 2017 Evidence Report (Kerb et al. 2016) collected studies that use the UK Climate Projections (UKCP09), the global CMIP5 model ensemble, single models and other scenario-based approaches to identify 60 risks and opportunities to reduce long-term vulnerability to climate change. The time periods covered in CCRA2 include current, 2020s, 2050s, 2080s, and post-2100s for sea-level rise. The Evidence Report focuses on the action needed in stronger policies and research priority for in the next five years (2017-2012) to tackle five major risks thar are climate change-related:

- Flooding and coastal change risks to communities, businesses and infrastructure.
- Risks to health, wellbeing and productivity from high temperatures.
- Risk of shortages in the public water supply, and for agriculture, energy generation and industry, with impacts on freshwater ecology.
- Risks to natural capital including terrestrial, coastal, marine and freshwater ecosystems, soils and biodiversity.
- Risks to domestic and international food production and trade.

The Evidence Report investigated the impact of climate change in the following aspects: natural environment and natural assets, infrastructure, people and the built environment, business and industry, international dimensions, and cross-cutting issues to help the UK government deliver its second Climate Change Risk Assessment report (CCRA2) by January 2017, which will update the national adaptation programmes (NAP) in 2018.

2.3.5 USA

The U.S. Department of Homeland Security (DHS), completed in 2006 the National Infrastructure Protection Plan (NIPP), a comprehensive risk management framework that defines critical infrastructure protection (CIP) roles and responsibilities for all levels of government, private industry, and other sector partners. The NIPP provides an approach to establish national priorities, goals, and requirements for critical infrastructure and key resources (CI/KR) protection aiming at the most effective manner to reduce vulnerability, deter threats, and minimize the consequences of attacks and other incidents (DHS, 2013). The cornerstone of the NIPP is its risk management framework that establishes the processes for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector risk. The risk management framework is structured to promote continuous improvement to enhance CI/KR protection by focusing activities on efforts to:

Set security goals: Define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective protective posture.

Identify assets, systems, networks, and functions: Develop an inventory of the assets, systems, and networks, including those located outside the United States, that comprise the Nation's CI/KR and the critical functionality therein.

Assess risks: Determine risk by combining potential direct and indirect consequences of a terrorist attack or other hazards, known vulnerabilities to various potential attack vectors, and general or specific threat information.

Prioritize: Aggregate and analyze risk assessment results to develop a comprehensive picture of asset, system, and network risk, establish priorities based on risk, and determine protection and business continuity initiatives that provide the greatest mitigation of risk.

Implement protective programs: Select sector-appropriate protective actions or programs to reduce or manage the risk identified and secure the resources needed to address priorities.

Measure effectiveness: Use metrics and other evaluation procedures at the national and sector levels to measure progress and assess the effectiveness of the national CI/KR protection program in improving protection, managing risk, and increasing resiliency.

The risk management framework can be applied to an asset, system, network, or function basis, depending on the fundamental characteristics of the individual CI/KR sectors. Sectors that are primarily dependent on fixed assets and physical facilities may use a bottom-up asset-by-asset approach, while sectors with diverse and logical assets may use a top-down business- or mission-continuity approach.

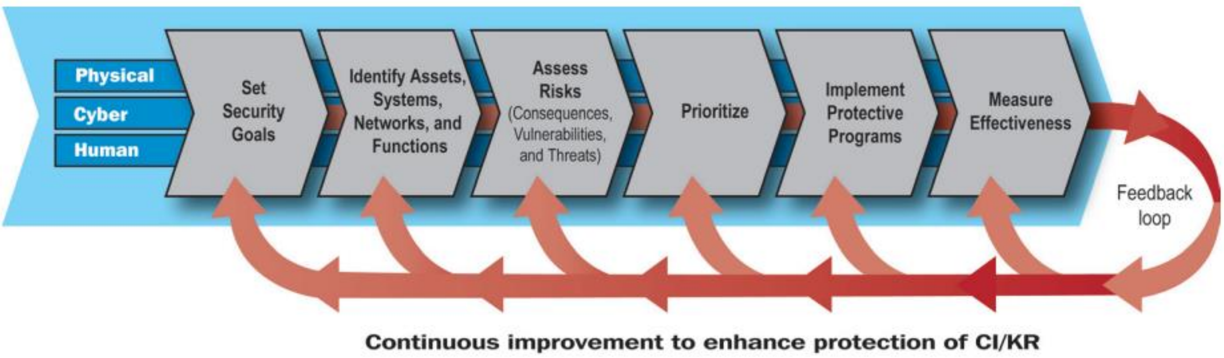


Figure 4: Phases of the NIPP.

The criteria of the national-level comparative risk assessment are based on the criteria set forth in Homeland Security Presidential Directive 7 and can be divided into four main categories (DHS, 2010):

- Human Impact: Effect on human life and physical well-being (e.g., fatalities, injuries).
- Economic Impact: Direct and indirect effects on the economy (e.g., costs resulting from disruption of products or services, costs to respond to and recover from the disruption, costs to rebuild the asset, and long-term costs due to environmental damage).
- Impact on Public Confidence: Effect on public morale and confidence in national economic and political institutions.
- Impact on Government Capability: Effect on the government's ability to maintain order, deliver minimum essential public services, ensure public health and safety, and carry out national security-related missions.

Within the NIPP, risk is a measure of potential harm that encompasses threat, vulnerability, and consequence: Risk (R) = f(C, T, V), where an asset's risk is a function of the likely consequences (C) of a disruption or successful attack; the likelihood of a disruption or attack on the asset, often referred to as the threat (T) to the asset or the asset's attractiveness; and the asset's vulnerability (V) to a disruption or attack.

2.4 Sectoral approaches

2.4.1 Impacts on Transport modes

(UN, 2013)

Road Transport

Climate change will certainly impact on the infrastructure, operations, safety and maintenance of the road systems, affecting all network managers and users. Main impacts include both direct (e.g. pavement deterioration and deformation, damages and subsidence in permafrost areas, general structural damage, traffic disruption and accessibility problems for tunnels and bridges caused by floods and bank erosion) and indirect (economic, environmental, demographic, and spatial planning). Road infrastructure will also suffer from asphalt rutting and/or melting, thermal expansion of bridge joints, landslides and bridge scouring or undermining.

Rail Transport

The rail sector is already affected by climate change with hotter summers, wetter winters, strong winds and sudden switches of seasons causing increased traffic disruption and higher costs of network maintenance and traffic as well as higher energy consumption. Main impacts include rail buckling, rolling stock overheating and failure, signaling problems, increased construction and maintenance costs, embankment and earthwork failures, bridge scouring, overwhelming of the drainage systems and speed restrictions, delays and operation disruptions. As such impacts are possible to increase in the next decades, effective climate change adaptation strategies are required that will include vulnerability assessment and mapping, maintenance and emergency planning, dedicated R&D actions and the introduction of effective design guidelines and protocols for lines construction using improved new technologies and for the rolling stock.

Inland waterways

As relatively small changes are projected for the mean water levels of inland waterways until 2050, climate change impacts are not expected to be significant until then. However, the foreseen greater temporal and spatial variability in water levels can certainly create problems, particularly after 2050 that require integrated waterway planning, investments, maintenance and management. Main impacts include restrictions and cost increases due to very low and high water levels, land infrastructure inundation, and sedimentation issues in navigation channels as well as building new water reservoirs.

Seaports

Seaports will bear some of the worst impacts of climate change due to its nature – placement at the edge of seas and land - and probably mean sea level rise and higher and more frequent storm surges. The majority of seaport locations are currently vulnerable to coastal flooding, a situation that is foreseen to deteriorate in the future; at the same time, estuarine ports will be also vulnerable to fluvial floods and droughts. Main climate change impacts include infrastructure, equipment and cargo damages from inundation and wave energy changes, increases in the energy consumption for cooling cargo, changes in transport patterns due to the potential development of new shipping routes (e.g. Arctic Ocean lanes), higher port construction and maintenance costs, changes in flow and sedimentation patterns in ports and navigation channels and insurance issues.

2.4.2 Energy sector risk

(DHS, 2010)

Historically, the Energy Sector has been proactive in developing and applying vulnerability assessment methodologies tailored to its assets and systems. However, no single vulnerability tool or assessment methodology is universally applicable. Stakeholders use different assessment tools that are developed by professional and trade associations, Federal organizations, government laboratories, and private sector firms. The number of tools in use is large, and the vast majority of significant facilities in the Energy Sector have already undergone assessments using one or more of these tools.

Various risk assessment methodologies exist and attempt to address the diversity of assets in the Energy Sector. Some methodologies are tailored to a specific segment of the sector (e.g., electricity, oil, natural gas, or their system components), while others are used to assess risks at the system or sector level. In addition, some have broad applicability that extends across multiple CI sectors.

In the U.S., one example is the Energy Sector Control Systems Working Group, utilizing the Energy Control Systems Roadmap, which is a Department of Energy (DOE)-led collaborative effort to address cybersecurity issues. Other products include vulnerability and risk assessment-related methodologies, checklists, lessons learned, support for policy analysis, and guidelines for various types of assets. The programs have also established partnerships with infrastructure owners/operators, State and local governments, and a wide range of industry associations. Energy industry associations have developed and disseminated security guidelines to help screen assets, including:

- Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition, API, and National Petrochemical & Refiners Association.
- Security Guidelines for the Petroleum Industry and American Public Gas Association.
- Pipeline Security Guidelines.
- Security Guidelines for the Electricity Sector.
- Critical Infrastructure Protection (CIP) Reliability Standards

The complexity, diversity, and interconnectedness of the Energy Sector dictate the need for assessing consequences at many different levels of detail:

- Asset or facility level.
- System, sector, and urban area level.

- Regional and/or national level.

These assessments must consider both physical and cyber interdependencies within the Energy Sector and among the other CI/KR sectors at all levels. Interdependencies may have national, regional, State, and/or local implications and are considered to be an essential element of a comprehensive examination of physical and cyber vulnerabilities.

Another U.S. approach is the Risk Management Guide (RMG). Adopted in 2008 by the U.S. DoE, it serves as a non-mandatory approach for implementing the requirements of directive DOE_O_413.3A (Program and Project Management for the Acquisition of Capital Assets) (U.S. DoE, 2010). It is a guideline for risk management of projects, not of processes. The RMG method includes the full risk management loop, and therefore exceeds pure RA methods.
The RA part of the method comprises the following steps:

- Risk Identification.
- Assignment of the Risk Owner.
- Assignment of Probability and Consequence.
- Assignment of Risk Trigger Metrics.
- Risk Register.
- Risk Analysis:
  - Qualitative Risk Analysis.
  - Quantitative Risk Analysis.
  - Project Learning Analysis.
  - Error and Variance Analysis.
  - Contingency Adequacy Evaluation.

RMG-DOE addresses physical, organisation and personnel assets. The method focuses on technical and human failure, but as these threats are put in the context of a project, a direct comparison with the other methods would distort the picture. The method offers extensive checklists for determining threats and effects. Vulnerabilities are incorporated into the risk estimation. The method provides metrics for probability and effects, which makes comparisons between projects possible.
Strong points of RMG-DOE are the rigorous metrics and the extensive glossary of terms, which enables a consistent understanding of the terms used.

2.4.3 Gas Infrastructure Europe

(Gas Infrastructure Europe, 2016)

The GIE Security Risk Assessment Methodology is an integrated approach, amongst the European energy infrastructure operators, to assess the highest threats of failure and highest potential consequences to the safety of the public and industry workers, the environment, and production of gas infrastructure (facilities, systems, and components). The GIE Security Risk Assessment Methodology follows an “asset approach” focusing on the identification, analysis, evaluation of the risks that have impact on the assets and on their components. The GIE Security Risk Assessment Methodology, developing the management processes defined in the ISO 31000 Risk Management, represents a tool for the risk management framework and considers the heterogeneity of the European gas companies (in terms of size, distribution on the network, etc.), the common objectives in complying the EC directives and the protection requirements of the gas Infrastructure assets.

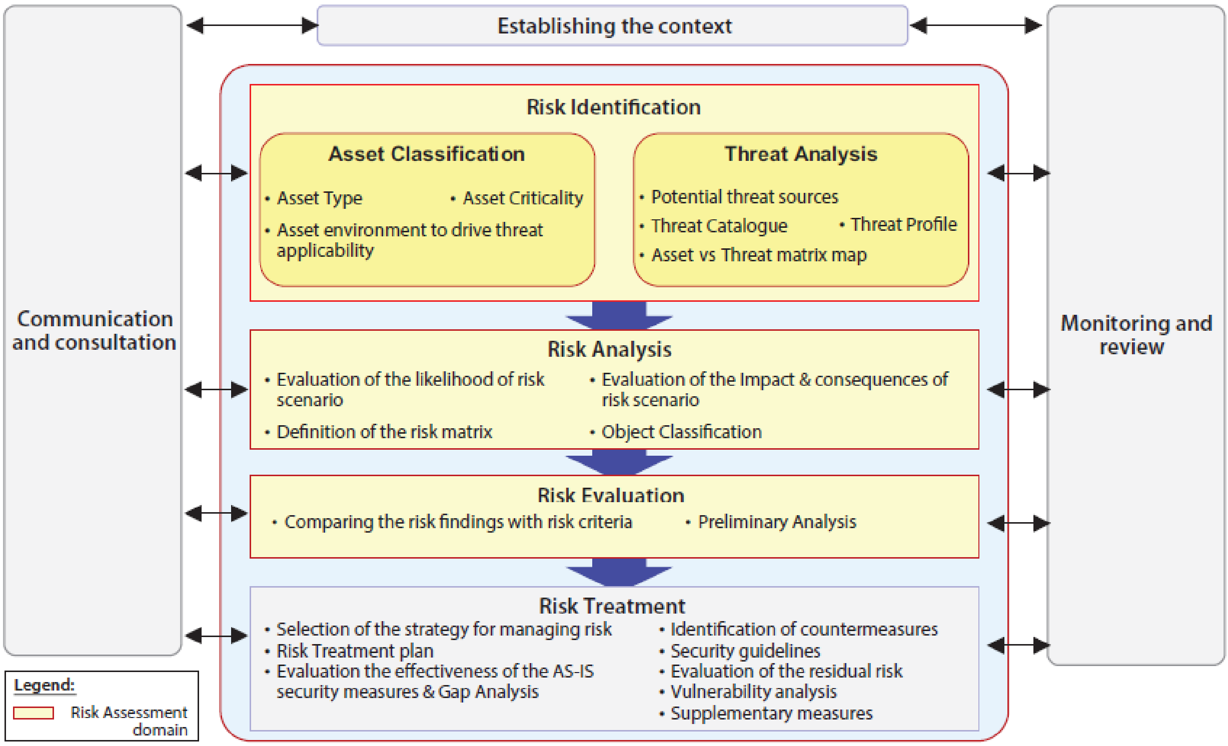


Figure 5: Security Risk Assessment - Framework Overview (GIE 2016).

The methodology introduces a Security Risk Assessment tool for supporting companies to properly collect and analyze information and data, following the defined methodology, in order to define the global security risk level for each asset considered (Gas Infrastructure Europe, 2015).

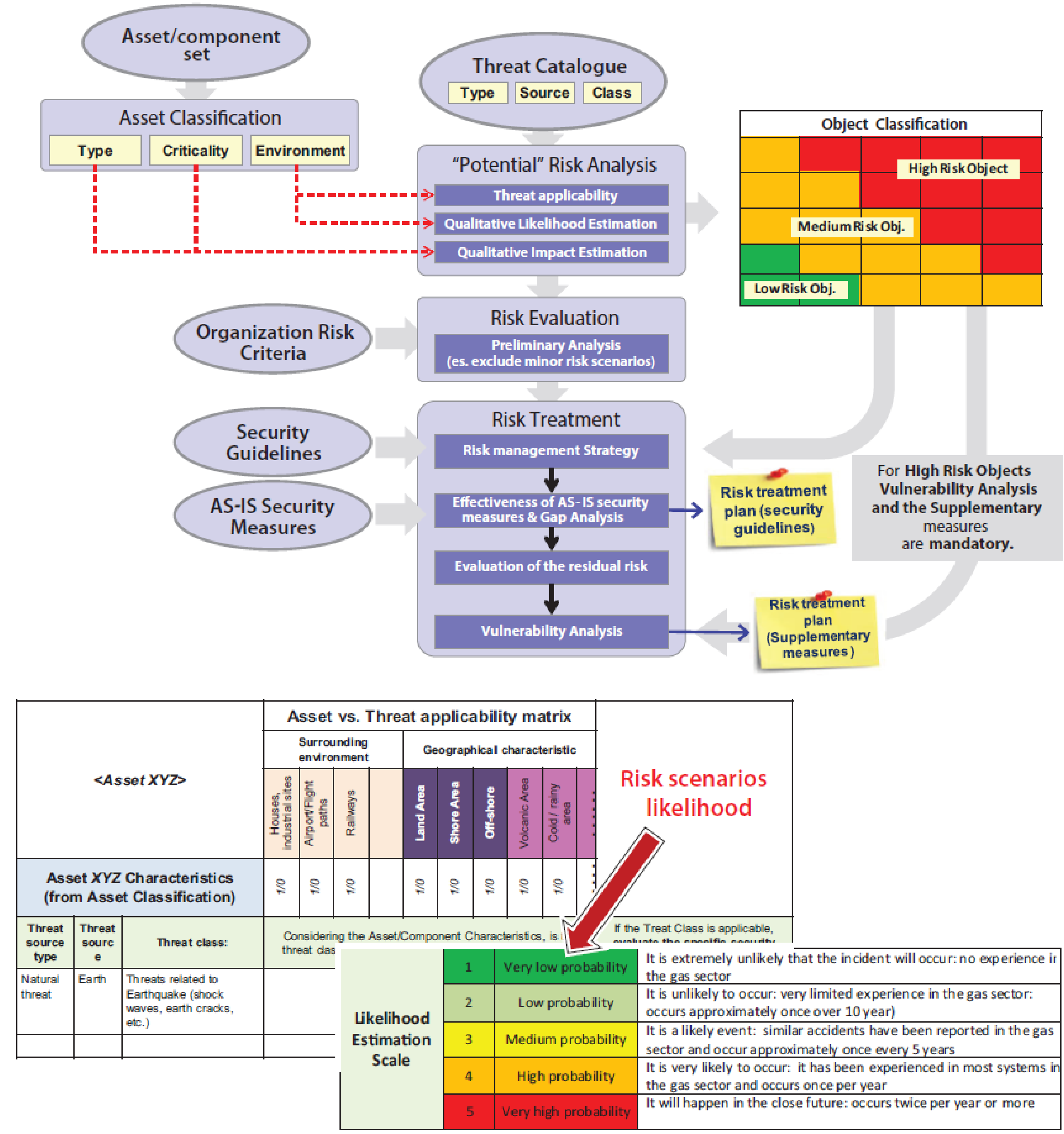


Figure 6: Risk management method of GIE 2015.

2.4.4 E-ISAC

(https://www.esisac.com)

The methodology was developed by the U.S. Department of Energy's Office of Energy Assurance (OEA) in 2002. The program is designed to develop, validate, and disseminate assessment and survey methodologies , to provide training and technical assistance; and stimulate actions to mitigate significant problems. The method is meant for wide use within the U.S. energy sector. The E-ISAC RA method comprises three main phases and a set of substeps:

- Pre-assessment
  - Define objectives and scope of assessment.
  - Establish information Protection procedures.
  - Identify and rank Critical Assets.
- Assessment
  - Analyze Network Architecture.
  - Assess Threat Environment.
  - Conduct Penetration Testing.
  - Assess Physical Security.
  - Conduct Physical Asset Analysis.
  - Assess Operations Security.
  - Examine Policies and Procedures.
  - Conduct Impact Analysis.
  - Assess Infrastructure Interdependencies.
  - Conduct Risk Characterisation.
- Post-assessment
  - Prioritise Recommendations.
  - Develop Action Plan.
  - Capture Lessons Learnt and Best Practices.
  - Conduct Training.

ES-ISAC addresses physical, ICT, and organisational assets. Although personnel are mentioned, it is not explicitly addressed. Only threats stemming from human intent or cascading effects are addressed by this method. ES-ISAC focuses more on the recognition of risk factors than on the scoring of them, making comparing results difficult. A strong point are the checklists, that are provided. One checklist is stating what information is required to complete the RA method and where such information can be found. Another checklist helps to determine assets.

2.5 Multi-sectoral approaches

2.5.1 PAS 55

PAS 55 Assessment Methodology (PAM) was developed in 2003 and revised in 2008 by a number of organisations under the leadership of the Institute of Asset Management. It is based upon the ISO management systems Plan-Do-Check-Act approach. It built on the structure of existing standards in order to ease understanding and adoption. It comprises a set of guidelines which focus on the management of physical assets. Human, ICT and organisational assets are only considered in the method as far as they have a direct impact on the management of physical infrastructure assets. The framework of the method is holistic and the method distinguishes between five categories of assets:

a) physical assets (natural resources, infrastructure, machinery, plant, equipment, buildings, IT systems);
b) human assets (leadership, management, workforce, skills, knowledge and experience);
c) financial assets (cash, investments, equity, credit rating);
d) information assets (data and information);
e) intangible assets (reputation, customer and staff impression, public image/relations, brand value, licenses, patents, trademarks, copyrights) and
f) culture.

The methodology provides guidelines for asset management rather than providing one fixed method. Key steps that are recommended in this methodology to ensure a systematic approach are:

1) classify assets;
2) identify credible risks;
3) identify the risk controls that exist;
4) determine level of risk;
5) determine the tolerability of the risks;
6) prepare and evaluate options and action plans to improve risk controls if necessary;
7) review adequacy of action plan;
8) maintain new and existing risk controls and ensure that they are effective.

For each of the steps, PAM refers to established methods or gives guidelines on what to include. Strong points of this methodology are the concordance to standards, the availability of training courses and that the method is certifiable.

2.5.2 RAMCAP plus

The RAMCAP (Risk Analysis and Management for Critical Assets Protection) method was developed by the US company ASME-ITI, (ASME-ITI, 2005), starting in 2003. This RA method aimed at reducing risk from terrorist attacks. In February 2009, the method was extended to include all risk (all hazards) and subsequently called RAMCAP plus. The result is a high-level risk assessment and management method that can be tailored to be used in various sectors.
For seven sector-specific types of sector-specific objects, specific guidance documents have been made available to facilitate the adaptation of the RA method to the specific needs of the sector. For the energy sector, the following guidances are of interest:

- petroleum refineries,
- liquefied natural gas terminals,
- nuclear power plants,
- nuclear spent fuel storage and transportation, as well as
- dams and locks.

The method is meant to be used widely by all security managers of CI and aims at delivering results which allows comparing risk factors within and across sectors at asset, system, region, state and national levels and across time. The method covers seven distinct steps:
Step 1 – Asset Characterisation
Step 2 – Threat Characterisation
Step 3 – Consequence Analysis
Step 4 – Vulnerability Analysis
Step 5 – Threat Assessment
Step 6 – Risk and Resilience Assessment
Step 7 – Risk and Resilience Management
RAMCAP plus explicitly addresses physical objects and personnel as assets. Organisational assets might be included into one of these objects, but this is not clear. The method addresses all threat types and by providing consistent metrics for probability, vulnerability, and effect supports comparing of results, even across sectors is made possible. The method provides checklists for threats and effects. Strong points of this method are the fixed metrics and that the method is not sector specific but is supported by specific guidelines for each infrastructures.

2.5.3 RVA Model

(http://brs.dk/eng/inspection/contingency_planning/rva/Pages/vulnerability_analysis_model.aspx)

The RVA, developed by Danish Emergency Management Agency, comprises of four sectors, each being supported by an interactive MS Word document.

- Part 1: Definition of purpose, participants and scope of the analysis.
- Part 2: Scenario development. The users generate their own risk scenarios based on what is most relevant to them.
- Part 3: Elicitation and assessment of risk factors and vulnerabilities associated with each scenario by the users. Risk factors are assessed according to likelihood and consequences. Vulnerabilities are assessed according to existing capacities to prepare for, respond to, and recover from the type of incident in the scenario.
- Part 4: Presenation and comparison of scenarios regarding risk and vulnerability profile.

This method addresses all assets and all threats. It provides checklist for threats, vulnerabilities and effects and even comes with a small scenario databank for threats. The method is simple and the supporting tools are simple and effective. They consist of Microsoft Word forms that allow free text, while providing a rigorous template. The metrics in this method are very qualitative, which would make comparisons between assessments difficult.

2.6 Risk assessment of interconnected CI

In the following we discuss aspects of inter*connection* and inter*dependency*. More deteailed definitions of the two terms are presented in the following, but generally one can say that a interconnectioin is given if two assets are related to each other, i.e. if they are part of one structure. Interdependencies are typically defined as bidirectional relationships where the state of one infrastructure affects or is correlated to the state of another asset.

2.6.1 Interconnected Infrastructures

Many sector depend on other sectors' resilience and thus it is essential that these interdependencies are understood in order to improve the resilience of infrastructure (HM Government, 2011). Many methodologies have been extended from sectoral to network approaches (EC, 2012).

Table 1: Dependencies and impacts.

Sector	Dependencies on Infrastructure	Impacts on other Sectors
Energy	• Water cooling in power stations and fuel refining • ICT for control and management system of electricity and gas • Transport for the fuel supply chain and workforce • Gas storage and distribution relies on electricity supply	• ICT wholly dependent on energy • Transport dependent on fuel and increasingly electricity • Water dependent on energy for treating, pumping and processing as well as control systems
ICT	• Energy for all services • Transport for maintenance workers	• All sectors increasingly dependent on ICT for control systems, especially the smart grid • Increasing dependence on ICT for sensing and reporting the condition of the infrastructure
Transport	• Energy infrastructure for fuel and increasingly electricity • ICT for management of services and networks • Drainage infrastructure to prevent flooding • Internal dependencies within and across modes (e.g. airports and roads)	• All sectors dependent on transport to transport workforce to sites
Water	• Energy for treating, pumping and processing • ICT for control systems • Transport for workforce and supplies of chemicals for processing	• All workplaces require water for staff • Cooling water for some energy infrastructure.

Modes of coupling

Interdependency is a bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other (Rinaldi et al., 2001). Risk assessment and management within the frame of an infrastructure requires an understanding of how and to what degree composing subsystems are interdependent. This requirement is even more essential in transport system infrastructures where interdependencies play a major role. Interdependencies can be formulated amongst infrastructure subsystems in a multitude of ways:

Rinaldi, Peerenboom and Kelly (2001) discern the following types of interdependencies (Rinaldi et al., 2001):

- Physical Interdependency: Two infrastructures are physically interdependent if the state of each is dependent on the material output(s) of the other. As implied by the name, a physical interdependency arises from a physical linkage between the inputs and outputs of two agents.
- Cyber Interdependency: An infrastructure has a cyber interdependency if its state depends on information transmitted through the information infrastructure. Cyber interdependencies are relatively new and a result of the pervasive computerization and automation of infrastructures over the last several decades.
- Geographic Interdependency: Infrastructures are geographically interdependent if a local environmental event can create state changes in all of them. A geographic interdependency occurs when elements of multiple infrastructures are in close spatial proximity. Given this proximity, events such as an explosion or fire could create correlated disturbances or changes in these geographically interdependent infrastructures.
- Logical Interdependency: Two infrastructures are logically interdependent if the state of each depends on the state of the other via a mechanism that is not a physical, cyber, or geographic connection. Logical interdependencies may be more closely likened to a control schema that links an agent in one infrastructure to an agent in another infrastructure without any direct physical, cyber, or geographic connection.

Perimann (2007) considers interdependencies to exist at four levels

- Physical; representing a direct linkage between infrastructures
- Geospatial; resulting from the co-location of infrastructure components
- Policy; resulting from higher level decision making affecting infrastructures otherwise not connected physically of geospatially
- Informational; depicting reliance on information passed between sectors and/or infrastructures

Haimes, Santos, Crowther, Henry, Lian & Yan also identify four “modes of coupling” between infrastructure components (Haimes, et al., 2008):

- Physical Coupling: These couplings exist when energy, information or matter is physically transferred from one component to another.
- Logical and Information Coupling: Logical couplings provide mechanisms by which coupled systems will conditionally behave based on shared measurements and functional relationships. Information couplings involve mechanisms by which information is physically transferred from one device to another by way of signal transmission.
- Inter-Regional Economic Couplings: These couplings exist when the production, distribution and consumption of commodities are dictated in part by regional interdependencies defined by physical infrastructures, import and export flows, and relative geographic distances.

- Inter-Sector Economic Couplings: These couplings exist among interconnected economic sectors causing disruptions to propagate.

Rinaldi et al. (2001) introduced six categories to classify incidents impacting interdependent critical infrastructures: Type of Failure, Infrastructure Characteristics, State of Operation, Type of Interdependencies, Environment, Coupling and Response Behavior. Ezell (2000) adopted the Hierarchical Holographic Modeling, considering a multitude of mathematical and conceptual models, each of them devoted to represent a particular aspect of the system: hierarchy, functions, components, operations etc. For each of the aforementioned attributes the following categories can be specified:

Type of failure:
- Common cause: a disruption of two or more infrastructures at the same time because of a common cause (e.g., natural disaster, right-of-way corridor)
- Cascading: a disruption in one infrastructure causes a disruption in a second infrastructure
- Escalating: a disruption in one infrastructure exacerbates an independent disruption of a second infrastructure (e.g. the time for recovery or restoration of an infrastructure increases because another infrastructure is not available)

Infrastructure Characteristics:
- Organizational
- Operational
- Temporal: Infrastructure time constants – Time scales of interest
- Spatial: Components (part, unit, subsystem, system, infrastructure, interdependent infrastructures) – Geographic scale (cities, regions, national, international)

State of Operation:
- Normal
- Repair/Restoration
- Stressed/Disrupted

Environment:
- Economic
- Legal/Regulatory
- Technical
- Social/Political
- Business
- Public Policy
- Security
- Health/Safety

Coupling and Response Behavior:
- Adaptive (Response behavior)
- Inflexible (Response behavior)
- Loose/Tight (Degree of coupling)
- Linear/Complex (Type of interaction)

These dimensions are depicted in the following diagram.

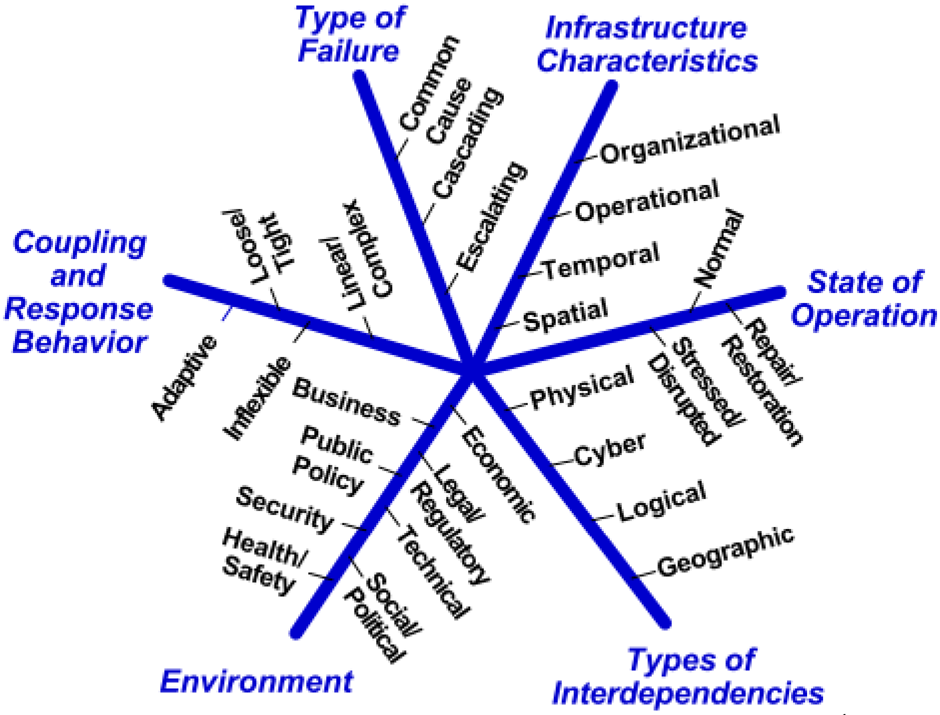


Figure 7: Dimensions for describing infrastructure interdependencies [1]

There are different ways of defining and characterizing interdependencies. Sometimes it may be useful to distinguish between dependencies and interdependencies. Utne et all. (2010) use "direct dependencies", which are relatively easy to identify, model, and analyze; and interdependencies, which are mutual dependencies that may be dangerous, but hard to understand.

Rinaldi et al. (2001) define interdependencies between infrastructures as a bidirectional relationship and dependencies as unidirectional. Bidirectional relationships means that the state of one infrastructure affects or is correlated according to the state of another infrastructure.

Zimmerman (2001, 2004) distinguished the spatial and functional interconnectedness and dependency. Spatial interconnectedness was set to account for proximity between infrastructures as the most important relationship between the systems. Functional interconnectedness referred to a situation in which an infrastructure is necessary for operation of another infrastructure, for example, the pumps in a water treatment system needing electricity in order to function. There are also situations with both types of interconnectedness.

The term interdependency is used in EU-CIRCLE for both unidirectional or bidirectional dependencies, regardless of the causal direction of the dependency.

2.6.2 Interconnected simulation approaches

Recent research has been involved in the creation of risk assessment frameworks in interconnected critical infrastructures using a multitude of simulation approaches in order to explore and model

[1] Diagram taken from "Infrastructure Interdependencies", a presentation of Terrence K. (Terry) Kelly, Ph.D. Senior National Security Officer for the White House Office of Science and Technology Policy

network interconnections. Some of the most prominent approaches designed for this purpose are the following:

Ouyang et al (2009) proposed that the vulnerabilities of critical interdependent infrastructures are related through two procedural approaches: structural vulnerability and functional vulnerability. For structural vulnerability, infrastructure topologies are the only consideration, while operating regimes of different infrastructures need to take into account functional vulnerability. Structural vulnerability is related to attacks and can be described as the decrease of system efficiency after attack. The authors propose that only infrastructure topologies are considered and the most important thing is to determine what characteristics are used to describe structural efficiency.

Criado (2006) and Crucitti (2003) present several definitions on structural efficiency, such as average shortest distance, network diameter and cluster efficiency, but they all have some limitations. Usually, the average reciprocal shortest path lengths of networks are used to measure the structural efficiency and this approach is generally accepted.

Zhang and Peeta (2011) proposed a generalized modeling framework that combines a multilayer network concept with a market-based economic approach to capture the interdependencies among various infrastructure systems with disparate physical and operational characteristics. The various infrastructure systems were modeled as individual networks connected through links representing market interactions. The market interactions capture the various types of interdependencies through supply–demand mechanisms. The modeling framework used a multilayer infrastructure network (MIN) concept, the computable general equilibrium (CGE) theory, and its spatial extension (SCGE), to formulate an equilibrium problem. Numerical experiments were presented to illustrate the capability of the model to capture various types of interdependencies and to provide insights on the importance of these interdependencies for real-world problems.

Mukherjee et al (2010) introduced an integrative network-based approach to modelling co-dependent infrastructure systems and simulating them within the general purpose framework of situational simulations. The authors implemented the situational simulation using a proposed process model and the information model, thus providing a prototypical product interface. The simulation was made interactive, allowing decision makers to account for complex adaptive interactions among co-dependent infrastructure systems, and to account for non-linear feedbacks and counter-intuitive behaviour. The model was implemented within the general purpose framework of situational simulations that can be used by public infrastructure emergency management agencies to test crisis management strategies, assess risk, and specifically identify and prepare for events that expose system vulnerabilities.

Johansson & Hassel (2010) introduced an approach for modelling interdependent technical infrastructures. The modelling approach considered structural properties, as employed in graph theory, as well as functional properties to increase its fidelity and usefulness. By modelling a fictional electrified railway network that consists of five systems and interdependencies between the systems, it was shown how the model can be employed in a vulnerability analysis. The model aimed to capture both functional and geographic interdependencies. It was concluded that the proposed modelling approach is promising and suitable in the context of vulnerability analyses of interdependent systems.

Eusgeld et al (2011) studied the interdependencies within critical infrastructures (CI) emphasizing the importance of potential failure propagation among infrastructures leading to cascades affecting all supply networks, presenting a systems-of-systems (SoS) approach. An overall model was required to provide security and reliability assessment taking into account various kinds of threats and failures. The work analysed the interdependencies between industrial control systems, in particular SCADA (Supervisory Control and Data Acquisition), and the underlying critical infrastructures addressing the vulnerabilities related to the coupling of these systems. An integrated model contained detailed low level models of (sub)systems as well as a high level model, covering all hierarchical levels was employed. On the other hand, a coupled model aggregates different simulated outputs of the low level models as inputs at a higher level. Strengths and weaknesses of both approaches are analyzed and a model architecture for SCADA and the system under control are proposed.

Event-driven simulation simulate objects in a way to mimic the behavior of their real-life counterparts. In addition, a priority queue is used as a buffer mechanism to store a representation of "events" that are about to happen. This queue stores events on a time-of-occurrence basis, meaning that it is based on the time each event is bound to happen, so that the earliest element will always be the next event to be modeled. As an event occurs, it can trigger secondary events. These subsequent events are also stored into the queue so that execution continues until all events have been processed. This approach was used by the EU-funded Integrated Risk Reduction of Information-based Infrastructure Systems (IRRIIS) project (http://www.irriis.org).

The federative approach is based on the unification and integration of modular simulation tools for each distinct aspect of the network under consideration. It functions primarily as a method of modeling functional interdependencies among various “closed-system world” simulators. This approach was used by the Designing A New Research Facility For Critical Infrastructure Protection (DIESIS) EU-funded project aiming at coupling stand-alone simulators in order to simulate large-scale systemic relations (http://www.diesis-project.eu).

The limitations of the simulation-based approaches are: (i) most of these tools do not allow users to explicitly conduct theoretical analysis or analyze the mathematical properties of the underlying base model, which mostly is a black box to end users, if such a model even exists, (ii) not all aspects of the interdependencies can be included in the same simulation model as it typically concentrates on one aspect such as market or physical interdependency, (iii) the quality of simulation is highly dependent on the assumptions made by the modeler regarding agent behavior, and such assumptions may be difficult to justify theoretically or statistically, (iv) systematic approaches to calibrate the simulation parameters using realistic benchmark data are lacking, and (v) most simulation packages focus only on one system and simulate the impacts from it to other systems.

2.6.3 Input – Output approaches

The supply and demand approach: This approach is based on a “node and edge” representation where a node functions as an entity that produces, converts or consumes a resource while an edge is the actual means of delivering that resource to or from the node. In that way, the supply and demand network is formulated with edges that depict underlying dependencies among nodes. This approach was developed by the British Columbia University, resulting in the development of the I2SIm simulator.

The Leontief-based approach: This approach uses the original Leontief model as a means of tackling the problem of interdependent infrastructures. Originally, the model was used as a way to model the economy of a region/country by using economic sectors (represented as nodes) that were connected with one another. Through these connections outputs of one sector can be used as inputs for another one. By substituting the consumption/production concept with the notion of inoperability the above approach can be extended into interdependent infrastructures.

Crowther et al. (2004) proposed a Hierarchical Holographic Model (HHM) to account for the interdependencies of the highway transportation system. Six HHM perspectives relating to transportation interdependencies were identified:

(a) Emergency Response and Recovery (ERR) Jurisdiction, looks at the connections among the governmental, private sector and volunteer organizations that respond to emergency situations.
(b) Intermodal, covers the interconnections among the various modes of transportation. These include: highway, railroad, aviation, ports and public transportation/transit.
(c) Physical, looks at infrastructure elements that are located near the transportation infrastructure or integrated into it, such as electric power and communication lines (especially those carried by bridges).
(d) Economic, looks at different economic sectors and their interdependencies with transportation. Some of the major industries are manufacturing, agriculture, service and trade.
(e) Functional, looks at the agencies directly involved in the operation and maintenance of the transportation infrastructure and their relationship with supporting agencies
(f) Users, pertains to industry sectors that depend on the transportation infrastructure

Additionally the Inoperability Input Output model has been employed to provide a quantifiable measure for translating the physical inoperability of certain assets within the transportation infrastructure into compatible economic perturbation inputs.

Pant et al. (2011) described the interdependent adverse effects of disruptive events on inter-regional commodity flows resulting from disruptions at an inland port terminal. Their approach integrated a risk-based Multi-Regional Inoperability Input-Output Model, which measured the cascading regional effects of disruptions to interconnected industries, with models, simulating port operations such as commodity arrival, unloading, sorting, and distributing. The models capture three disruption scenarios at the port and provide measures of impact to industries that use the inland port terminal facility. A case study highlighted the disruptive effects of a closure of the Port of Catoosa in Oklahoma.

The aforementioned approaches of Pant et al. and Crowther et al. have several limitations. First, the network and spatial characteristics of the infrastructure systems are not considered. Thereby, each infrastructure system is modeled as a single node or sector in the economy. Consequently, the risk transmission among components within the same system at different locations cannot be captured. Second, a linear risk transmission input–output relationship is assumed, which is not realistic given real-world complexities. Third, the input–output factors and other coefficients are considered time invariant, precluding the ability to address dynamic issues. A side effect of the constant input–output factor assumption is that all systems will eventually evolve to complete failure over time if there is no external effort to stop the disruption in every system. Usually, this is not the case in reality for most systems due to characteristics such as redundancy, substitution, partial failure, self-healing, and fault-tolerance. Fourth, the existing models primarily focus on the analysis of failure (inoperability) risk transmission, which is only one aspect of infrastructure interdependencies. Business-as-usual scenarios are not addressed, though the approach has the potential to do so. Fifth, the methodologies to calibrate model coefficients in practice using available data are not adequately discussed.

2.6.4 Network based approaches

The Markov chain approach: This approach uses Markov-chain techniques in order to capture and model the change of state of interconnected infrastructures. The behaviors of these infrastructures are described by their states and by the possible transitions between these states. This approach usually poses significant challenges due to the exponential growth in the number of configurations to be evaluated.

Sultana and Chen (2009) presented an integrated model for simulating the vulnerability of a network of hydroelectricity generating infrastructures based on fragility curve development, flood frequency analysis, petri net development with extended stochastic analysis and Markov Chain generation and its extended analysis, when the hydroelectricity generating infrastructures are subjected to floods, it specially models the flood induced infrastructure interdependency and can be applied to other disasters induced interdependencies' modeling.

The Bayesian network approach: This is a probabilistic approach that can be applied in modeling and subsequently in the prediction of the behavior of a system, based on observed stochastic events. Within this approach, the variables of a Bayesian network are the components/assets of the network, while the links represent the interaction of nodes leading to network system ‘‘success’’ or ‘‘failure’’.

Ouyang et al. (2009) brought forward a Complex Network theory based, topology-driven method to comprehensively analyze the vulnerability between interdependent infrastructures. Complex Network (CN) theory is one of the best known approaches for performing interdependency analysis. Nevertheless, the approach can only model the certain topology structure of interdependencies, while it can do nothing on uncertain characteristics and behaviors of studied CISs like social or human factors.

The network-based models can utilize the network characteristic of infrastructure systems and address the spatial impacts of risks and disruptions. However, akin to the input–output models, these models focus primarily on security-related scenarios and disruption analysis. In addition, they rely heavily on probabilities, and at times, conditional probabilities of disruption to the network components. However, it is difficult to measure these probabilities or estimate them using empirical data. Also, these models are static, and the market aspects of the infrastructure systems are not incorporated. Therefore, the types of infrastructure interdependencies that can be modeled using solely this approach are rather limited. Another key barrier to the successful implementation of this approach is the disparate nature of network characteristics across the various infrastructure systems such as spatial scale, flow characteristics and patterns, flow routing principle, transmission speed, and user behavior.

2.6.5 Object oriented models

Object-oriented modeling has been shown to offer an attractive paradigm for describing the dynamic system operational behavior, with close adherence to the reality of the coupled processes involved. One of the major advantages of an object-oriented approach for modeling and simulating CI is the possibility to include physical laws into the simulation, and to emulate the behavior of the infrastructure as it emerges from the behaviors of the individual objects, and their interactions. This modeling achieves a close representation of the system behavior by integrating the spectrum of different stochastic phenomena which may occur, thus generating a multitude of representative stochastic, time dependent event chains. To integrate stochastic time-dependent technical and non-technical factors into the vulnerability assessment of a CI, a two-layer object-oriented modeling approach can be deployed. For example, an electric power system can be thought of as a stochastic hybrid system that can be modeled by a Finite State Machine (FSM) whose states involve continuous variables with uncertain dynamics. Stochastic processes are probabilistic component failure models which can be simulated by Monte Carlo techniques.

Panzieri et al. (2005)employed the so called Complex Adaptive Systems (CAS) approach, where independent networked systems (generally named agents) autonomously elaborate information and resources in order to define their outputs. The CAS approach is particularly useful for situations, including the case of infrastructures interdependencies, where there is sparse or non-existent macro-scale information. Sandmann (2007) and Nicola et al. (2001) propose stochastic models of networks covering a broad field of models and tools that might be applicable to (inter-) dependency modeling. These models are designed for events that have a high impact upon CIs but are most likely to be rare.

Panzieri et al. (2005) determines several different matrices to account for the interdependencies between heterogeneous CIs:

- An Operative Level Incidence Matrix; where the rows represent the set of nodes that need the output of the node to perform their activities,
- A Requirement Incidence Matrix; where the rows represent the set of nodes providing the needed resources to i-th agent.
- Three Binary Fault Incidence Matrices (FIMs); where the presence of a 1 in any position means that a fault may be propagated from the i-th node to the j-th one. FIMs correspond to three different types of interdependencies, namely:
    - Physical FIM describing fault propagation via the physical linkages
    - Geographical FIM emphasizing that faults may propagate among nodes that are in close spatial proximity.
    - Cyber FIM describing propagation of faults related to cyberspace

Casalicchio et al. (2010) proposed an agent-based modelling and simulation solution for critical interdependence modelling. The approach, named Federated-ABMS, relied on discrete agent-based modelling and simulation and federated simulation. It provides a formalism to model compound complex systems, composed of interacting systems, as federation of interacting agents and sector specific simulation models. The application of the formal model is performed to a target system, composed of a communication network and of a power grid.

Balducelli et al. (2005)developed interacting agents for modelling the discrete event simulation as a tool to approach interdependencies analysis and evaluation for critical infrastructures. The objective of the simulations is to study and analyse the interdependencies of the considered infrastructures. A discrete event simulation system was developed, using agent-oriented programming, considering the following limited sets of critical infrastructures: a great hospital infrastructure, a railway transportation infrastructure and other public transportation infrastructures. Faults inside the electricity distribution system were simulated, producing electrical power outages whose duration could be variable with respect to time and space, and generating consequences inside the transportation infrastructures. The hospital infrastructure users, such as different types of physicians, nurses, subsidiary personnel, students and patients are also modelled using agent oriented architectures.

Yong Ge et al. (2010) developed the GeoPetri Net system by incorporating the Petri net in a geographical information system to reveal the geographical interconnections between CI systems, but its feasibility might be limited some degree when other forms of interdependencies are considered. Eusgeld et al. (2011) considered to adopt High Level Architecture (HLA) standard to study interdependencies by decomposing the type of all-inclusive simulator into multiple domain-specific simulators and combining them in a distributed simulation environment, and communicating through network connection. But the communication infrastructure itself is still vulnerable when completely interconnected.

McNally et al. (2007) proposed a way to learn the functional and geographic interdependencies diagrammatically and geographically through the loosely coupled system of GIS and an ontology-based information system, both intra-domain and cross-domain interdependencies within CIs. It throws light on visualizing the interdependencies technologically, and GIS is a more general method for studying geographical interdependencies.

Simmonds et al. (2010) proposed a set of five predefined relations between assets that define varying levels of granularity: contains, used by, equals, interacts with and proximity of. Those five relations were deemed sufficient to relate the assets covering the majority of examined cases:

*Contains.*As used as in physical or logical containment. This relation is to be used when there is a logical, functional or operational dependency through physical or logical containment

Used by. As used in a one-way logical, functional or operational dependency; this may or may not be through physical interaction.

Equals. As used in a logical, functional, operational but not physical equivalence. If two assets are related by ‘equals’ then for the purposes of risk management they may be considered the same asset.

Interacts with. As used in a symmetric logical, functional or operational association; this may or may not be through a physical interaction. This is to be used when the nature of the interaction or dependency between two assets is vague or not well understood at present.

Proximity of. As used in the physical proximity of, e.g. an ‘Oil Dump’ being in the ‘proximity of’ ‘Storage Depot’. This relation should be used only with a particular physical threat in mind to mark out the assets in the physical ‘fallout’ area of some immediately affected asset. The following set of rules may be defined in order to fully account for consequences in transportation networks / assets:

- If the asset has permanent structural damage, then all assets contained therein should suffer permanent structural damage.
- If the asset has partial structural damage, then all assets contained therein should suffer permanent / partial structural damage or be non-operational.
- If the asset has permanent structural damage, then all assets that use this will be made non–operational.
- If the asset has partial structural damage, then all assets that use this could be made non–operational.

The main problems of object oriented modeling are related to the slow simulation speed, and the large number of input parameters in the analysis. However, by focusing on specific aspects, the model can be simplified, and the computational burden reduced.

2.6.6 (Semi-) quantitative approaches

Risk analysis can also be based on the extensive definition of risk scenarios. In the vast majority of cases the number of such scenarios is large so the second step is to filter and rank the scenarios according to their severity, as determined by their likelihood and consequence. Expert opinions are heavily used to guide the process and estimate the output.

The DECRIS model (Utne et al. 2010) utilizes experience from risk analyses within different critical infrastructures, and one of the main objectives is to develop an all-hazard generic risk and vulnerability analysis methodology suitable for cross-sector infrastructure analysis. Several aspects were examined, e.g., safety, economic impact and loss of services. The framework was implemented in the following steps:

1. Describe the initiating event.
2. Identify interdependencies. Perform qualitative analysis.
3. Perform a semi-quantitative assessment of the risk of the scenario.
4. Perform a detailed quantitative analysis of interdependencies (optional).
5. Evaluate risk and measures to reduce interdependencies.
6. Cost/benefit analysis (optional).

2.7 Related reseach projects

2.7.1 STREST

(http://www.strest-eu.org)

STREST focuses on earthquakes, tsunamis, geotechnical effects and floods, and on three principal CI classes: (a) individual, single-site, high risk infrastructures, (b) distributed and/or geographically extended infrastructures with potentially high economic and environmental impact, and (c) distributed, multiple-site infrastructures with low individual impact but large collective impact or dependencies. Standardized tools are used for hazard and risk assessment of low probability-high consequence (LP-HC) events, and their systematic application to whole classes of CIs, targeting integrated risk mitigation strategies. The output of a probabilistic multi-site loss assessment is a loss exceedance curve. The loss ratios that are sampled for assets of a given taxonomy industrial facility category at different sites can be considered to be either independent or fully correlated.

2.7.2 MATRIX

(http://matrix.gpi.kit.edu)

The core objective of the MATRIX project is to develop methods and tools to tackle multiple natural hazards (including earthquakes, landslides, volcanic eruptions, tsunamis, river floods, winter storms, wildfires and coastal phenomena) within a common framework. Natural extreme events threaten different regions of Europe suffering not only from individual hazards, but also from multiple events that occur in combination. The developed procedure consists of three levels: (1) Level 1 qualitative analysis, (2) Level 2 semi-quantitative analysis, and (3) Level 3 quantitative analysis. In this way, MRA is performed step by step. An application of the quantitative Bayesian network model via the Virtual-city tool illustrates its use. In this specific case, the scenario of debris flow triggered by both earthquakes and precipitation is considered. The calculated mean expected loss increases with respect to the same return period, taking into account cascade effects. The quantitative model using a Bayesian network has several features: (1) It is a probabilistic model instead of a deterministic model. The uncertainties in the parameters and their inter-relationships are represented by probabilities. (2) A large number of parameters and their inter-relationships can be considered in a systematic structure in the model. The probabilities of one parameter can be updated via available information. The change in one parameter will influence the others in the network through their inter-relationships. (3) Physical mechanisms, previous studies, and statistical data can be incorporated within the Bayesian network.

2.7.3 RAMSES

(http://www.ramses-cities.eu)

Following the simulation of socio-economic, climate, and transport futures, the Urban Integrated Assessment Framework (UIAF) has been adopted to explore the potential urban impacts of climate change. The framework has been redeveloped in an open-source modelling environment to allow more flexible operation, to look forward to the testing of multiple adaptation options. This is achieved through an overlay of spatial footprints of climate hazards (such as flood extents) onto the projections of future urban form and population patterns to assess the potential damage or disruption to city services and citizens. The relationship between climate hazard (e.g. temperature field or flood extent) and climate impact is dependent upon the exposure and vulnerability of the urban infrastructure. Thus, impact assessment is achieved through a combination of hazard, vulnerability, and exposure in a given spatial location. The approach uses downscaled climate simulations alongside future scenarios of employment and population and transport infrastructure development. The framework includes simulations of pluvial flooding and air quality. Pluvial flooding is incorporated into the UIAF by linking the dynamic flood model CityCAT with future projections of precipitation and scenarios of urban adaptation (e.g. changes in urban greenspace). The impacts of pluvial flooding are considered in the direct sense, through the inundation of transport links by surface water, and in the indirect sense through disruption to commuting journeys across the urban area. The approach developed in RAMSES in connection with the climate change risk analysis:

- provided a high level climate change risk analysis that captures information on hazard, exposure and vulnerability in urban areas;
- integrated information from multiple climate change hazards;
- analysed over 50 of the latest generation of climate model runs to explore the variability in climate changes;
- exploited cloud computing power to model hydrodynamic processes using the new pan-Europe 25m DEM for the flood modelling;
- developed a coherent, flexible, stable, scalable, transparent and very robust model to assess vulnerabilities and risks at different scales based on indicators – but not dependent on any particular indicator;

- developed a data model for vulnerability assessments based on a dichotomous classification of vulnerability factors that minimises redundancy and simplifies interpretation;
- delivered a ranking of European cities relative to each other in terms of their vulnerabilities and risks, with respect to a number of pre-defined climate change –driven hazards;
- clustered European cities in a number of coherent and homogeneous groups according to the type and intensity of the vulnerabilities and risks faced by each city.

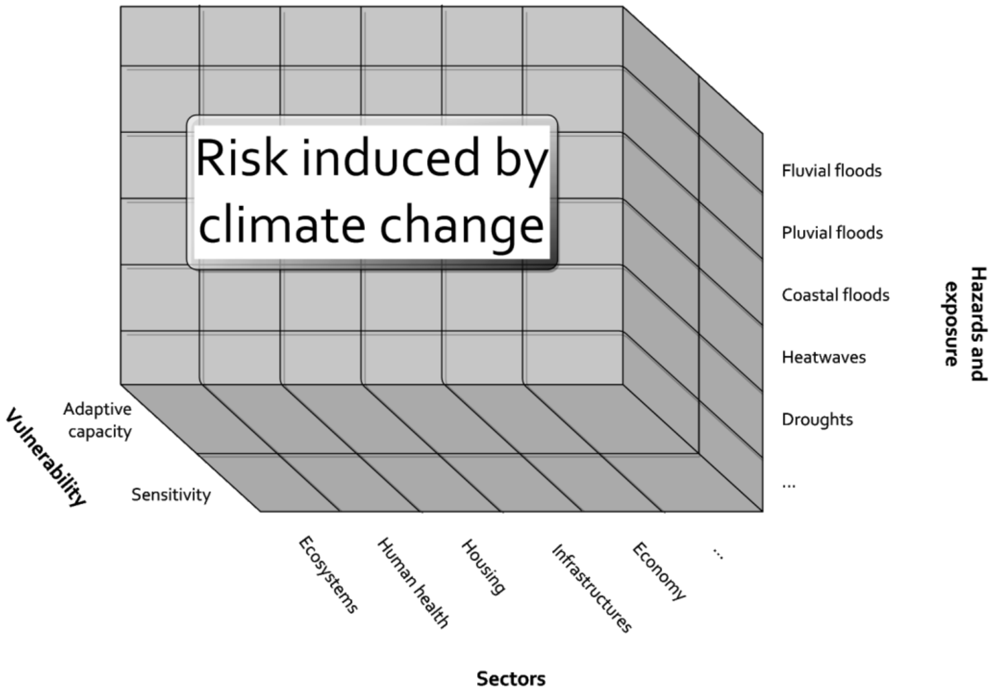


Figure 8: RAMSES conceptualisation

2.7.4 COUNTERACT

(http://cordis.europa.eu/project/rcn/85653_en.html)

COUNTERACT (**C**luster **O**f **U**ser **N**etworks in **T**ransport and **E**nergy **R**elating to **A**nti-terrorist A**CT**ivities) was developed within the context of a FP6 project from 2006 to 2009. The aim of the method is to develop generic security guidance for energy supply chains in order to meet and mitigate terrorist threats. As the method focuses exclusively on terrorist threats it uses a human intent specific method to assess risks, based on harm (effect) and availability (vulnerability/threat). Although the method can be applied at various levels of hierarchy, it does not provide a mechanism for transfering the results of multiple risk assessments into a higher hierarchical level.

The method is made of the following nine steps:

1. Establish and gain support from top management to perform the study
2. Define study objective and study boundaries; which assets shall be included in the assessment
3. Planning of the work with respect to availability resources, information requirement and time
4. Data collection and information gathering
5. Asset characterisation

    a. Asset harm
    b. Asset availability
6. Compilation of an asset attractiveness matrix
7. Evaluation and recommendation of attractiveness reducing measures according to the as low as reasonably practicable (ALARP) principle
8. Reporting.
9. Implementation and follow-up of identified measures

Strong points of the threat assessment module is the methodology of limiting the considered assets to only the assets that are relevant for terrorists and a checklist of necessary information to complete the method and expertise that can deliver the information.

2.7.5 INFRARISK

(http://www.infrarisk-fp7.eu/)

INFRARISK develops a stress test framework to analyse the impacts of very rare natural hazards on rail and road networks. The project develops a GIS platform that supports quantitative modelling of climate hazards and their impact to infrastructure. Climatic 'source events' can include rainfall and temperature. Source events can lead to different 'hazard events'. The impact on road and rail network can be either seen as an 'infrastructure event', where the focus is on the damage caused to a specific element of the network (such as a road segment, bridge or tunnel) or a 'network event', where the focus is on how the hazard affects the network as a whole (for instance the effect on traffic flow). This analysis can inform other models interested in 'consequence events', which may be the economic losses due to the network being inaccessible or the loss of life due to the damage to routes used by the emergency services. A decision support tool will be developed to conduct stress tests for infrastructures under varying conditions.

2.7.6 INTACT

(http://www.intact-project.eu/)

The INTACT risk analysis framework illustrates that impacts to CI are determined by the three main components: ExtremeWeatherEvent(EWE)/hazard, Vulnerability and Exposure. Exposure could be seen as a characteristic or physical attribute of the system at risk or as being independent of the vulnerability of a system. The likelihood and magnitude of adverse CI impacts is determined by hazard, vulnerability and exposure, where vulnerability is considered as a function of susceptibility and capacities of response. The EWE/Hazard is comprised of Probability of occurrence and intensity. The impact to the CI is also influenced by environment, functions, human staff and technical structures. Risk is thus the result of three elements (two probabilities and one effect (exposure)). Risk is seen as a sort of ex-ante perspective of CI impacts. Risk assessment and communication are influenced by risk governance meaning contextual factors for risk-related decision- making such as regulatory or legal frameworks, safety standards, financial arrangements, innovation management and the general sociopolitical culture. Risk transfer is to manage risks, by shifting the financial consequences of particular risks from one party to another. It is most commonly used in relation to the insurance sector and particularly for risks with low probability and high consequences.

2.7.7 RAIN

(http://rain-project.eu)

The risk framework of RAIN addresses the quantitative modelling approaches for critical transport, energy and telecom infrastructures which are highly interconnected and form 'systems of systems' that tend to be vulnerable during extreme hydro-meteorological events. A systematic risk analysis framework that explicitly considers infrastructure networks in response to extreme weather events and develops an optimization tool for series of mitigation strategies. The risk framework in RAIN project includes the: a) Hazard assessment, b) Vulnerability assessment, c) Consequence analysis, d) Risk evaluation. The RAIN project aims to:

- quantify the complex interactions between weather events and land based infrastructure systems (i.e. transport, telecoms, energy etc.),
- develop an operational analysis framework that considers the impact of individual hazards and the coupled interdependencies of critical infrastructure through robust risk and uncertainty modelling,
- consider cascading hazards, cascading effects and time dependent vulnerability,
- develop technical and logistic solutions to minimise the impact of these extreme events, include novel early warning systems, decision support tools and engineering solutions to ensure rapid reinstatement of the infrastructure network.

The Probability Sort algorithm is used to study cascading effects/domino models. It takes advantage of the fact that active probability components are often in an exponential small region of the state space and also lies on a continuum between a simple Maximum likelihood (ML) estimation and a full Bayesian probability analysis.

2.7.8 RESIN

(http://www.resin-cities.eu)

In the Resin project risk is defined as the probability of occurrence of a disturbance which results from the combination of hazard, exposure and vulnerability. Thanks to adaptation to climate change (ACC) and disaster risk reduction (DRR), exposure is reduced and risks are recognized and assessed, and then resilience is built to compensate or avoid them. Within RESIN, ACC depicts actions implementation in order to withstand climate change impacts and ensure the same infrastructures' performance level. This should allow critical infrastructures to continue to function during a disturbance or quickly recover to its original services, increasing infrastructures and all interrelated city components' resilience (CI, buildings, public spaces etc.). Disaster Risk Reduction is defined as the concept and practice of reducing disaster risks through systematic efforts to analyze and reduce the causal factors of disasters. Reducing exposure to hazards, lessening vulnerability of people and property, wise management of land and the environment, and improving preparedness and early warning for adverse events are all examples of disaster risk reduction.

2.7.9 PREDICT

(http://www.predict-project.eu)

In PREDICT, the Scenario-based Reasoning (SBR) tool is a decision support tool that can be used for the mitigation of cascading effects of crisis situation through improved situational awareness and decision making. The SBR tool will provide insight on future cascading effects through the systematic inspection of possible scenarios based on current observations and what-if assumptions. The SBR tool will provide a list of scenarios based on likelihood (or risk). It supports the exploration of scenarios for processes of sense making and decision making. The goal is to provide crisis management staff with relevant information for decision making and planning. A component named PROCeed will provide a Foresight and Prediction Tool (FPT). The FPT will allow for the development and the analysis of different alternative scenarios of future evolution of a given situation. This component will use the available information on the considered situation (e.g. observations) and models describing the (causual) relations between problem-relevant factors (these models can be local or distributed ones) to construct multiple scenarios of the possible future course of events. The FPT will also provide a description of each individual scenario, including events within the scenario, which will be visualized by appropriate means depending on the user needs. The process is covers the following steps:

1. Identify the area which is threatened/at risk;
2. Identify the CI within the threatened area;
3. Assess the threat's first order impact to the CI elements;
4. Identify the dependencies between CI's elements in the area;
5. Get insight into the possible course of action.

2.7.10 ASCCUE

(http://www.seed.manchester.ac.uk/cure/research/research-projects/asccue/ (Fedeski & Gwilliam, 2007))

The ASCCUE project develops a methodology for assessing the risk to larger urban areas and examine how climate change will affect the built environment.The cost of damage to a larger urban area are calculated as the arithmetic sum of the individual damage costs to its constituent buildings. The method can support separate estimates for each type of hazard.

If estimates for different probabilities of occurrence of the hazard are made, the results provide a range of probable costs. It may also be possible to assess the total risk for an area subject to more than one type of hazard by combing the costs for each hazard, provided that the hazard events are independent. By summing, the overall cost of climate change can be estimated.

The developed procedure foresees to 1) estimate the total cost of damage over a period due to the several hazards occurring at their present rate of incidence, and 2) to repeat the estimation for a revised rate of hazard incidence following climate change, and 3) to calculate the difference between them as a measure for climate change costs.

2.7.11 ClimVar & ICZM

(Satta, et al., 2016)

Along the mediterranien coasts, local authorities are facing the complex task of balancing development and managing coastal risks, especially coastal erosion and flooding, and to be prepared for the unavoidable impacts of climate change. ClimVar is a collaborative effort to promote Integrated Coastal Zone Management (ICZM). The local scale approach provides a useful tool for local coastal planning and management by exploring the effects and the extensions of the hazards and combining hazard, vulnerability and exposure variables in order to identify areas where the risk is relatively high. The resulting values are hosted in a geographic information system (GIS) platform. Individual variables and aggregated risk scores can be color-coded and mapped across the coastal hazard zone. The system provides a set of maps that allow identifying areas within the coastal hazard zone with relative higher risk from climate-related hazards. The method can be used to support coastal planning and management process in selecting the most suitable adaptation measures.

2.7.12 Swiss Re model

(http://www.swissre.com/rethinking/the_effects_of_climate_change.html, (Schwierz, et al., 2010))

Severe wind storms are one of the major natural hazards in the extratropics and inflict substantial economic damages and even casualties. Insured stormrelated losses depend on (i) the frequency, nature and dynamics of storms, (ii) the vulnerability of the values at risk, (iii) the geographical distribution of these values, and (iv) the particular conditions of the risk transfer. It is thus of great importance to assess the impact of climate change on future storm losses. A coupled approach is presented, using output from high-resolution regional climate model scenarios for the European sector to drive an operational insurance loss model. An ensemble of coupled climatedamage scenarios is used to provide an estimate of the inherent uncertainties. The operational insurance model (Swiss Re) uses a European-wide damage function, an average vulnerability curve for all risk types, and contains the actual value distribution of a complete European market portfolio. The technique can be a useful tool for future research on the impact of climate change that is relevant for policy makers, scientists and economists.

2.7.13 MOVE FP7

(http://www.move-fp7.eu)

In MOVE the vulnerability assessment provides one (or several) aggregated indicator(s) or a set of indicators reflecting the different causal factors of vulnerability to a hazard. The generic concept is multi-hardard, multi-dimensional, and holistic. Risk is considered as a function of hazard and the defined vulnerability indicators. In a first step, indicators reflecting the different dimensions (factors) of vulnerability are built. The vulnerability indicator(s) obtained is (are) a function of exposure, fragility and lack of resilience. The next step is to go from a vulnerability assessment to a risk assessment. A holistic evaluation of disaster risk has been achieved by means of the adaptation of the methodology proposed by Carreño et al. (2007). The methodology takes into account not only the expected physical damage, the number and type of casualties or economic losses (first order impact), but also the conditions related to social fragility and lack of resilience conditions, which favour the second order effects (indirect impact) when a hazard event strikes an urban centre. Contextual conditions such as the socio-economic fragility and the lack of resilience are described by a set of indicators that may aggravate the physical risk. The total risk is a combination of a) the direct effect, and b) the indirect effects.

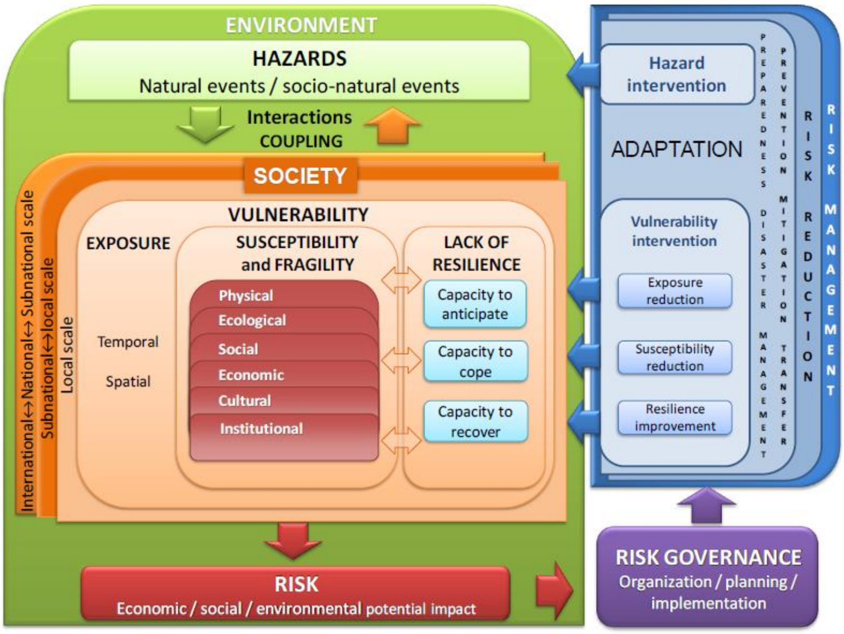


Figure 9: MOVE conceptual framework of a holistic approach to disaster risk assessment and management.

2.7.14 ERA-NET ROAD

(http://www.eranetroad.org, http://kennisonline.deltares.nl/product/22249)

Initiated by the ERA-NET initiative, the RIMAROCC framework is designed for road risk management on all decision levels and on all geographical scales of pertinence. RIMAROCC is a method where the objective is to facilitate the production of a risk management study by or for a road authority. The method can be used to mitigate threats. Risk is defined as the combination of threat, vulnerabilities and consequences. Threat comprises hazard and environmental factors. The hazard is described by climate factors, and the environment (the surroundings) is described by contextual site factors, e.g. land use. Vulnerabilities describe the properties of the assets or functions that may be harmed; these are factors that affect the vulnerabilities and minimise the consequences of an event. In the RIMAROCC vulnerability. Vulnerabilities include factors such as infrastructure-intrinsic factors, traffic and environment. Consequences describe the outcome of the realised threat and include human life and injuries, economic losses, reconstruction cost etc. When using the RIMAROCC method, the appropriate working methods depend on the scale of the analysis to be executed as well as available resources. More information on working methods is available in ISO 31010. Possible working methods are for example:

- Individual:
    - Desk studies
    - Interviews
    - Questionnaires, Inquiries
- Group sessions:
    - Brainstorm sessions (group sessions)
    - Electronic board room session (acceleration room)
    - Field visits

Key steps	Sub-steps
1. Context analysis	1.1 Establish a general context 1.2 Establish a specific context for a particular scale of analysis 1.3 Establish risk criteria and indicators adapted to each particular scale of analysis
2. Risk identification	2.1 Identify risk sources 2.2 Identify vulnerabilities 2.3 Identify possible consequences
3. Risk analysis	3.1 Establish risk chronology and scenarios 3.2 Determine the impact of risk 3.3 Evaluate occurrences 3.4 Provide a risk overview
4. Risk evaluation	4.1 Evaluate quantitative aspects with appropriate analysis (CBA or others) 4.2 Compare climate risk to other kinds of risk 4.3 Determine which risks are acceptable
5. Risk mitigation	5.1 Identify options 5.2 Appraise options 5.3 Negotiation with funding agencies 5.4 Formulate an action plan
6. Implementation of action plans	6.1 Develop an action plan on each level of responsibility 6.2 Implement adaptation action plans
7. Monitor, re-plan and capitalise	7.1 Regular monitoring and review 7.2 Re-plan in the event of new data or a delay in implementation 7.3 Capitalisation on return of experience of both climatic events and progress of implementation
Communication and gathering of information	

Figure 10: RIMAROCC framework - scope of steps and sub-steps.

The method is a cyclical process to continuously improve the performance and capitalise on experience. It starts with an analysis of the general context where risk criteria are established and ends with a reflective step where the experiences and results are documented and made available to the organisation. In practice, the steps are not always totally separate. There can be work going on in several steps at the same time but it is very important that the logical structure is maintained. There are feedback loops from each step to the previous ones and also a marked loop from the last step as a reflection and as part of the cyclical process.

2.7.15 WEATHER

(http://www.weather-project.eu/)

The main concept of the systemic risk terminology is illustrated by Figure 11. The assessment of weather-related impacts requires two steps: the recording of damages and the application of an economic evaluation framework on this quantitative dataset. Further, the issue of generalisation of country- or event-specific findings to larger geographical entities is of particular interest when trying to grasp the size of the problem.

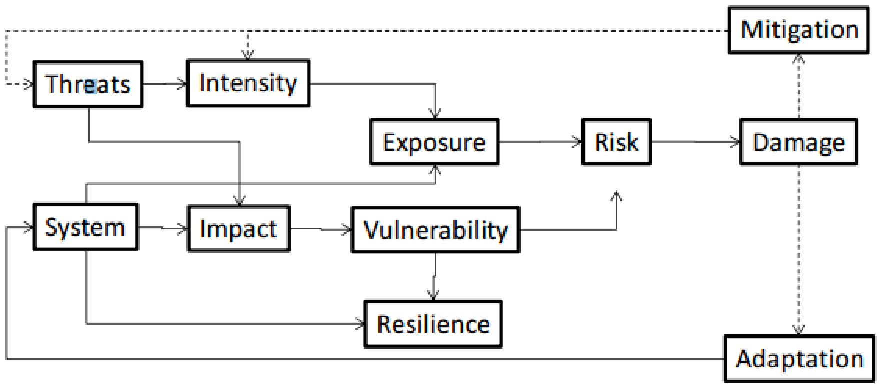


Figure 11: Terms and concepts of systemic risk theory within WEATHER project

For each of the four modes (road, rail, waterborne and air) the following categories of damages are considered:

1. Infrastructure damages and impacts on infrastructure maintenance, wear and tear and operations, e.g. snow removal, cleaning, small-scale repair measures, etc.
2. Vehicle fleet damages and impacts on the costs of service provision, e.g. additional personnel, energy costs or vehicle preparation.
3. User travel time costs, including time for freight movements, and perceived service quality, e.g. reliability, crowding and temperatures in vehicles.
4. Traffic safety, i.e. the number killed, severely and slightly injured transport users.

In case the original sources of damage reporting provide with cost values these values are used. Otherwise, a simplistic procedure is applied to estimate missing data and economic costs.

2.7.16 EWENT

(http://ewent.vtt.fi/)

The objective of EWENT is “to assess the impacts and consequences of extreme weather events on EU transport system”. The calculation method in the EWENT project tried to describe the overall risk of extreme weather events to different transport modes giving an overall picture of the risk situation in Europe. Risk indicators are used to compare situation in different countries both inside the climatic regions and within EU-27. It furthermore identifies the most vulnerable traffic modes in different parts of Europe. However, the results – the hazard, vulnerability and risk indicators – must be considered as a “ranking system” and definitely not as exact measures of risk. The risk is defined as a product of natural hazard and vulnerability, which means operationally that risk is the product of selected maximum probabilities of consequences and ranking numbers of vulnerabilities. The hazards - leading to time delays, accidents or infrastructure damages or increased maintenance needs - follow the climate zone division, where several countries belong to one climate region, whereas the vulnerabilities are calculated for each type of traffic (freight, passenger) in each mode and in each country. Hazard is characterized by the probability of the outcome of the chain of events from weather phenomena to final consequences to society, including health (accidents), property (material) and delay consequences. Between a phenomenon and a consequence of the phenomenon there exists a direct causal connection, often physical in its nature such as falling trees or lightning. The actual consequence of the phenomenon takes place when the impacts affect the transport system performance indicators such as safety and timeliness.

A phenomenon will occur with a certain probability, which can be subjective or based on the historical data, in a geographical area. Moreover all the connections in a causal model have probabilities associated. Between a phenomenon and a consequence multiple paths may exists that have different probabilities. In this project, a method is developed for filtering the most relevant set of paths seeking for a maximum probability path from each consequence node to a phenomenon. A dynamic programming approach is used that utilizes the Bellman's principle of optimality. The outcome of these calculations are used to describe the natural hazard of different extreme weather events in each climatological area and directed to various transport modes. The final consequences stand for the endpoint of the concatenation of events starting from extreme weather phenomenon and ending to societal effects. These final consequences include 1) time delays, 2) infrastructure damages or increased maintenance costs and 3) accidents. The hazard indicators vary between values 0.01 to 0.99 depending on how strong the relationships are in the causal chains from weather phenomena to final consequences. The probability values were derived using several methods: values obtained using statistical empirical materials or case studies, expert assessments, or the combination of both.

2.7.17 SEERISK

(www.seeriskproject.eu)

This EU project aims at the harmonization of risk assessment methodologies in southeast Europe. A common risk assessment methodology in SEERISK project has been developed and was applied in six case study areas (Markovic et al. (2016), Papathoma-Köhle et al. (2016)). The direct and indirect estimated damage of these events exceeded 200 million Euros. This study demonstrates an application of the SEERISK methodology for drought and drought-related wildfire risk assessment.

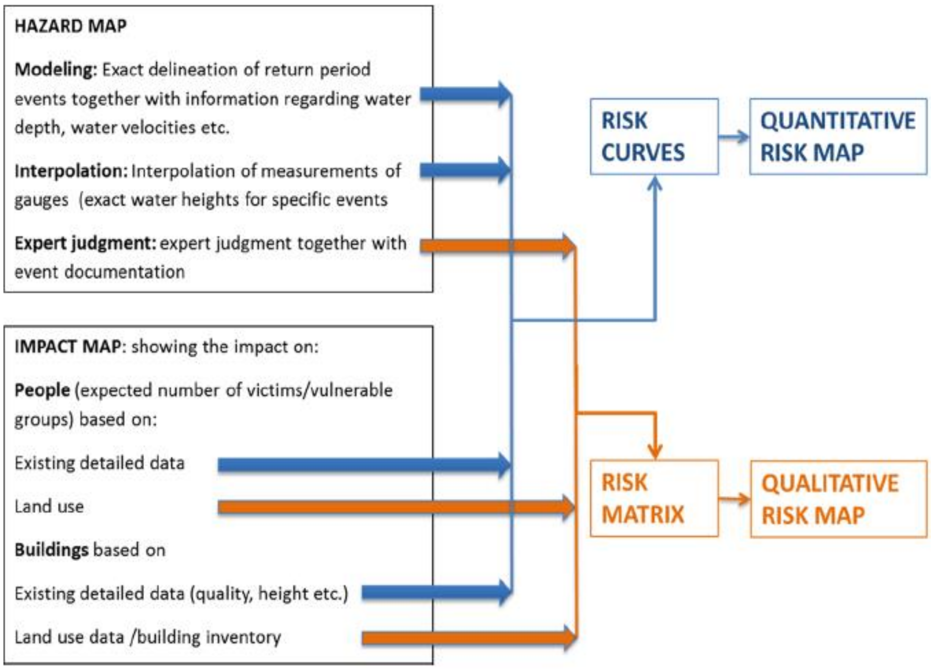


Figure 12: SEERISK risk assessment methodology for droughts.

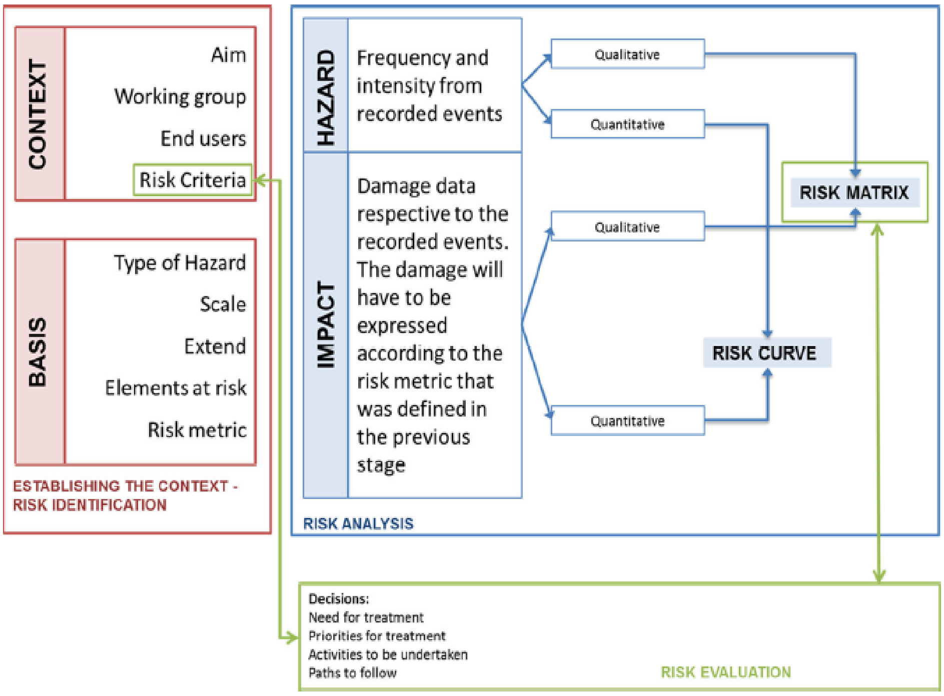


Figure 13: SEERISK overall methodology.

2.7.18 ClimWatAdapt

(www.climwatadapt.eu)

In the first step of the integrated assessment framework developed by ClimWatAdapt, all information is collected into a comprehensive database. There is the assessment of vulnerability hotspots, vulnerable sectors, and the assessment of appropriate adaptation strategies. The central component in is a database (DB) with the relevant parameters coming from the reference scenarios and other generic information. A set of vulnerability indicators (VI) is defined and the results are stored in the DB. Since these data are existent at different spatial levels across Europe, such as river basins, NUTS-2 units, or countries, a set of processing functions is needed, which allows geo-spatial analysis in order to evaluate the impact indictors and store the results in the DB. At this point, the basic information for the vulnerability assessment is prepared. The vulnerability assessment is structured by the DPSIR framework (Drivers, Pressures, State, Impacts, Response) that is commonly applied and widely adopted by the European Environment Agency (EEA) because of its simplicity, wide acceptance and its applicability for reporting environmental problems. Concerning the vulnerability assessment, most of the datasets came from large-scale modelling, especially those related to water quantity. Hydrological and water use related model outcomes were merged. In this way, indicators were exclusively generated for describing the future of Europe’s freshwater resources. From the modelling perspective, 9 selected measures were evaluated by applying a model; the selected measures address water withdrawal in a sense of changing technologies and efficiency rates and water supply in terms of desalination and waste water reuse. For the EU, direct economic costs of flooding and their final implications in terms of growth and wealth for the economic systems affected were estimated by using a Computable General Equilibrium model (CGE).

2.7.19 CREW

(http://www.extreme-weather-impacts.net)

A key component of the CREW project was the development of a 'Severe Weather Events Risk and Vulnerability Estimator' (SWERVE). SWERVE used the latest probabilistic climate model output and climate downscaling tools to project the frequency and severity of future extreme weather for the South East London Resilience Zone (SELRZ) for two periods centred on the 2020s and 2050s assuming medium greenhouse gas emissions. The historical period of 1961-1990 was also used as a reference baseline indicative of 'current' conditions. This output was then applied to models of weather-related hazards comprising flooding, heat waves, subsidence, drought and wind. High resolution maps and charts of current and future hazards have been produced based on location specific and user-relevant thresholds. This has resulted in one of the broadest assessments to date of different weather-related hazards impacting on the city scale. The Extreme Weather Event Socio-Economic Model (EWSEM) has sought to advance the analysis of local socio-economic impacts of flood risk in the context of a changing climate. CREW addressed four major challenges: (1) understanding the effects of long term increases in flood risk (as opposed to the impacts of particular flood events); (2) accounting for agglomeration economies and other spatial spillovers; (3) modelling interactions between sectors; and (4) understanding the behavioural response to flood risk.

2.7.20 FEMA HAZUS

(http://www.fema.gov/hazus)

HAZUS is a risk assessment methodology for analyzing potential losses from floods, hurricane and earthquakes and distributed by FEMA. HAZUS couples scientific and engineering knowledge with geographic information systems (GIS) technology to estimate physical, economic, and social impacts of disasters. It graphically illustrates the limits of identified high-risk locations due to earthquake, hurricane and floods. Users can then visualize the spatial relationships between populations and other more permanently fixed geographic assets or resources for the specific hazard being modeled, a crucial function in the pre-disaster planning process.

2.7.21 CORFU

(http://corfu7.eu/)

The CORFU project adopted novel methodologies and models into a DPSIR framework for investigating the flooding impact and a city's resilience to cope with such events under various current and future scenarios. The assessments were based on detailed hydrodynamic analyses and damage estimations in different urban growth and climate change conditions, as well as a series of adaption strategies. CORFU developed a Bayesian probabilistic optimisation algorithm for urban growth modelling to estimate the parameters required for urban flood modelling in mega cities. The results were analysed using a GIS-based damage assessment model to quantify the impacts. The quantitative and qualitative attributes of a flooding event were integrated into the Flood Resilience Index to describe the ability of urban infrastructure to deal with flood events. The CORFU framework was implemented in seven case studies – Barcelona in Spain, Beijing in China, Dhaka in Bangladesh, Hamburg in Germany, Mumbai in India, Nice in France and Taipei in Taiwan. Each of the case studies has different environmental and socio-economic features and flooding problems to be tackled with. They also have a variety of data availability and quality, infrastructure status, future planning and policy making mechanisms. The generic framework developed in CORFU allowed the comparisons between European and Asian cities to be made, which shows the potential for a wider implementation.

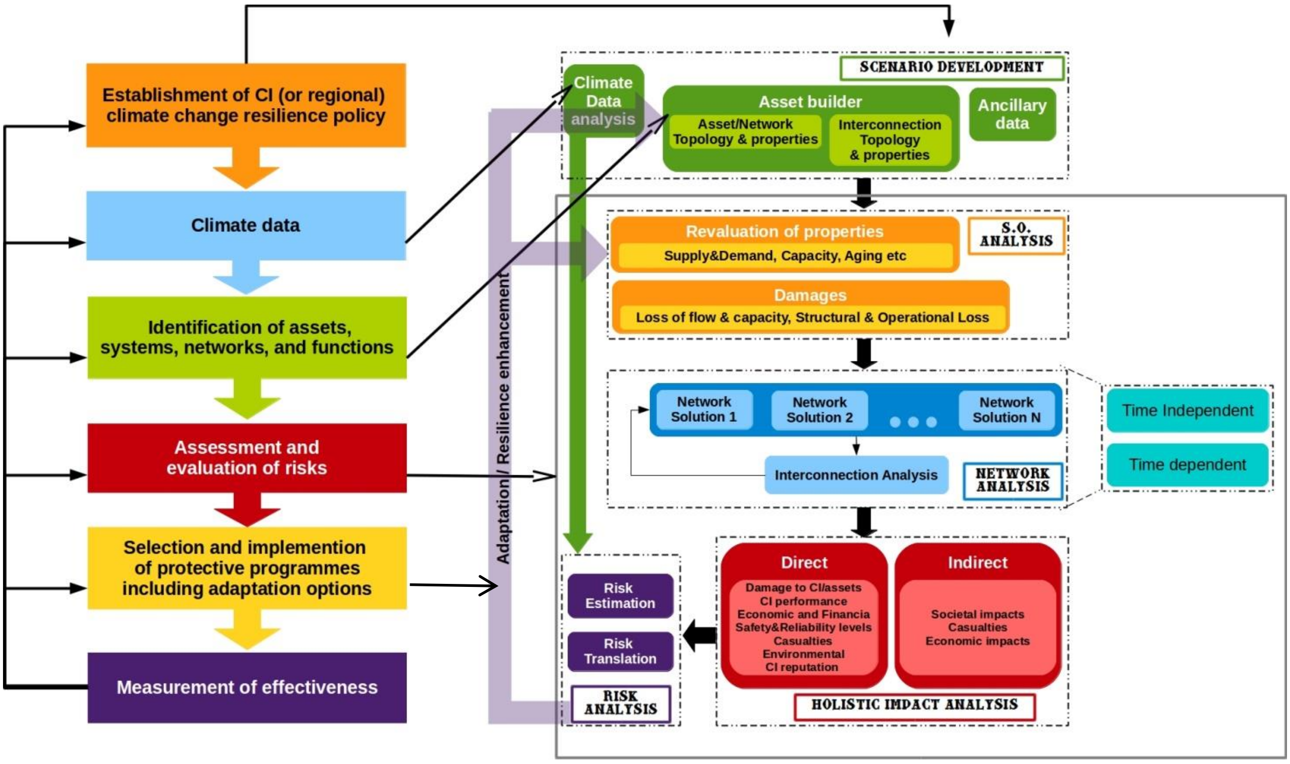
2.7.22 PEARL

(http://pearl-fp7.eu/)

The PEARL project focuses on the impact of extreme events in coastal regions, where rapid urbanisation is taking place in many countries. The pace of development is often too fast to be properly managed. Combined with climate change, flood risk is quickly increasing and threatening coastal communities. To cope with the problem, PEARL is developing a holistic flood risk assessment framework to investigate the consequences of extreme events to the society. PEARL adopts an Agent Based Model (ABM) to analyse the impact on different types of sectors or infrastructure. It particularly considers the cascading effects to represent the indirect impact and economic loss caused by extreme events. Therefore, adaptive risk management strategies for coastal communities can be evaluated and implemented to strengthen the flood resilience.

3 Risk management and risk assessment approach of EU-CIRCLE

This chapters introduces the EU-CIRCLE risk management framework, through a detailed description of its main components, and potential application in studies related to Critical Iinfrastructures resilience to climate change. The framework process, schematically depicted in Figure 14, introduces elements from the processing of climate information and related climate hazards (WP2), and the CI resilience and adaptation approach (WP4). The described modeling process to estimate and quantify risk will be introduced into the CIRP (WP5)



Risk management process Risk Modelling process

Figure 14: EU-CIRCLE framework

3.1 Overal concept and process steps

The proposed approach within EU-CIRCLE aims to provide a comprehensive framework to identify the risks of multi – climate hazards to heterogeneous interconnected and interdependent critical infrastructures, as the first step to improving resilience of vulnerable social and economic support systems to climate change impacts while climate proofing existing critical infrastructure (in terms of identifying indicators and reference states, anticipated adaptive / transformation activities, and investment costing).

The infrastructures which are assessed within EU-CIRCLE are highly sensitive to high or low values of meteorological parameters, as identified in "D1.3 EU-CIRCLE strategic context". The analysis of extremes or changing climate patterns is used to determine an optimum balance between adopting high safety and societal protection standards that are very costly on the one hand, and preventing major damage to equipment and structures that are likely to occur during the useful life of such infrastructure on the other hand. Most existing infrastructures have been designed under *the assumption of stationary climate* conditions using historic values and observations. This basic concept assumes that although climate is variable, these variations are however constant with time, and occur around an unchanging mean state. This assumption of stationarity is still common practice for design criteria for (the safety / security levels of) new infrastructure, even though the notion that climate change may alter the mean, variability and extremes of relevant weather variables is now widely accepted. Even new infrastructures, or expansion – adaption of existing ones is typically designed on the basis of historical information on weather and climate extremes as these have been identified in pertinent engineering standards, such as the European standards on structural design (EUROCODES).

Our aim is to use a validated scientific approach based on the existing operational approaches discussed in Section 2 of this document identify existing, evolving and emerging climate risks/opportunities, vulnerabilities to interconnected infrastructures and adaptation options, that are summarised in the following elements:

- Assessment of risks using improved methods of assessment and new knowledge, from the literature, partners expertise and opinions of stakeholders.
- Identification of how climate change risks to CI interact with other socio-economic factors to affect the level of risk or opportunity.
- Assessment of the perceived level of "acceptable risk", i.e. the level of risk that each infrastructure owner/operator or societal group is willing to accept before supporting the implementation of any disaster risk reduction and/or climate change adaptation actions
- Estimation of the effect of different risks acting together (multi-hazard), either due to concurrent timing, acting on the same location or the same receptor (coincidence).
- Assessment of how ageing or asset (infrastructure) state deterioration has an impact on risk levels, safety margins and its reliability. Determining whether changing climate patterns in the future should lead to changes of engineering standards and climate thresholds, to make CI more robust to hazards of greater magnitude and frequency.
- Assessment of the magnitude of impact for different hazards and for different impact / consequence categories.
- Assessment of the uncertainties, limitations and confidence in the underlying evidence, data used and analysis for different risks.
- Production of risk estimates that can directly communicate the evidence in such a way that is credible, robust, relevant and can be used to inform decisions (e.g. adaptation, risk reduction) by stakeholders, governments etc.
- Provision of new insights and improved evidence-based analysis of recorded disasters and their major impacts, through their re-examination.

The framework description itself must be flexible and generic enough to facilitate a multitude of different assessment situations, and at the same time provide meaningful guidance and allow to compare the outcomes.

3.2 Analysis question

The proposed risk assessment is equally applicable in different analyses, pertinent to the EU-CIRCLE that are introduced below.

Analysis 1. Assessment of the current climate related risks for a specific hazard to a single CI / CI network / area of interest with interconnected and interdependent CI

Initially a description and quantification of the impact of climate parameters (and secondary hazards) on the performance levels of the CI (also accounting for the economic, social and environmental and reliability components) will be performed. "Current" may be interpreted as "present-day" risks, but it may also mean a point in the past depending on what baselines are used in the available evidence. Part of this analysis also identifies climate-related thresholds (EU-

CIRCLE D3.2 Report of climate related critical event parameters, M31) or events which pose a specific risk, so that these can be precisely examined and analysed. A description and quantification of the key socio-economic impacts that results from the disruptions of services due to climate variability will then be introduced allowing for a collective analysis and assessment.

Analysis 2. Examination of how key drivers may alter risk in the future, or expose new risks (climate change)

Based on an assessment of how climate change will shape the future, and on information on thresholds relevant to the specific hazards under examination, a customised quantification of the latest evidence on future climate drivers and therefore impacts will be undertaken, including an assessment of the uncertainties related to such information. When considering changes in a particular event or threshold, the EU-CIRCLE approach will evaluate the evidence on the likelihood of that change occurring. The assessment will use the following timescales, as agreed at the 2nd EU-CIRCLE project workshop:

- ✓ Next 20 years
- ✓ 50 years
- ✓ 100 years
- ✓ The lifetime of the infrastructure

This analysis will include a baseline assessment of the risks to CI assuming no additional adaptation options (similar CI exposed to future hazards) under various climate change scenarios (see Figure 15), as well as a second assessment which considers how currently planned or future potential adaptation actions will affect the overall scale of risk in the future. This will describe/quantify potential interactions between risks or adaptation options and determine the net effects of risks / resilience or adaptation acting together, for both incremental change and extreme events. Each future estimation will be placed together with a “confidence estimate”.

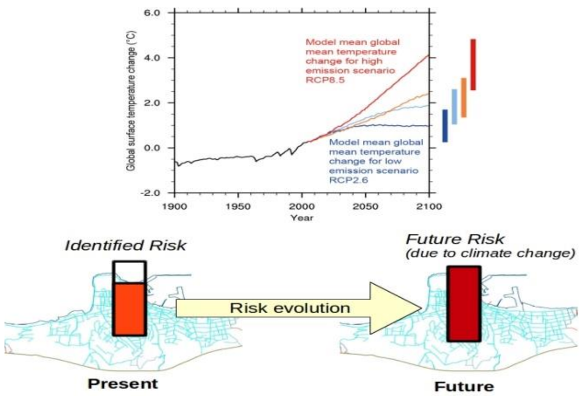


Figure 15. Identify, assess and quantify the risks that CI are exposed to, and how these will evolve under different climate change scenarios (e.g RCP 2.6) under no-adaptation policy options.

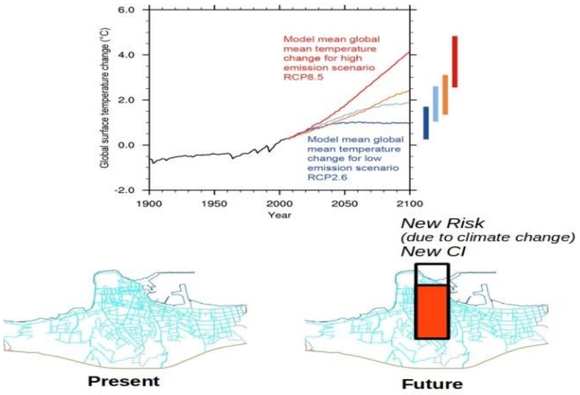


Figure 16. Identify new risks that may apprear under future climate conditions, or due to new CI being planned (or expanded) in the future

Analysis 3. Identification of climate change adaptation or risk mitigation options and definition of priorities

EU-CIRCLE will also be used to examine alternative strategies for mitigating risks to CI (see previous steps in Analysis 1 and Analysis 2) and strengthening their resilience (as identified in D4.1) such as: enhancing business continuity and the defences of interconnected infrastructures and implementation of long term adaptation options. A comparative assessment of these, using well identified criteria (e.g. cost – benefit analysis) will return scientific evidence for supporting informed decision making. The process will result in a detailed narrative of identified risks (from an amalgamation of various user inputs and scenario builds and the results and their subsequent interpretation of different numerical models).

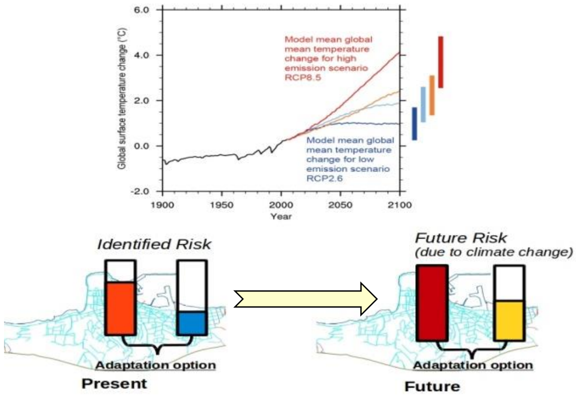


Figure 17. Assessing risks in the future under the application of different adaptation options policies and measures.

3.3 Risk management within EU-CIRCLE

3.3.1 The science/operational background

This section is devoted to describing background to the EU-CIRCLE interpretation of the risk management process. It is based on the following documents and operational contexts:

- International Standards on Risk management ISO 31000 (ISO, 2009) and AS/NZS 4360 (AS/NZS, 1999)
- Definitions and categorization of interdependencies between infrastructures from Rinaldi et al. (Rinaldi 2001 and 2004),

- The National Infrastructure Protection Plan Risk Management Framework (NIPP) of the U.S. Department of Homeland Security (DHS 2013 a, b) as introduced in chapter 2.
- Analytical steps related to resilience capacities as described in EU-CIRCLE "D4.1 Resilience framework".

Ideal workflows for risk management are provided by international standards such as ISO 31000 (ISO 2009) and AS/NZS 4360. The following figure is taken from ISO 31000 standard and depicts the ideal risk management process.

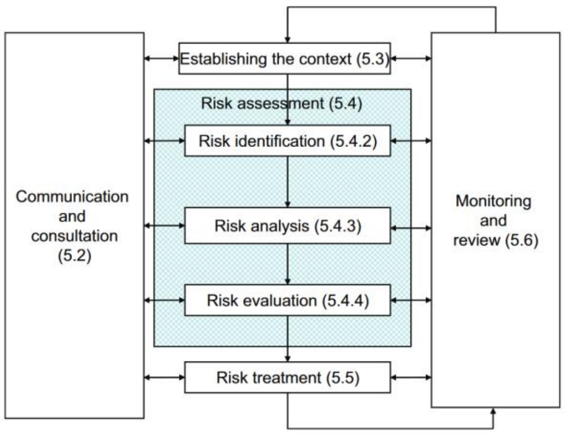


Figure 18: Risk management process proposed by ISO 31000 (ISO31000, 2009)

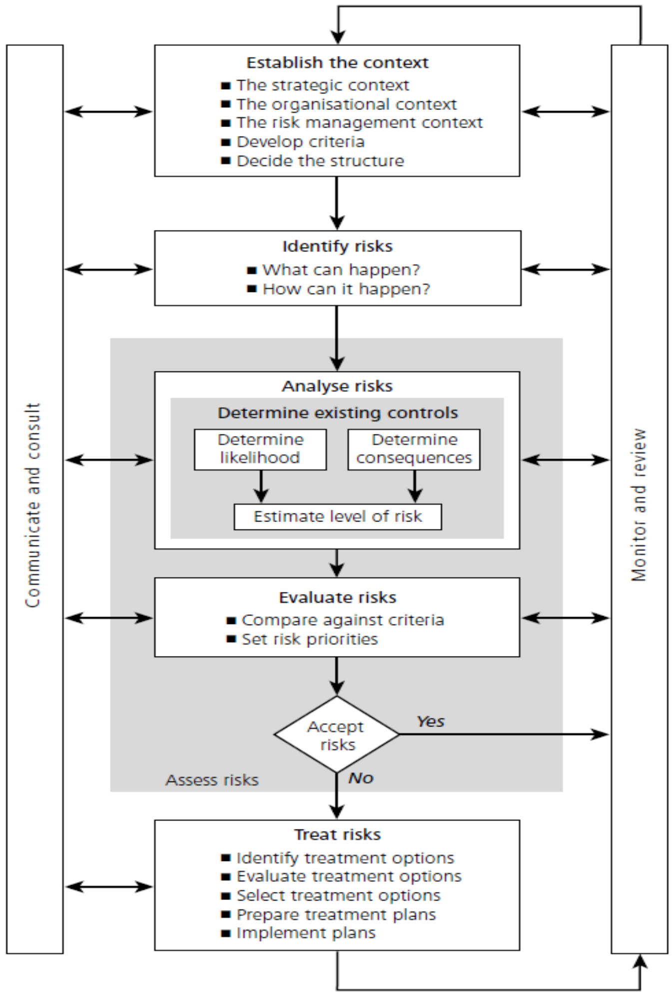


Figure 19: Risk management process proposed by AS/NZS 4360 (AS/NZS, 1999)

Risk management is depicted in both standards identically. However, ISO 31000 is considerably more generic and abstract whilst AS/NZS 4360 provides more concrete advice by means of explanations, definitions and examples. The following figure presents the risk management process as proposed by AS/NZS. However, neither the ISO nor AS/NZS standards on risk management explicitly address resilience as a development objective or as a diagnostic approach.

Comprehensive studies on (national) frameworks as well as software tools dedicatedto risk management, including risk assessment, are provided for example by Pederson et al. (2006), Yusta et al. (2011) and Giannopoulos et al. (2012). Yusta analysed 55 methodologies and applications related to risk assessment and discovered variations between them in terms of:

- critical infrastructure sectors considered,
- modelling techniques (such as agent based / systems dynamics / rating / network theory),
- maturity and availability of detailed methodological information and software tools (e.g. restricted access/ commercially available / on development) and
- risk assessment stages actually facilitated

Further differences can be explained by the target audience. However, commonalities exist in the general approach to how risk is assessed, which is considered for the analytical stages should be undertaken for the management of risk:

- hazard identification,
- risk assessment,
- prioritization of actions,
- programme implementation, and
- measurement of effectiveness.

Smaller differences obviously exist in the clustering of single procedural steps to more generic, aggregated working stages. For example: “prioritization of actions” can be conceived either as a single working step or can constitute one element within “programme implementation”.

The NIPP describes the aim of a risk management framework to establish the process for combining consequence, vulnerability, and threat information (DHS 2013a and DHS 2013b). It aims to merge the efforts in the protection of critical infrastructures and key resources from both the public and private spheres. The NIPP includes the following steps[2]:

1. Establishment of security objectives
2. Identification of assets, systems, networks, and functions
3. Assessment and evaluation of risks
4. Selection and implemention of protective programmes
5. Measurement of effectiveness

3.3.2 EU-CIRCLE process of risk management

The five working steps of the NIPP provide the frame of reference for the EU-CIRCLE risk management framework, which has being modified according to the project’s scope and objectives (Figure 14). The following steps make up the EU-CIRCLE risk management process:

1. Establishment of CI (or regional) climate change resilience policy, or specific business orient decision that will be addressed within the proposed framework
2. Identification, collection and processing of climate related data and secondary hazards
3. Identification of assets, systems, networks, and functions
4. Assessment and evaluation of risks
5. Selection and implemention of protective programmes including adaptation options

[2] Yusta et al. (2001) describes the NIPP as a six-step process, whereas the DHS call it five-step. DHS aggregates step 3 and 4 as „assess and analyse risks“. Content wise, there is no difference.

6. Measurement of effectiveness

Step 1 - Establishment of CI (or regional) climate change resilience policy

This step includes the identification of the resilience policy(ies) of a CI or of a region within which interconnected CI networks reside. Typically, these policy objectives have a timespan of multiple years and may be related to specific issues or cross-sectoral matters. Typical questions to consider in this step include for example:

- What must and what should be protected?
- Which potential consequences are relevant (economic, social, environmental etc.) for this appraisal?
- What are the priorities?
- What is an acceptable risk and what is a non-acceptable risk?

Within this step, internal and external factors are also identified. According to ISO 31000, these includes – but are not limited - to:

- Social, cultural, political, legal environment;
- Key drivers and trends having an impact on the objectives;
- Policies, strategies already in place;
- Capabilities such as resources and knowledge;
- Organizational structures, roles and accountability, relationships between actors.

Step 2 – Identification, collection and processing of climate related data and secondary hazards

This step involves the identification of the (climate related) pressures and parameters that influence the interconnected network of CI within a region of interest. It involves analysis of the historic climate (and secondary hazard) data, future climate projections from existing databases and/or if this required the provision of specialised simulations.

Step 3 – Identification of assets, systems, networks, and functions – Interdependent Infrastructure analysis

This step will identify and characterise the infrastructure that is likely to be affected by climate hazards. In order to achieve this, a structured analysis of all CI elements that provide "critical services" will be undertaken. The following approach is proposed:

- Compilation of a registry of assets for all EU-CIRCLE relevant sectors .
- An analysis of interconnections, networks and (inter-) dependencies including the various types, such as physical, cyber, geographic, logical or social (inter-) dependencies.

An extensive analysis of the CI network(s) asset definition and interconnection is elaborated in section 3.4.3 of this document. An extensive analysis and assessment of the identified assets within EU-CIRCLE will be delivered in "D3.1 Registry with CI assets and interconnections".

Step 4 – Assessment and evaluation of risks

The primary aim of the EU-CIRCLE framework is to provide a common ground whereby different risk assessment methodologies and modelling schemes, from the critical infrastructure and the natural hazards communities can co-exist and interact in a logical manner. To achieve this different risk assessment schemes will be harmonized into a single interoperable approach or alternatively "translating solutions" will be created between the different risk approaches.

The minimum basis of the proposed risk assessment framework is to be compatible with

- ✓ the National Risk Assessments (Section 2.3)
- ✓ EPCIP programme (Section 2.2.1)
- ✓ IPCC report (section 2.2.3)
- ✓ Sendai Framework with Disaster Risk Reduction (Section 2.2.4)
- ✓ International standards, e.g. ISO 31000 Risk Management.

A common understanding and clear elucidation the final risk estimation allows for the easy and direct interpretation of the derived risk metric. Within EU-CIRCLE different alternatives could be employed such as numeric estimation of risk (given restrictions in providing a single number from different types of impact estimates) and/or uing the risk matrice approach in accordance with recenet practices and with finite number of classes. As an example, *risk matrices in national risk assessment plans* have been set with quantified probability/likelihod and impacts/consequences on a 5x5 scale (the Risk Matrix approach in Figure 20), these categories differ and could lead to different interpretations of severity of risks and, ultimately, different conclusions. According to this report some of the risk matrices are numbered 1 to 5 or use letters A to E – 1 and A being low probability/impact and 5 and E being high probability/impact, whereas other approaches use a specific terminology to express ranges.

Additionally, within EU-CIRCLE the "acceptable level of risk" should be determined by users of the CIRP, which will guide the analysis of adaptation policies and mitigation options and provide a reference level of comparison. The acceptable level of risk is a "user defined" parameter.

Probability/Likelihood ↑						
	Very likely/Certainly					**Critical**
	High				**High**	
	Medium			**Medium**		
	Low			**Low**		
	Very low, unlikely	**Very low**				
		Negligible, minor,	Small	Medium, moderate	high	Severe
	Consequences →					

Figure 20. Example 5x5 Risk matrix

The level of very low risk (blue) usually is considered as broadly acceptable or negligible risk. On the other hand, level of Critical risk (red) is considered as non-acceptable risk i.e. this risk cannot be justified on any grounds. The rest of the risk levels within risk matrix (green, yellow and brown) are usually considered as the tolerable risk, meaning that it is tolerable only if risk treatment (reduction) is impractical or if its resource requirements (financial and human) are grossly disproportionate to the improvement gained.

The proposed risk modeling approach of EU-CIRCLE is described in section 3.4.

Step 5 - Selection and implemention of protective programmes including adaptation options

This step will involves according to ISO 31000, the process of "selecting one or more options for modifying risks and implementing those options". The AS/NZS Standard 4360 formulates: "Selection of the most appropriate option involves balancing the cost of implementing each option against the benefits derived from it". An ideal work flow for step 5 is proposed by AS/NZS 4360 which is also the base recommended for EU-CIRCLE. Risk treatment activities need to be identified, selected and implemented, if one or more risks are considered to be non-acceptable.

In detail, this step consists of the following:

- Identification of resiliency enhancement(s) / adaptation option(s), that aim to:
  - reduce the likelihood of occurrence
  - reduce the impacts / consequences
  - transfer in full or partly the risk
  - avoid risk
- Assessment of the risk treatment, resiliency enhancement , CI adaptation options options
- Preparation of risk treatment, resiliency enhancement , CI adaptation plans
- Implementation of risk treatment plans (out of the scope of EU-CIRCLE)

Within the EU-CIRCLE approach, risk treatment may be approached using a hierarchical strategy and examining different alternative options leading to the elimination and/or reduction of risk levels. The priority of the examined solutions is related to the elimination of identified risk, followed but suggested actions towards risk reduction. ***The risk treatment options are directly linked to the CI resilience capacities identified in "D4.1 EU-CIRCLE CI resilience framework to climate hazards 1st version".***

Table 2: Link between EU-CIRCLE Risk Management and Resilience

Resilience Capacity (D4.1)	Reduce Likelihood	Reduce Consequences	Transfer risk	Avoid Risk
Anticipatory	X	X	X	X
Absorptive		X		
Coping		X	X	
Restorative		X	X	
Adaptive				X

Step 6 - Measure effectiveness

Once one or more risk reduction measures are introduced, progress towards achieving the objectives must be evaluated regularly. Risks, effectiveness, goals or other circumstances may change after initial implementation. Monitoring and review helps to keep the plans relevant.

Within EU-CIRCLE this step will be implemented during the analysis of the examined case-studies (WP6) in order to assess the capacity of the risk management framework to (according to ISO31000 & NIPP 2013 goals):

- ensure that risk controls are effective and efficient in both the design and operation of CI;
- obtain further information to improve the risk assessment process;
- analyse and learn lessons from events (including near-misses), changes, trends, successes and failures;
- identify when risk treatments and policy objectives must be revised; and
- identify emerging risks.

Horizontal implementation

Within EU-CIRCLE, the Climate Infrastructure Resilience Platform (CIRP) which will inherently include the developed risk assessment framework, will support the climate related policy objectives. These technologies must be adapted to the actual, individual assessment context. The concrete and most relevant results include:

- The definition of goals;
- Nature and types of causes and consequences and how they will be measured;
- Assessment of the likelihood of appearance of a hazard under present and future climate scenarios;
- Timeframes of the likelihood and consequences;
- Identification and specification of the decisions that have to be made;
- Definition of methodologies regarding risk assessment (how is the level of risk determined);
- Determination of a methodology for evaluating effectiveness.

3.4 Modelling risk within EU-CIRCLE

The EU-CIRCLE approach for assessing risk can be used to support the entire project's objectives and scope of assessing an interconnected infrastructure's exposure to climate stressors and determining which hazards carry the most significant consequences (section 3.6) leading to an assessmen of their present day resilience. **The Consequence – based Risk Management (CRM) generic approach has been selected**, and analyzed in the following paragraphs to support the intended analysis of EU-CIRCLE. The key advantage of this approach is that it uses an optimization-based prescriptive model of system operation as the starting point for the study of infrastructure behaviour: *these models inherently accommodate disruptions to infrastructure as straightforward changes to input data* (Kim (2008), Gardoni (2009), Garcez & Almeida (2014), Wennersten et al. (2015), Shand et al. (2015)).

The proposed modeling approach encompasses an identity simulation of infrastructures' operating protocols, mimicking decisions for sustaining flow of services using quantitative tools that can help determine how to operate a system, even in the presence of disruptions. This technique requires that the essential domain-specific details about the infrastructure system's operation in terms of its operator's goals and the limitations on its capabilities are captured and depicted. It also incorporates unambiguous measures of system performance for the infrastructure, and of the different business continuity alternatives and adaptation measures to be introduced.

A special feature of the applied CRM approach is that it places the modelling and analysis of interconnected and interdependent infrastrutcures as a core component. CIs are fundamentally (inter-)connected through a wide variety of mechanisms and dependency types (Rinaldi et al., 2001), such that a mutual relationship exists between the states of any given pair of components in the systems and/or networks. For instance, power grids depend on gas networks to fuel generation units. Water networks provide cooling and help to control emissions from coal-based power generators. Water and gas networks are heavily dependent on power for operating pumping stations and control systems. If a particular system is damaged, this damage is propagated to other systems due to the interdependent nature of the systems (i.e., cascading failures). Therefore, an emerging need exists for modelling complex and interdependent critical infrastructure to better understand their susceptibility to potential hazards.

Consequence-based Risk Management has been used in climate/disaster risk reduction across regions or systems that incorporate identification of uncertainty in all components of climate risk modeling and quantify the risk to societal systems and subsystems (Kumar (2015), Cimallaro (2016)). It also enables policy-makers and decision-makers to ultimately develop risk reduction strategies and implement mitigation actions. The result of this action will be introduced into the Climate Infrastructure Resilience Platform, an IT tool that integrates spatial information, data, and visual information into an environment for performing climate loss assessment and analysis. The developed interface will integrate a variety of data types aand sources from diverse users and CI stakeholders. The proposed EU-CIRCLE risk methodology facilitates the definition and connection of CI specific and generic analyses to create workflows, explore and introduce new scientific possibilities by creating new workflows from the existing components.

A workflow of the EU-CIRCLE variant of the CRM process (Figure 21) where different climate hazards (scenarios) will be examined corresponding to specific policy/scientific questions such as those described in D1.3 and D1.5 are illustrated below:

- What is the current risk level of one infrastructure in a region, due to a specific climate hazard, and how is risk estimate anticipated to change in the future?
- Which asset of an infrastructure is most vulnerable to extreme events, and could propagate its impacts to interconnected infrastructures' assets?
- What is the most damaging climate hazard in a region? how is this attributed to its constitutional elements (society, economy, etc)? how will its behaviour may change in the future?
- How resilient are the infrastructures of region to a specific climate hazard;
- Which is the optimal adaptation measure for an infrastructure under a list of potential alternatives? Is the same adaptation measure also beneficial for other climate hazards?

Scenarios will be simulated and assessed starting from **a baseline scenario** (without the presence of a hazard) and compared to the impacts from another scenario run (with the presence of hazards). In general, damages derived from hazard events can be described through damage functions on the critical parts of Critical Infrastructures assets which directly or indirectly affect demand, supply, and capacity on the networks nodes which in turn results changes on the network's attributes. Subsequently a simulation will be performed consecutively on the CI network (e.g. starting from the electricity network) and then to another network (e.g. transportation) and so on, until all parts of the interdependencies between networks (e.g. electricity and transportation network) are accounted for. During the preliminary analysis, damages-impacts are placed into the interconnected network, while in the last step, an analysis of the new modified interdependent network is performed comparing the results with those of the basic scenario analysis, in order to define on the one hand which assets are affected while on the other hand to predict network functionality. The consequence of a risk is defined as a measure of the disruption and impact of a incident not only on a single asset, but on society in general and is thus used in conjunction with likelihood to assess its overall severity by combining the likelihood and the consequence assessments using a 5-categories risk matrix. This matrix constitutes the basis of our risk assessment framework. It is an important tool used to map each combination of likelihood, probability and consequence severity to a single risk level (Very Low, Low, High, Severe and Critical).

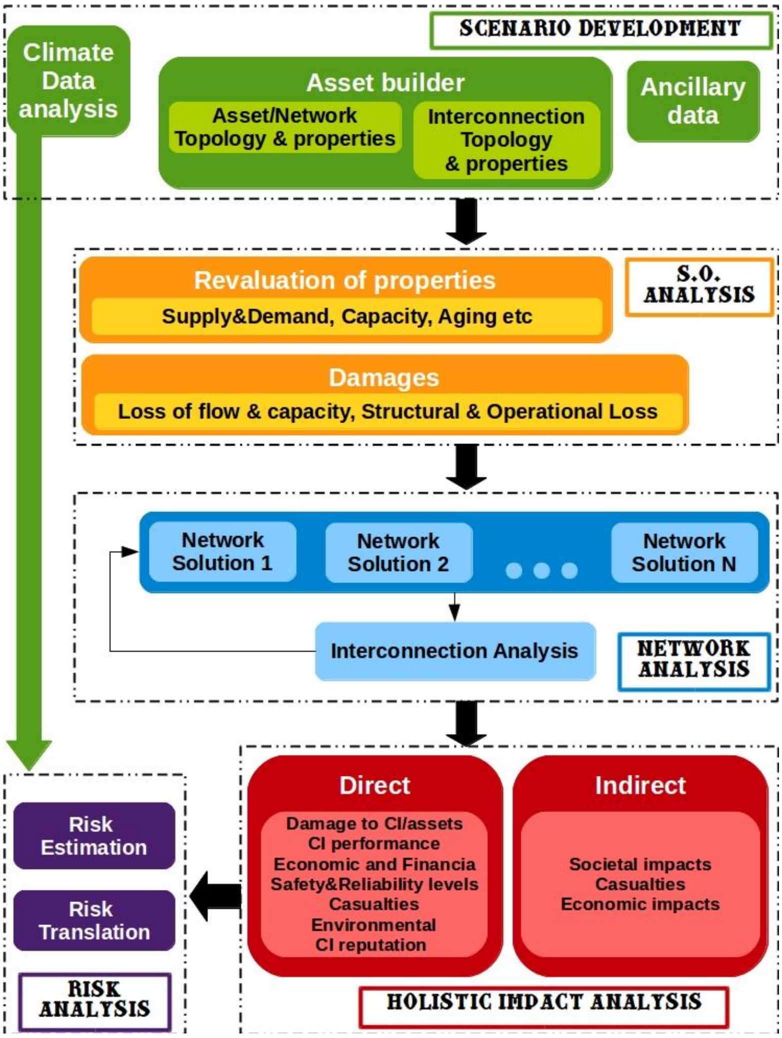


Figure 21: EU-CIRCLE generic risk modelling methodology

The proposed CRM approach within EU-CIRCLE has the following features

- ✓ Arbitrary level of spatial disaggregation depending on the desired analysis,
- ✓ Attention to different timescales, which is highly dependent on the climate information used
- ✓ Multi-hazard risk assessment with cross-sectoral interactions assessment.
- ✓ Consideration of resilience capacities - adaptation options

The EU-CIRCLE modelling approach, implementing the CRM, that will be implemented in CIRP, can be categorized in five distinct steps as schematically demonstrated in Figure 21 and analysed in the following paragraphs, namely 1) Scenario Development SD, 2) the Structural & Operational analysis SO, 3) the Network analysis NA, 4) Impacts assessment IA and 5) Risk and Resilience estimation RR; the links of which to the EU-CIRCLE risk management process is presented in Figure 14.

Model Step 1: Scenario Development (SD) constitutes the initial phase of the proposed approach, described in Sections 2, whereby:

- the scientific question or policy objective is determined as well as a selection/processing of the existing data needed to reach the overarching objective
- the climate data from multiple sources are processed and ingested
- The network(s) is created using a network builder tool from inputs including the topology, properties and interconnections of CI assets. The resulting infrastructure consists of connections between nodes of the same networks, interconnections between different networks, flow values that characterize the link between nodes and capacity as a property of nodes.

The result of the network builder combined with the climate data are used as inputs for the second step.

Model Step 2: The Structural & Operational (SO) analysis accept as input the constructed network –and- climate data and returns an output quantifiable information on how different assets react to different intensity events, described in Sections 3.4. The asset behavior can be deduced via, fragility equations, tabulated values and/or any other model that express changes from the normal state due to a hazard. Two different options exist:

- changes to network properties which include changes in supply and demand of nodes and capacity of links, without any physical or operational damage.
- changes to the network properties due to structural damages (partial or full), personnel loss, etc.

Model Step 3: The Network analysis (NA) procedure utilises the results of the SO step and calculates for each network the simulated flow and estimates how each network affects its interconnected networks; see Section 3.5 of this document.

Model Step 4: The Holistic impact analysis (IA) is conducted where the quantified impacts due to the hazard under examination are calculated using the results of the NA step and other relevant information from the SO analysis (more details in Section 3.6). The impacts include direct consequences to the infrastructure and also impacts to society.

Model Step 5: The Risk and Resiliency Analysis ($\boldsymbol{RR}$). Using the estimated likelihood of the event (step1) and the results from the impact analysis (step4), the risk of a specific hazard is estimated and the resilience of the network (RR) is calculated, (which is described in Section 3.7, and Delivrable 4.1 respectively).

Due to existing assumptions, simplifications, and discretization of analysis parameters (see – Section 3.8 for further details), the assessment results will contain uncertainties. The accuracy of the description of the assets, their properties and how they react to a hazard, and the hazard itself, are uncertainty factors in the methodology. In order to make the results produced more accurate and reliable, it is necessary to improve the description and information of the infrastructure and to perform a sensitivity analysis concerning the hazard chosen, the fragility and damage curves/functions and the discretization of the topology.

The goal of the proposed approach is to enable us to perform extensive simulations of heterogeneous and interconnected networks, such as water, energy, transport, ICT, also allowing for the total (100% reduction) or partial loss of service. This can be achieved with the description of networks as a set of node and links between them. Moreover, connections between different kinds of networks are necessary in order to carry out interdependency analyses between different kinds of networks. Thus, the network analysis methodology can be categorized horizontally, that means each network is solved separately, and vertically , which refers to capturing the effect from one network to another. After the completion of network analysis and interdependency analysis, a holistic impact analysis and a risk assessment can be performed.

3.4.1 Risk Estimation - generic framework

In this section EU-CIRCLE defines a generalized risk assessment methodology for interconnected and heterogeneous critical infrastructure networks following the ISO31000 approach, where risk is defined as "the combination of the consequences of an event or hazard and the associated likelihood of its occurrence". This approach is also the most commonly employed approach in the Member states National Risk Assessment Plans (European Commission, 2010).

Formula 1

$$Risk = Hazard\ impact \times Probability\ of\ occurence$$

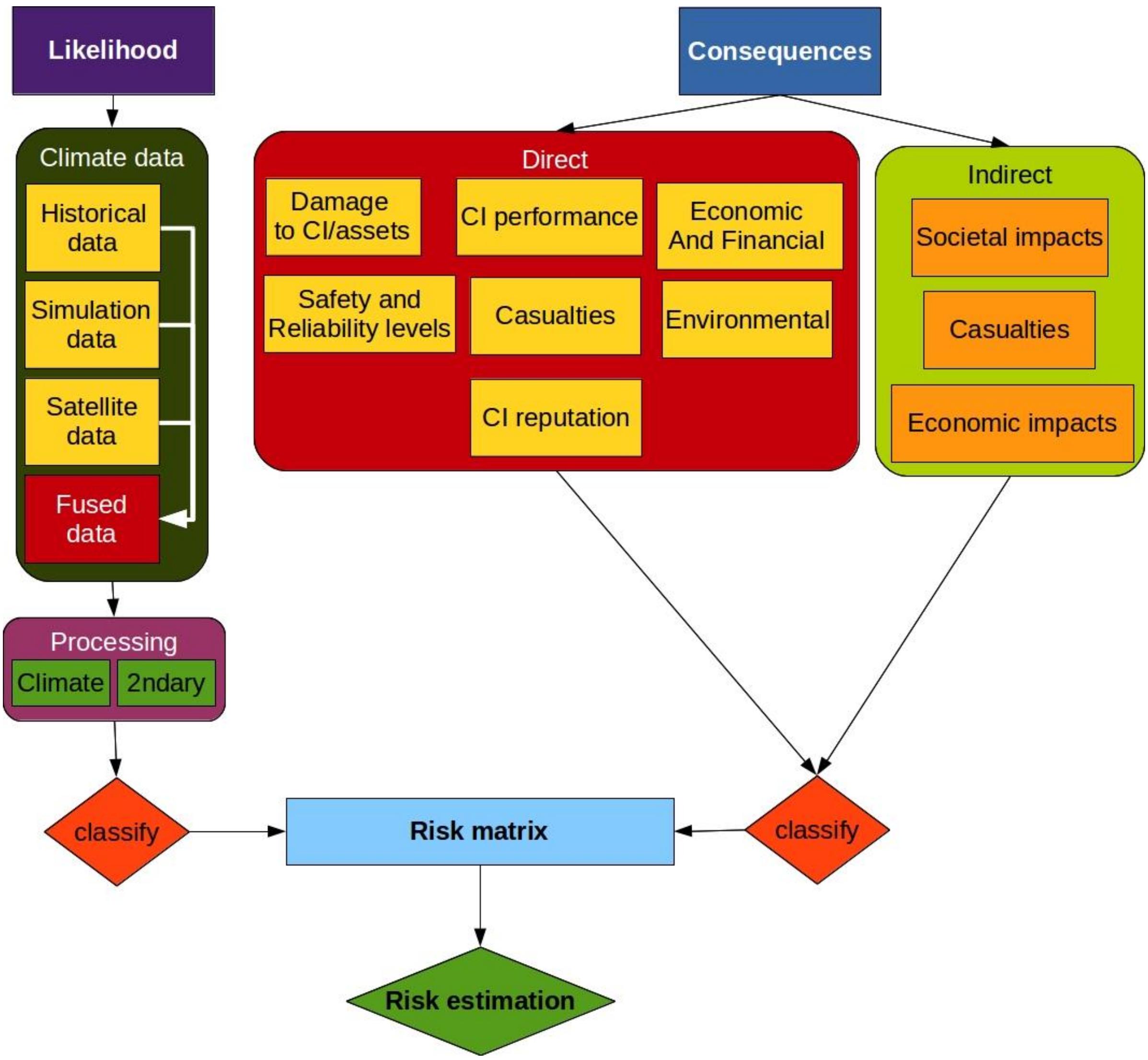


Figure 22: General Risk Assessment Framework Methodology.

In order to apply this approach, the following definitions are proposed:

Likelihood (probability of occurrence) refers to the initial probability of a risk scenario to occur and is usually defined as:

- frequency of one or more incidents at various time scales (as defined by CZ, IE, LT, NO, PL, HU in their NRAs)
- probability of occurrence within 1 year (as defined by EE, EL in their NRAs)

An explanatory approach on how to define the likelihood of climate hazards in this approach can be found in Section 3.4.2. Within EU-CIRCLE the number of different categories of likelihood/probability of occurrence can be user defined, although the most common approach (e.g. NRAs) the 5x5 risk matrix process is followed:

VERY LOW or VERY RARE	**LOW**	**MEDIUM**	**HIGH**	**VERY HIGH or VERY LIKELY**

The levels of likelihood, in the framework of EU-CIRCLE, are defined by the internationally accepted descriptive terms, classified into a set of five categories, corresponding to numerical values from the NRAs and IPCC (Table 3). :

Table 3: Examples from classifications of likelihood by the MS in their NRAs.

<table>
<tr><th>Country</th><th colspan="2">Very Low</th><th>Low</th><th>Medium</th><th>High</th><th colspan="2">Very High</th></tr>
<tr><td>CZ</td><td colspan="2">Occurs less than once in 1000years</td><td>Occurs once in 100 – 1000 years</td><td>Occurs once in 10 – 100 years</td><td>Occurs once in 1– 10 years</td><td colspan="2">Occurs more than once in 1year</td></tr>
<tr><td>EE</td><td colspan="2">Probability within 1 year: 0.005% to 0.05%</td><td>Probability within 1 year: 0.05% to 0.5%</td><td>Probability within 1 year: 0.5% to 5%</td><td>Probability within 1 year: 5% to 50%</td><td colspan="2">Probability within 1 year: 50% +</td></tr>
<tr><td>EL</td><td colspan="2">Probability within 1 year: less than 0.001%</td><td>Probability within 1 year: 0.001% to 0.01%</td><td>Probability within 1 year: 0.001% to 0.01%</td><td>Probability within 1 year: 0.01% to 0.1%</td><td colspan="2">Probability within 1 year: more than 1%</td></tr>
<tr><td>IE</td><td colspan="2">Once every 500+ years</td><td>Once every 100-500 years</td><td>Once every 10-100 years</td><td>Once every 1-10 years</td><td colspan="2">More than once every 1 year</td></tr>
<tr><td>LT</td><td colspan="2">Less than once in 100 years</td><td>Once in 50 to 100 years</td><td>Once in 10 to 50 years</td><td>Once in 1 to 10 years</td><td colspan="2">More often than once a year</td></tr>
<tr><td>PL</td><td colspan="2">1 in 500 years or even more rarely</td><td>1 in 100 years</td><td>1 in 20 years</td><td>1 in 5 years</td><td colspan="2">Once a year or more</td></tr>
<tr><td>SE</td><td colspan="2">≤0.0001 on a yearly basis</td><td>0.0001 – 0.001 on a yearly basis</td><td>0.001 – 0.01 on a yearly basis</td><td>0.01 – 0.1 on a yearly basis</td><td colspan="2">>0.1 on a yearly basis</td></tr>
<tr><td>UK</td><td colspan="2">Between 1 in 20,000 and 1 in 2000</td><td>Between 1 in 2,000 and 1 in 200</td><td>Between 1 in 200 and 1 in 20</td><td>Between 1 in 20 and 1 in 2</td><td colspan="2">Greater than 1 in 2</td></tr>
<tr><td>IPCC</td><td>Exceptionally unlikely</td><td>Very unlikely</td><td>Unlikely</td><td>Medium</td><td>Likely</td><td>Very likely</td><td>Virtually certain</td></tr>
<tr><td>IPCC</td><td><1%</td><td>1-10%</td><td>10-33%</td><td>33-66%</td><td>66-90%</td><td>90-99%</td><td>>99%</td></tr>
</table>

Note that IPCC also uses a different terminology for the likelihoof of an event.

Consequences – Impacts are the result of the realization of a hazard and can comprise physical harm, injury, death, loss, damage to property or revenue as well as loss in reputation and credibility of the infrastructure. More specifically, as defined in the framework of the European Union, harm or damage from a possible or realized hazard and be measured in the following qualitative and quantitative parameters:

Range: relative to the radius of the geographic area likely to be affected by the loss or non-availability of the critical asset.

Severity: the consequences of the malfunction or damage/destruction based on the following criteria, which correspond to direct and indirect impacts (Section **Error! Reference source not found.**):

- The damages to the CI and its performance levels, including the cascading effects on other critical infrastructures and technologically related incidents.
- Safety levels and CI degradation due to ageing,
- Casaulties related to the infrastructure operation stage,
- The economic impact (level of economic loss or/and degradation of products and services).
- The environmental impact, identified as greenhouse gas emissions, priority air pollutants, emissions to water and toxic substances,
- The impact on the reputation and prestige of the CI operator.
- The social and psychological impact to the population of not being able to use the services of the specific CI .
- Casualties to the city / region / community that the CI perates
- Economic impacts to the wider economic sectors

The level of the Consequences, for the purpose of the EU-CIRCLE risk analysis framework, will be described through a two levels approach where initially a quantifiable number is generated (numerical, categorical, etc) and then this is classified into a finite number of categories attributing weights to each category through a user-defined classification mechanism. According to the NRA process, the internationally accepted five category may be used as an example:

NEGLIBLE	SMALL	MEDIUM	HIGH	SEVERE

The different consequence/impacts components that are proposed by EU-CIRCLE are described extensively in section **Error! Reference source not found.**. Section 3.7.3 also compares this impacts with the different approaches followed by the EU MS in order to compile their NRA plans.

The proposed approach allows to examine very specific policy questions such as: What is economic risk to the transportation infrastructures under future extreme rainfall conditions. In order to respond to this policy question using the EU-CIRCLE methodological approach, the impact categories could conatin the economic component (accounting for direct & indirect impacts) or in combination to other categories attributing higher weights to the former.

The proposed approach also allows for the direct comparison of risk levels for same underlying climate conditions and exposure level, between different infrastructures located at the same region or even at infrastructures located in different regions and operated by different operators. Although the proposed methodological framework allows for this comparison, it is very important that EU-CIRCLE users perform this assessment with extreme caution.

Finally, Risk is estimated through a mapping between the identified likelihood/probability of occurrence and the collective impact catgories. Following the NRA convention as an example, risk is determined in a five category system, in accordance with the previous classification of likelihood and consequences.

VERY LOW	LOW	MEDIUM	HIGH	CRITICAL

With the Likelihood and Consequences/Impacts being classified into 5 distinct categories each, an original risk matrix consisting of 25 cells and five irregularly shaped zones is build to determine the overall risk (Table 4). The same approach can be used to estimate risks relating to a specific impact, such as "what is economic risk exposure of an infrastructure to flooding". Besides the risk quantification as a categorical variable, it is possible to provide numerical estimates of risks, as the individual compenets are initially processed using numerical estimates for both the likelihood and consequences.

Table 4: Risk matrix.

	CONSEQUENCES/IMPACTS				
LIKELIHOOD	**NEGLIGIBLE**	**SMALL**	**MEDIUM**	**HIGH**	**SEVERE**
VERY HIGH	LOW	MEDIUM	HIGH	CRITICAL	CRITICAL
HIGH	VERY LOW	MEDIUM	MEDIUM	HIGH	CRITICAL
MEDIUM	VERY LOW	LOW	MEDIUM	MEDIUM	HIGH
LOW	VERY LOW	VERY LOW	LOW	LOW	MEDIUM
VERY LOW	VERY LOW	VERY LOW	VERY LOW	VERY LOW	LOW

Again, other risk matrix sizes and zone shapes could be deployed by the CIRP user as well.

Risk is estimated with a degree of uncertainty (the analytical way of assessing it is presented in Section 3.8), following the IPCC and UK-CCRA ***concept of confidence.*** As an example one of the findings of the IPCC-AR5:

Climate change is projected to reduce severe accidents in road transport ***(medium confidence)***

3.4.2 Estimation of Likelihood / Probability of occurrence

Estimation of likelihood/probability of occurrence is a core element of the EU-CIRCLE Risk Management Framework (see Step-2, section 3.2.2), and involves the collection and processing of all related climate information from available sources (historical, simulation, satellite), in order to generate:

1. An estimation of the probability of occurrence of the hazard under the specific scenario.

2. All necessary data that are needed to estimate the impact of the hazard to the infrastructures (Section **Error! Reference source not found.**).

EU-CIRCLE risk modeling could utilise any type of climate information on a temporal and spatial scaling (depending on the requirements of the scenario under examination) using multiple sources of climate data such as:

- historical observations
- climate models (e.g. CORDEX, CMIP5)
- numerical weather prediction models
- satellite data (e.g. Copernicus)
- fused data

The climate data processing within EU-CIRCLE are analysed in WP2, and the workflow presented in (Figure 23) and in a tabulated format below (Table 5):

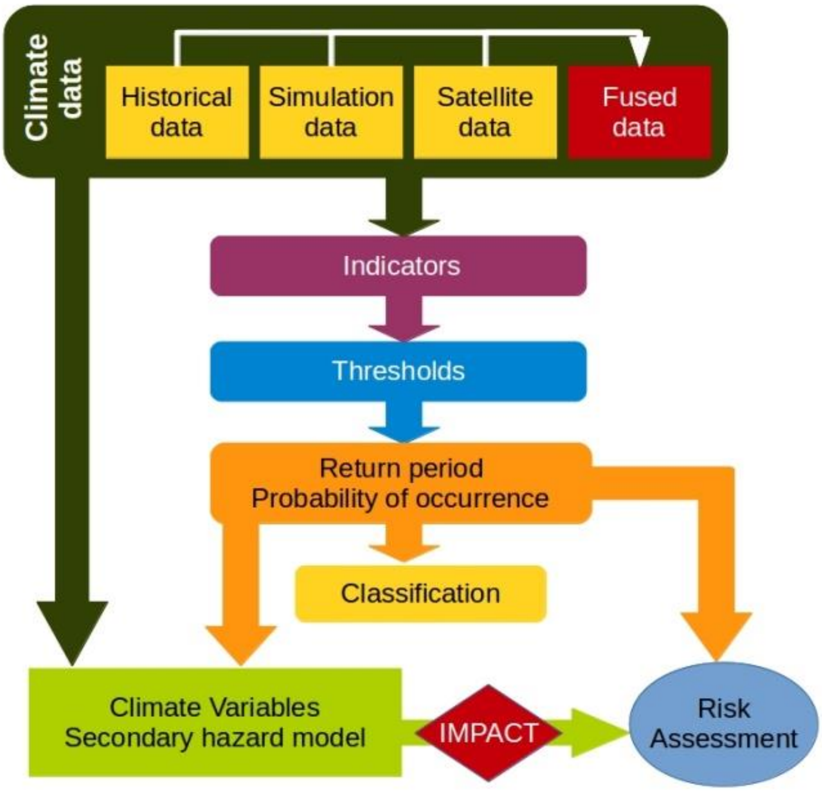


Figure 23. Workflow of the initial procedure of risk assessment

Two worked examples are presented for illustration.

Example 1 relates to the risk of forest fires (further details in Table 5), in which we make use of the Fire Weather Index (FWI) (EFFIS, JRC), which is an index composed of six sub-indices referring respectively to the daily variation of water content for fuels with different response time changes in weather conditions, the initial rate of spread for propagation, the quantity of fuel and the expected intensity of the flame front. Disastrous incidents of wildfires, which are often in southern European countries, have taken place in Greece in 2007 resulting in 65 deaths, in Spain in 2005 resulting in 11 deaths and in Portugal resulting in 15 deaths, according to the International Disaster Database (http://www.emdat.be/).

Example 2 relates to the risk of heat wave, a prolonged period of excessively hot weather, which may be accompanied by high humidity. In Europe, one of the most severe events of extreme temperature/heat wave occurred in 2003 and cost the lives of more than 50,000 people throughout Europe. (EM-DAT).

Table 5. Climate data processing in the framework of EU-CIRCLE Risk model with worked examples

	Example: Forest Fires	**Example: Heat Waves**
Collection of climate data from existing databases Collection from available databases climate historical or predicted or processed data, depending on the problem to solve, that are used to calculate the appropriate indices for a certain period and place of interest. **Databases:** ECA&D, CORDEX, CMIP5, etc. **Models and Tools:** GCM, RCM, ESD, etc.	Temperature Rainfall Wind Relative humidity	Temperature Humidity
Indicators Indicators measure the actual status of the environment before, during or after an event and serve as a reference status or as a signal for environmental/climate change over time (qualitative or quantitative). Indicators are referring directly to climate parameters related to the risks or to climate indices that give measure of a risk appearign or not.	Fire Weather Index (FWI)	Temperature Heat Index - Humidex
Thresholds Represent quantitative critical values derived from the examined scenario. So it is important to identify where there is a likelihood of unsustainable trends of certain indicators related to environmental issues that show threshold phenomena. These thresholds may be related not only with extreme phenomena (floods, fires, extreme weather events), but to mean climate values, standard deviation of a variable etc., depending on the assessed scenario.	FWI > 150 at least 10 days	HI > 54 °C
Return period / Probability of occurrence Based on the threshold and the indicators that have been specified, and also the processed data, we calculate the probability of occurrence of the risk scenario or its return period. A Return level with a return period of T = 1/p years is a high threshold x(p) whose probability of exceedance is p (likelihood of rare events).	1:100 yr or p=0.01%	1:200 yr
Classification The levels of Likelihood are defined by the internationally accepted descriptive terms, classified into a set of five categories.	Very Low – Very rare Low Medium High Very high- Very Likely	Very Low – Very rare Low Medium High Very high- Very Likely
Climate variables/ Secondary hazard model Collection of climate variables per case study for further processing or as input data in the secondary hazard model	Fire Spreading Model	Temperature Humidity

(fire, flood model etc.)		
Impact Input of above previous processed data for the impact model	Fire-line intensity Fire Temperature Radiative force	Temperature Humidity

During the initial procedure of risk assessment, the uncertainties are also estimated which are related to the climate information, and are subsequently processed in Section 3.8.

The timescales involved may also be linked to the expected annualized probability of an event (return period), frequently used as an indicator value for the expected probability of occurrence. As a numerical example, the value of 0.5% annual probability is translated as an event occurring 1 in 200 years, which is a higher value of appearance than a 1 in 1000 (0.1%) annual probability event. This concept is also related to the likelihood component of risk resulting in the "cumulative probabilities" of an infrastructure being exposed to a predefined event, and therefore directly linked to the design standard. As a numerical example, for any infrastructure asset with a 100 year design life, there is a 63% cumulative probability of seeing the 100 year snowfall, which is a high enough probability that this event should be considered in the design phase.

Changes in extreme events may be difficult to detect locally, even when powerful methods based on extreme value analysis theory are used. The Generalized Extreme Value (GEV) distribution was introduced into meteorology by (Jenkinson, 1955) and is used extensively to model extremes of natural phenomena such as precipitation (Gellens, 2002), temperature (Nogaj, et al., 2007) and wind speed (Coles and Casson (1999), Walshaw (2000)). It is possible to account for non-stationary conditions (climate change) using extreme value analysisas described in the following paragraphs.

In cases where examined data exhibit homogeneous climate characteristics i.e. stationarity, return periods may be estimated through extreme value theory. Under this examination all parameters of the GEV distribution are homogeneous across the region, or that the scale and shape parameters are homogeneous. Such an assumption would enable records from multiple stations or historical data to be combined to form a larger data sample. The spatial pooling approach has its origin in hydrology where it is known as regional frequency analysis. This approach is most effective for variables, such as precipitation, which have short "decorrelation" distances (that is, where the correlation between observations at different locations falls off quickly as the distance between stations increases).

Spatial pooling can also be done in other ways, such as by averaging parameter estimates from nearby locations. Parameter estimates based on the pooled information across the region are generally less uncertain than those from the data of individual records because the same amount of information is used to estimate a smaller number of parameters. This also leads to a reduction of uncertainty of the estimated extreme quantiles of the distribution.

According to WMO (2009), the best way to determine the return period from a specific climate parameter should comply with the following procedure:

Preparation of data series (in particular observations) for the analysis of extremes

The preparation of data series must include long and quality-controlled daily observational series to evaluate the intensity and frequency of rare events that lie far in the tails of the probability distribution of weather variables (temperature or precipitation) such as the 20-year return value (an event whose intensity would be exceeded once every 20 years, on average, in a stationary climate). T-year return value is the $(1\text{-}1/T)^{th}$ quantile of the GEV distribution (Rootzen & Katz, 2013). In some engineering applications, such analysis requires estimation of events that are unprecedented in the available record, say events that occur once in a hundred or thousand years (extreme quantiles of the statistical distribution), while the observation series may be only about 50 years long). Also, continuous data series with at least a daily time resolution are needed to take into account the sub-monthly nature of many extremes.

The concepts of return level and return period are commonly used to carry information about the likelihood of rare events such as floods. A return level with a return period of T = 1/p years is a high threshold x(p) (e.g., annual peak flow of a river) whose probability of exceedance is p. For example, if p = 0.01, then the return period is T = 100 years.

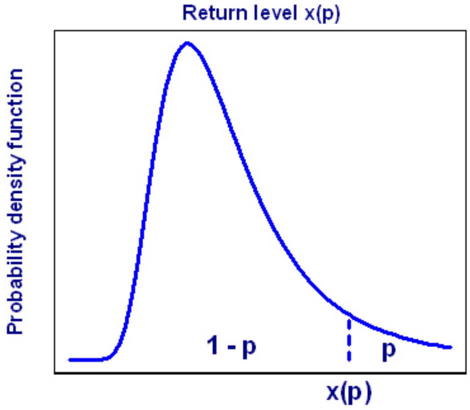


Figure 24: Probability density function.

Two common interpretations of a return level with a return period of T years are:

(i) Waiting time: Average waiting time until next occurrence of event is T years

(ii) Number of events: Average number of events occurring within a T-year time period is one

Utilization of descriptive indices and extreme-value theory to evaluate extremes

Extreme value theory complements the descriptive indices in order to evaluate the intensity and frequency of rare events that lie far in the tails of the probability distribution of weather variables. Two general methods can be used. One method, referred to as the “peaks-over-threshold” or POT method, under suitable conditions, and using a high enough threshold, extremes identified in this way will have a generalized Pareto, or GP, distribution, and the second more generally used method based on an explicit extreme value theory is the so-called “block maximum” method. In this method, one considers the sample of extreme values obtained by selecting the maximum (or in some cases, the minimum) value observed in each block (usually year or season). Statistical theory indicates that the GEV distribution is appropriate for the block maxima when blocks are sufficiently large.

In terms of the tail of a distribution, the corresponding theorem states that the observations exceeding a high threshold, under very general conditions, are approximately distributed as the generalized Pareto (GP) distribution. This distribution has three types: exponential, Pareto, Beta (Figure 25).

The **cumulative distribution function (CDF) of the GEV** distribution is:

Formula 2

$$F(x;\mu,\sigma,\xi)=\begin{cases}\exp\left\{-\left[1+\dfrac{\xi(x-\mu)}{\sigma}\right]^{-\frac{1}{\xi}}\right\}, & \xi\neq 0\\ \exp\left\{-\exp\left[-\dfrac{x-\mu}{\sigma}\right]\right\}, & \xi=0\end{cases}$$

Where three parameters, ξ, μ and σ represent a **shape, location, and scale** of the distribution function, respectively. Note that σ and 1 + ξ(x-μ)/σ must be greater than zero. The shape and location parameter can take on any real value. The shape parameter ξ affects the support of the distribution. More specifically, when ξ = 0, the GEV distribution is the Gumbel distribution ((Gumbel, 1958), used extensively in hydrology, meteorology and engineering). with support R; when ξ > 0, it corresponds to the Fréchet distribution and when ξ < 0, it corresponds to the (reversed) Weibull distribution families (Figure 25).

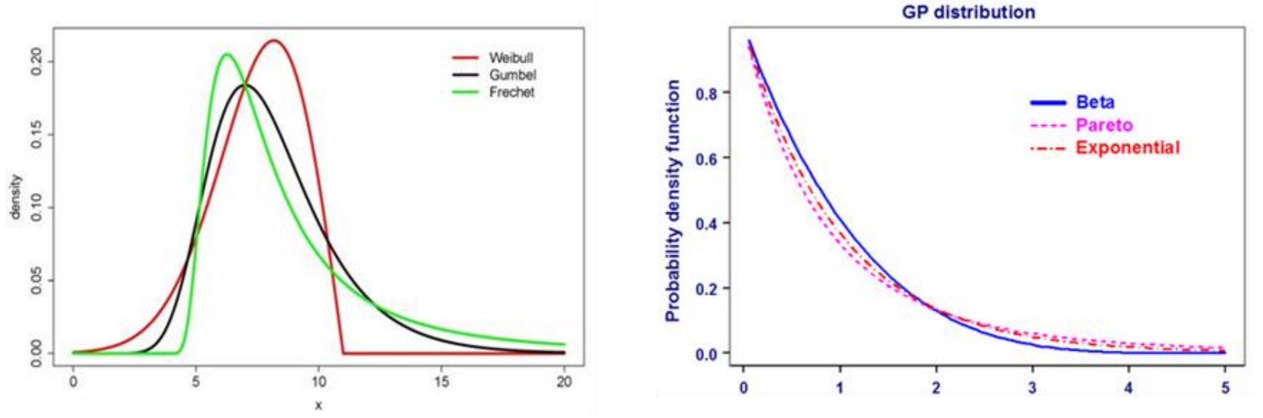


Figure 25: GEV distributions and POT distributions.

When comparing observations and model output, it is important to know what scales are represented by the observational data sets and how they might differ from model output to avoid misinterpretation. Global climate models are not yet able to provide scenarios with sufficient detail at the regional and local scale for many applications.

Their coarse spatial resolution affects in particular the projections for changes in extremes because extremes are often smaller in extent than the effective spatial resolution of the models. For this reason, downscaling (or regionalization) of global climate model projections using regional climate models (nested in the global models) or statistical techniques provides additional useful information (Giorgi, 2008).

The application of this classic theory assumes that time series are stationary. Adjusted techniques are recommended when there are indications for non-stationarity.

Trend calculation and other statistical approaches for assessing changes in extremes, mean values and other statistical metrics

Trends are the simplest component of climate change and provide information on the first-order changes over the time domain considered. This implies that the physical mechanisms behind the detected trends remain unknown. The calculated trends represent changes that can be due to natural internal processes within the climate system and/or external forcing, which can either be natural, such a solar irradiance and volcanic aerosols, or anthropogenic, such as greenhouse gases.

It is also possible to indicate a definitive trend in the mean value of a climate variable for a specific period that should be taken into consideration because it exceeds a critical value and may cause important environmental consequences.

It is important to test the goodness-of-fit of the fitted distribution (e.g. Kharin & Zwiers (2000)) and to assess the uncertainty of the estimates of the distribution's parameters by calculating standard errors and confidence intervals for these estimates. The latter can be done in a relatively straightforward way when the distribution has been fitted by maximum likelihood because in this case the underlying statistical theory provides expressions that generally give good approximations for these quantities (for example 90%, 95% and 99%).

Although very long period return values can be calculated (for example, once-in-thousand-year levels) from the fitted distribution, the confidence that can be placed in the results may be minimal if the length of the return period is substantially greater than the period covered by the sample of extremes. Estimating return levels for very long return periods is prone to large sampling errors and potentially large biases due to inexact knowledge of the shape of the tails of a distribution. Generally, confidence in a return level decreases rapidly when the period is more than about two times the length of the original data set.

The least square method is one of the approaches for trend estimation; nevertheless this method may be sensitive to individual values, such as a single outlying observation that lies either near the beginning or the end of the available data record. Such observations have "high leverage", meaning that the fitted trend can be strongly affected by their inclusion or exclusion from the data record. In such instances, a non-parametric method may therefore be more statistically robust because the indices generally have non-Gaussian distributions. For instance, it is possible to use Kendall's Tau (Kendall, 1938), which measures the relative ordering of all possible pairs of data points, where the year is used as the independent variable and the extreme index as the dependent variable.

The probability of detecting a trend in any time series depends on the trend magnitude, the record length, and the statistical properties of the variable of interest, in particular the variance. A trend is said to be detected when a test of the null hypothesis that no trend is present is rejected at a high significance level, such as five per cent or one per cent. (Frei & Schär, 2001) show that for precipitation, there is only a one-in-five chance of detecting a 50 per cent increase in the frequency of events with an average return period of 100 days in a 100-year record.

3.4.3 Critical infrastructure network topology and description

A parallel step to the estimation of climate change risk assessment is the definition of the CI in terms of its constituent elements – its assets –,their spatial placement within any given region of interest, and their interconnections.

An infrastructure system is generally a set of interconnected structural elements such as power generation stations, power distribution stations, power lines, pumping stations, water pipelines, pipeline junctions, bridges, roadways, etc. **This system can be modeled as a network that consists of nodes and links**. By considering the systems in this way, network flow algorithms can be employed to ascertain network behavior that is of interest to the CI stakeholder community. The importance of a single asset within an infrastructure system is based on how it contributes to the overall function of that system. By assessing disruption or loss of one or more system components, and measuring the consequences/impacts that result from this disruption in terms of the subsequent loss of system functionality, it is possible to evaluate the change in system performance after the disruption. Having an operational – network simulation model that provides a clear measure of system function (flows) allows us to systematically evaluate the importance of components by considering the consequence associated with their loss, but this requires that we assess how the infrastructure system will respond to each disruption. This approach and assessment should be used with caution because the contribution of a single component to system function may depend also on its interactions with other components. For example, the loss of a single component might not result in any change to system function (because there is redundancy elsewhere), but the simultaneous loss of this component in combination with other (supposedly) redundant components might be catastrophic to the system (Alderson, et al., 2015)

CI registry

Deliverable D3.1 will identify and collate the assets of each critical infrastructure (CI) within the scope of EU-CIRCLE, for inclusion in a registry. The information in the registry will then feed into the Climate Infrastructure Resilience Platform (CIRP). For the purposes of the EU-CIRCLE registry the following definitions are used:

Critical Infrastructure Asset is a physical long-lived resource, item, or entity that is operated as a system or network e.g. Airports, ports, coal powered plant, wastewater treatment plant, oil extraction platform etc. Critical Infrastructures within the scope of EU-CIRCLE include the following:

- Energy infrastructure
- Information and Communication Technology (ICT) infrastructure
- Water infrastructure
- Transport infrastructure
- Chemical industry infrastructure
- Health Sector
- Public Sector infrastructure

The registry will thus collect the assets of the CI sectors identified above in two steps:

1. The critical services of each CI sector will be identified, followed by subsequent identification of the assets that are required to provide these critical services, and described exhaustively in D 3.1. Once each asset has been identified, the interdependencies and the characteristics/attributes that describe the asset will also be identified e.g. size of asset, age of asset, materials of asset, capacity of asset, etc.
2. Identification of damage functions for each asset. This will be done jointly with D3.3.

An *example* of the information that will be identified and collected can be seen below for the Energy sector:

Table 6 Assets of the energy sector (Exemplary list)

Sector	Subsector	Critical Services	Assets
Energy	Oil	- Extraction - Refinement - Transport -Storage	- Oil platform - Oil well - Oil refinery - Oil transmission pipelines - Oil storage terminals - Tanker vessels - Rail cars

			- Trucks - Petrol stations
	Gas	- Extraction -Refinement -Transport -Storage	- Gas well - Compressor station - Gas transmission pipelines - Gas distribution pipelines
	Electricity	-Generation -Transmission - Distribution	- Boiler - Turbine - Combustion turbine (natural gas) - Steam Generator - Heat Recovery Steam Generator - Transmission towers - Transmission lines - Transmission substations - Grid - Substations - Distribution lines - Control room
	Coal	- Extraction - Transport - Storage	- Surface mines - Underground mines - Coal Bunker
	Renewables e.g. wind, solar, tidal, hydro, biomass	- Generation - Transmission - Distribution	- Hydroelectric dams - Offshore wind farms - Onshore wind farms - Solar PV farms - Concentrated solar power plants - Wind turbines - Hydroelectric turbines

An important aspect is the granularity of infrastructure registry. For example, a transport network can be either represented as an abstract and hence coarse node-edge model characterized only by certain traffic throughputs or – on the opposite side - as a fine grained model where every component is considered in detail, e.g. each road segment with traffic lights, pavements etc.

Asset Description

Within EU-CIRCLE each asset is defined as a granual component in the CI network (or network of networks) that has a set of states $S_{i[\text{Node}],j[\text{Network}]}^{k[\text{property}]}(t)$. The state of a critical infrastructure asset (at normal operating conditions) depends upon the underlying conditions which are required in order to provide the services and contribute to the respective CI network functionality. As such, it depends on various properties that are necessary for operation, and include the (although these may differ on a case by case basis):

- State of the physical structures, and equipment;
- Human capital (personnel) that operates the asset;
- Supporting infrastructures (power, gas, water, ICT / data transfer, sewage, transportation);
- Safety and secutiy equipment, procedures and training for hazards management (in order to anticipate, respond and recover to hazards)

The state Si(t) of the asset (and network) state may change during the EU-CIRCLE analysis. This change could be triggered by different causes including:

- Damages due to hazards (as described in Section 3.5)
- Maximizing operational capacity, which for the project is determined from the solution of the network simulation algorithms (Section 3.7)
- Operational conditions of the asset (e.g. safety state, maintenance)

All of the above conclusively result in altering service levels, or in a loss in the capacity level that each asset is able to contribute towards the operation of the CI network. The CI asset state is finally determined through its available capacity for the supply side of the system (production and transportation process) as a function of the maximum production capacity and reductions in that capacity due to damage of physical system or shortages of essential inputs (dependencies on other infrastructure services).

The final modelling design depends on the available infrastructure data and must be an appropriate compromise between expressiveness of modelling results and efforts. In the envisaged case studies, there seems no need for fine granular modelling and therefore a rather coarse approach with lower date demand is recommended for EU-CIRCLE. The modelling platform EU-CIRP and SimICI will be flexible to facilitate different granularity levels. For each asset, the interdependencies with other critical infrastructures will be identified as well as the characteristics that can describe each asset. These will be analytically introduced in D3.1.

Assessing ageing of CI assets

The robustness of infrastructure systems can be judged by their capacity to accommodate change over time. Ageing is one of many factors that affect the performance of infrastructure and its robustness against threats posed by common environmental conditions and extreme natural hazards. Infrastructure ageing often impacts other CI factors such as design, maintenance, and operation in increasing the asset’s vulnerability and exposure to damages.

The EU-CIRCLE framework proposeds to incorporate the aging process of CI, as part of the description of the assets, *using two temporal properties* : 1) the build year of the infrastrtcure (or the year of the last major upgrades) where it is assumed that the asset is at the present state and 2) the year where the scenario is examined (either in present times or the future) *and an ageing factor*, function or curve that quantifies in a mathematical perspective the rate of change.

Although any simulation property may be used, following related literature (Shamir & Howard (1979), Kleiner & Rajani (1999)) a time-exponential model is proposed

$$FS_{i,j} = PS_{i,j} * e^{AF*(FY-YB_{i,j})}$$

$FS_{i,j}$ denotes the Future State of node i of the network j, $PS_{i,j}$ stands for Previous State of node i of the network j, YB denotes the Year Built of the asset, AF denotes the Aging Factor of the asset, and FY denotes the Future Year date that we want to adapt the asset’s behavior.

CI interconnections and (inter-) dependencies

Critical infrastructures are usually interconnected and mutually dependent in various and complex ways, creating a critical infrastructure network. A critical infrastructure network is a set of interconnected and interdependent critical infrastructures interacting directly and indirectly at various levels of complexity and operating activity. It can be useful to distinguish between dependencies and interdependencies. According to Rinaldi et al. (2001), a dependency is a uni-directional linkage or connection between two infrastructures, through which one infrastructure influences or is associated/correlated to another. An interdependency is a bidirectional relationship between two infrastructures through which each infrastructure mutually influences or is associated to the other. More generally, two infrastructures are interdependent when each is dependent on the other.

Interdependence-related disruptions can be classified as cascading, escalating or common cause. According to Rinaldi et al. (2001), a cascading failure occurs when a disruption in one infrastructure affects one or more components in a second infrastructure, which subsequently causes the partial or total unavailability of the second infrastructure. An escalating failure occurs when an existing disruption in one infrastructure exacerbates an independent disruption of a second infrastructure, generally in the form of increasing the severity or the time for recovery or restoration of the second failure. A common cause failure occurs when two or more infrastructure networks are disrupted at the same time: components within each network fail because of some common cause.

In EU-CIRCLE D1.2, the critical infrastructure network cascading effects are defined as degrading effects occurring within a critical infrastructure and between critical infrastructures in their operating environment, including situations in which one critical infrastructure causes degradation of another ones, which again causes additional degradation in other critical infrastructures and in their operating environment.

There are different types of interdependencies and different ways of characterizing them. A comprehensive overview of various categorization approaches can be found in (Oyang, 2014). The following table lists the different approaches.

Table 7: Interdependency types (Ouyang, 2014)

Authors	Interdependency Types	Definitions
Rinalidi et al.,	Physical	The state of one infrastructure system is dependent on the material output(s) of another infrastructure system
	Cyber	The state of one infrastructure system depends on information transmitted through the information infrastructure
	Geographic	A local environmental event can create state changes in two or more infrastructure systems
	Logical	The state of one infrastructure system depends on the state of others via a mechanism that is not a physical, cyber, or geographic
Zimmerman	Functional	The operation of one infrastructure system is necessary for the operation of another infrastructure system
	Spatial	It refers to proximity between infrastructures systems
Dudenhoeffer et al.	Physical	There are direct linkages between infrastructure systems from a supply/consumption/production relationship
	Geospatial	There is co-location of infrastructure components within the same footprint
	Policy	There is a binding of infrastructure components due to policy or high level decisions
	Informational	There is a binding or reliance on information flow between infrastructure systems
Wallace et al.	Input	The infrastructure systems require as input one or more services from another infrastructure system in order to provide some other service
	Mutual	At least one of the activities of each infrastructure system is dependent upon each of the other infrastructure systems
	Shared	Some physical components or activities of the infrastructure systems used in providing the services are shared with one or more other infrastructure systems
	Exclusive or (XOR)	Only one of two or more services can be provided by an infrastructure system, where XOR can occur within a single infrastructure system or among two or more systems
	Co-located	Components of two or more systems are situated within a prescribed geographical region
Zhang and Peeta	Functional	The functioning of one system requires inputs from another system, or can be substituted, to a certain extent, by the other system
	Physical	Infrastructure systems are coupled through shared physical attributes, so that a strong linkage exists when infrastructure systems share flow right of way, leading to joint capacity constraints
	Budgetary	Infrastructure systems involve some level of public financing, especially under a centrally-controlled economies or during disaster recovery
	Market and Economic	Infrastructure systems interact with each other in the same economic system or serve the same end users who determine the final demand for each commodity/service subject to budget constraints, or are in the shared regulatory environment where the government agencies may control and impact the individual systems through policy, legislation or financial means such as taxation or investment

The categorization proposed by Rinaldi, Peerenboom, and Kelly (Rinaldi et al. 2001, Rinaldi 2004), is broadly used and distinguish four primary classes of interdependencies and is the starting point for the work of EU-CIRCLE. Rinaldi et al proposed the following interdependencies:

- **Physical Interdependency:** two infrastructures are physically interdependent if the state of each depends upon the material output(s) of the other. Physical interdependencies arise from physical linkages or connections among elements of the infrastructures;
- **Cyber Interdependency**: an infrastructure has a cyber-interdependency if its state depends on information transmitted through the information infrastructure. The computerization and automation of modern infrastructures and widespread use of supervisory control and data acquisition (SCADA) systems have led to pervasive cyber interdependencies;
- **Geographic Interdependency**: infrastructures are geographically interdependent if a local environmental event can create state changes in all of them. This implies close spatial proximity of elements of different infrastructures, such as collocated elements of different infrastructures in a common right-of-way;
- **Logical Interdependency**: two infrastructures are logically interdependent if the state of each depends upon the state of the other via some mechanism that is not a physical, cyber, or geographic connection. For example, various policy, legal, or regulatory regimes can give rise to logical linkage among two or more infrastructures.

Example of Interconnections

As a worked example, power grids depend on gas networks to fuel generation units. Water networks provide cooling and help to control emissions from coal-based power generators. Water and gas networks are heavily dependent on power for operating pumping stations and control systems. If a particular system is damaged, this damage is propagated to other systems due to the interdependent nature of the systems (i.e., cascading failures). Therefore, an emerging need exists for modeling complex and interdependent critical infrastructure to better understand their susceptibility to potential hazards. Consider an example of a power grid and water system shown in Figure 26: Energy – Water Network interconnections., where the electrical needs of a node in the water distribution network can be supplied by one or more nodes in the power grid.

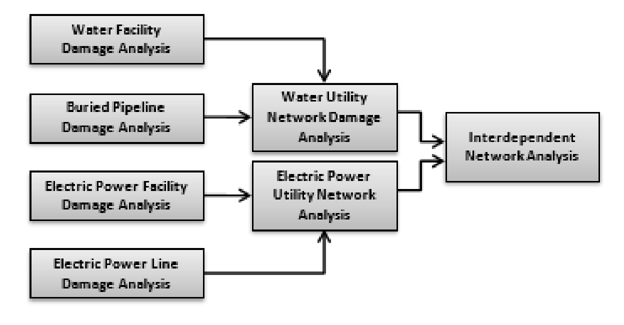


Figure 26: Energy – Water Network interconnections.

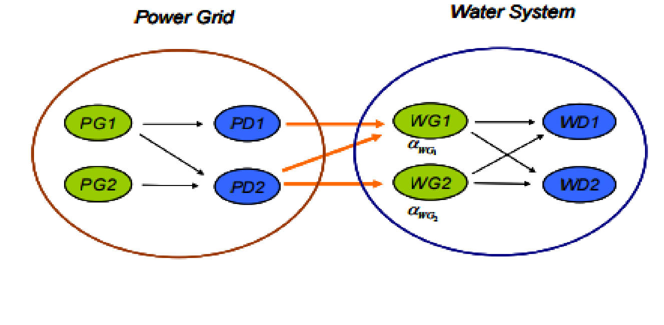


Figure 27: Example of a power grid and water system

To account for network interdependency, a relationship must be developed to describe how the failure of a node in one network is affected by failures in another network. This relationship can be determined as a function of the geospatial location of the network components and the associated connections. For example, in Figure 27, water generation node 1 (WG1) is dependent on power distribution nodes 1 (PD1) and 2 (PD2), and WG2 is dependent on PD2. WG1 and WG2 have backup power generation units for which their failure probabilities are a_{WG1} and a_{WG2}, respectively. The dependent nodes in the water system (e.g. WG1 and WG2 in Figure 27) must have power for proper functionality. Consider the failure of these nodes in the water system due to a power outage. Each dependent node has a backup power generation unit; therefore, both of the nodes on the power grid on which it is dependent and its backup power generator must fail so that the dependent node in the water system is rendered non-functional. This means that we need to consider the reliability of the backup supply unit in determining the strength of interdependency and in evaluating interdependency effects. Section 3.5 describes the proposed model to characterize the dependency of a node in the water system on the nodes in the power grid.

3.4.4 Structural and operational analysis

This step within the EU-CIRCLE risk modelling process aims to identify the impacts of the climate pressures using an mathematical quantification approach trying to accommodate different methodologies and frameworks that have been used in the literature and in different scientific domains. As such the main difficulty of the analysis is to harmonise the process and in parallel introduce new knowledge that will be generated from the project (and reported in D3.3).

The basic concept of this step is that the state of an infrastructure may be alterated due to the climate parameters. This is reflected in:

1) ***The supply (and transformation) capacity of the infrastructure***. The most characteristic example is the electricity generation from wind energy sources that is directly related to the wind speed and secondary to direction and air density

2) ***The demand of services from an infrastructure***. Characteristic examples include the water demand change due to temperature, precipitation and wind (House-Peters & Chang, 2011). For the purposes of EU-CIRCLE changes in service demand of an infrastructure due to changes in demographics, land use/land cover will be addressed with the best possible scientific knowledge and using data from 1) existing future scenarios on appropriate resolution, 2) land use planning from respective authorities, 3) expert's knowledge.

3) ***Damages to the assets***. These would reflect changes in the states of the asset and should result in a capacity loss (either in absolute terms or in relative ones).

    a. Alternatively, if there exist data for damages to the structural part of the asset (or infrastructure) or casualties to operators, then these should be transformed into capacity loss information to feed the remaining analysis.

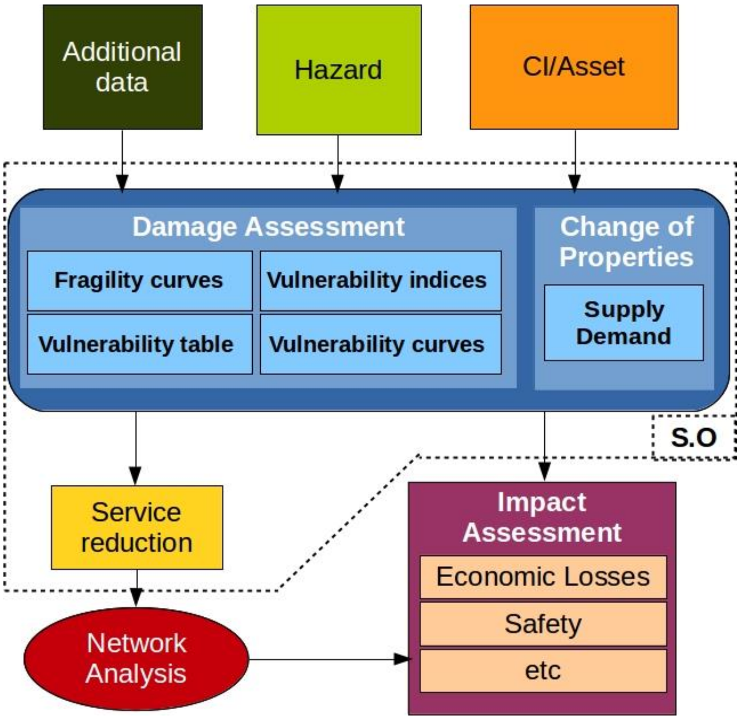


Figure 28. SOA process description

Figure 28, shows the use of the SOA and the different alternative approaches that my be used. The combination of the hazard characteristics, asset characteristics and properties and any other necessary information such as geographical, topgraphical, soil properties can be used in the damage assessment. The damage assessment according to EU-CIRCLE is a mathematical modeling that a specific hazard indices in the supply and demand, and the integrity state of the asset/network hence that are conveyed to

- Changes in the network properties (e.g. demand, supply, capacity of assets) that are used as inputs to the Network Analysis

- Inputs to the impact assessment models (e.g. structural damage leading to economic considrations) which are used in parallel with the solution of the Network Analysis.

A summary of existing models in the literature related to damages to the infrastructure operation is presented over the following paragraphs. The main use of this information will be to feed to the network analysis models (Section 3.5) with an modified values of the assets properties (mainly capacities) and network supply / demand parameters. Additionally, it is possible that climate parameters also have an impact on the interconnection strength between different assets. This is described in Section **Error! Reference source not found.**.

Damages. Under climate hazard conditions, components of an infrastructure system (e.g., pumping stations, bridges, power plants, etc.) experience stochastic damage and malfunction in their capacity with possible disruptions in supply and demand. These empirical or stochastic characteristics are generally assessed by fragility curves and damage-functionality relationships. In turn, uncertainties related to fragility curves or damage-functions result in uncertainties in the network states. For probabilistic disaster risk assessment, the vulnerability of exposed elements is assessed using functions that relate the intensity of the phenomenon that the hazard represents to the mean damage ratio or relative direct physical impact. Such functions are called vulnerability functions and they must be estimated for each one of the construction classes, so that a particular vulnerability function can be assigned to each one of the components in the exposure database. Each vulnerability function is characterized by a value known as the mean damage ratio (MDR) and its corresponding variance for each level of hazard intensity. That enables estimating the loss probability function at each level of intensity for the hazards under study (CIMNE, 2013).

Vulnerability indices based on indicators of vulnerability; mostly no direct relation with the different hazard intensities. These are mostly used for expressing social, economic and environmental vulnerability.

Vulnerability curves are constructed on the basis on the relation between hazard intensities and damage data. They provide a relation in the form of a curve, with an increase in damage for a higher level of hazard intensity. Different types of elements at risk will show different levels of damage given the same intensity of hazard. This is illustrated in the following figure, where the red line indicates an element at risk with a lower vulnerability than the green line. This method is mostly applied for physical vulnerability. Vulnerability curves are also named damage functions, or stage-damage curves. They can be subdivided into two types:

- **Relative curves**: they show the percentage of property value as the damaged share of the total value to hazard intensity.
- **Absolute curves**: show the absolute amount of damage depending on the hazard intensity; i.e. the value of the asset is already integrated in the damage function.

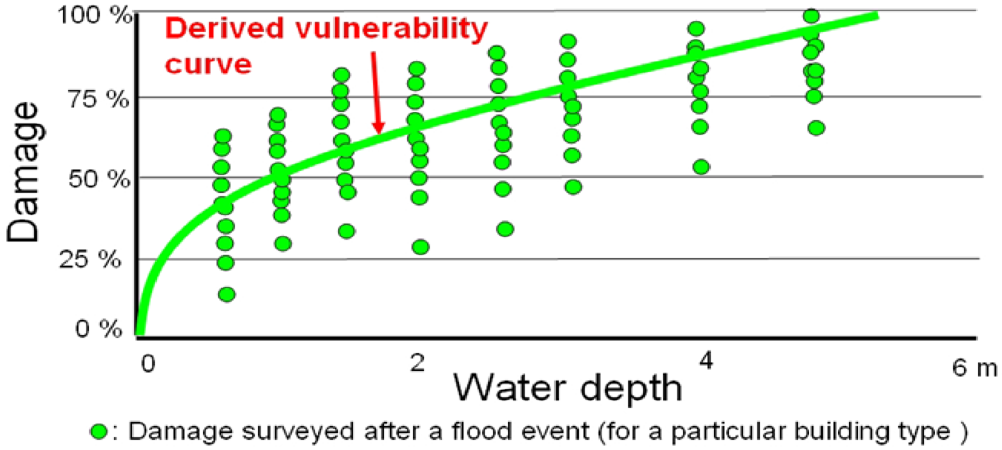


Figure 29: Illustration of the use of damage surveys for the generation of vulnerability curves.

Fragility curves provide the probability for a particular group of element at risk to be in or exceeding a certain damage state under a given hazard intensity. In Figure 30, there are four damage states defined (complete destruction, extensive damage, moderate damage, and slight damage). Given a particular level of hazard intensity, these four stages have different probabilities. For instance the left dotted line has 0 probability to be moderately damaged or worse. The middle dotted line indicated that the chance of being slightly damaged or more is very high, whereas the chance of complete damage is still 0. Fragility curves are used often in earthquake loss estimation, mostly for physical loss estimation

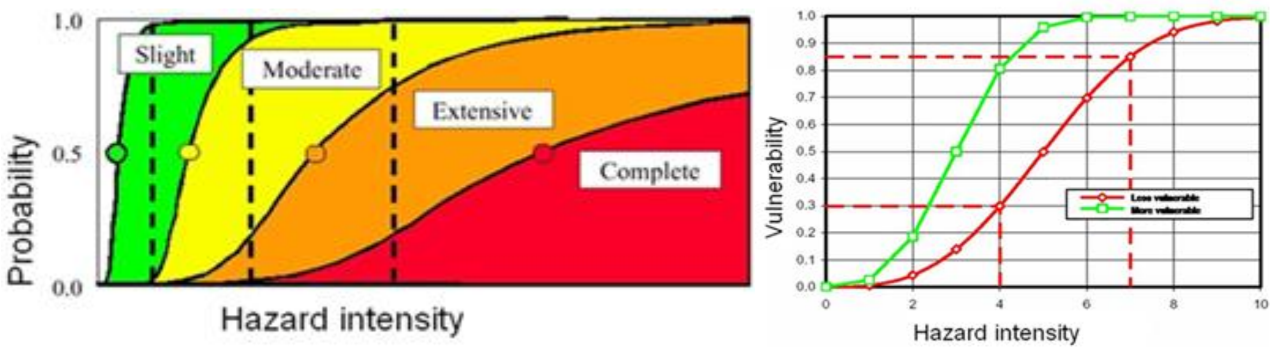


Figure 30: Fragility curves (above) andvulnerability curve (below)

Vulnerability table: the relation between hazard intensity and degree of damage can also be given in a table. In that case the smooth vulnerability curve is actually divided into a number of hazard intensity classes, and for each class the corresponding degree of damage is given..

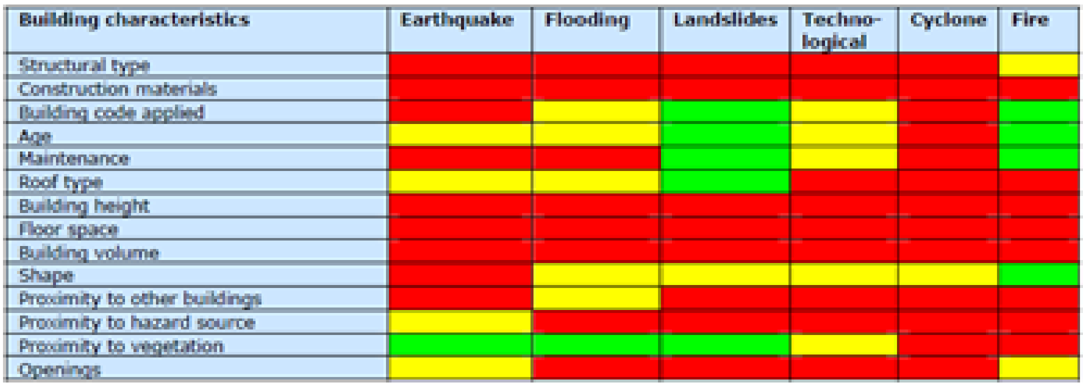


Figure 31: Summary of importance of building characteristics for damage estimation for different hazard types.

Flood example: United Kingdom Flood data base and damage functions of the Flood Hazard Research Centre (FHRC) from Middlesex University. This method deals with the derivation of damage curves from synthetic damage data. The main variables used are: depth of flood water within the buildings and the depth and extent of floodwater on the floodplain. Velocity is assumed to cause in rare cases structural failure. The data base has 100 residential and more than ten non-residential property types. Costs relate to restoration to pre-flood conditions, but do not always allow for full replacement. Absolute damage functions are used.

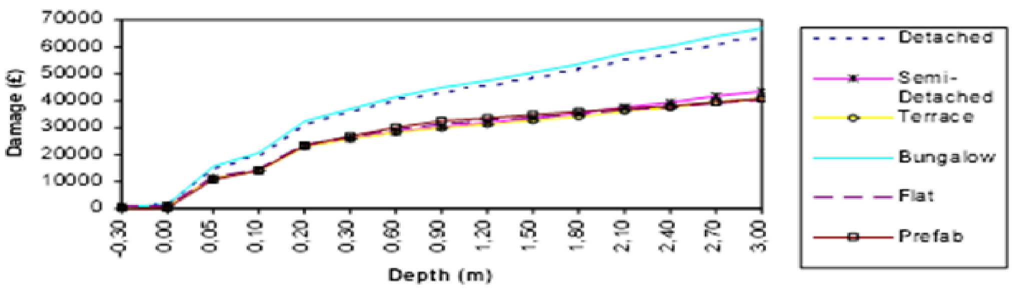


Figure 32: Synthetic depth-damage curves for different residential house types

(Source: Penning-Rowsell (2003))

3.5 Interconnected networks simulations

3.5.1 General network description

In the general EU-CIRCLE framework, the examined network consists of Generation (Supply) nodes G that produce the flow PR of services (either energy, water, transport of goods, data in the ICT domain, chemical prodcuts) in the links, Distribution(Demand) nodes D that consume the flow CS and Intermediate nodes $I$where the incoming flow is transmitted. These nodes are assets of the infrastructures with discrete properties, according to the definition of Section 3.4.3, and whose properties (such as the capacity) may (or maynot) be impacted by a specific climate hazard.

There are specific cases where a node has both properties of Generation and Distribution node without being at network endpoints, simultaneously, such a chemical factory that receives a flow of chemicals and produces a flow of a transformed product. The links are characterized by a value $f$equal to the flow multiplied by a “cost” number. The term “cost” expresses a property of the link that affects the flow, for example in electric grids, the loss of voltage due to distance can be defined as “cost”. The “cost” parameter, in our approach, is used in order to mathematically express our problem in terms of minimum cost and maximum flow optimization, as described analytically in section 3.5.5.

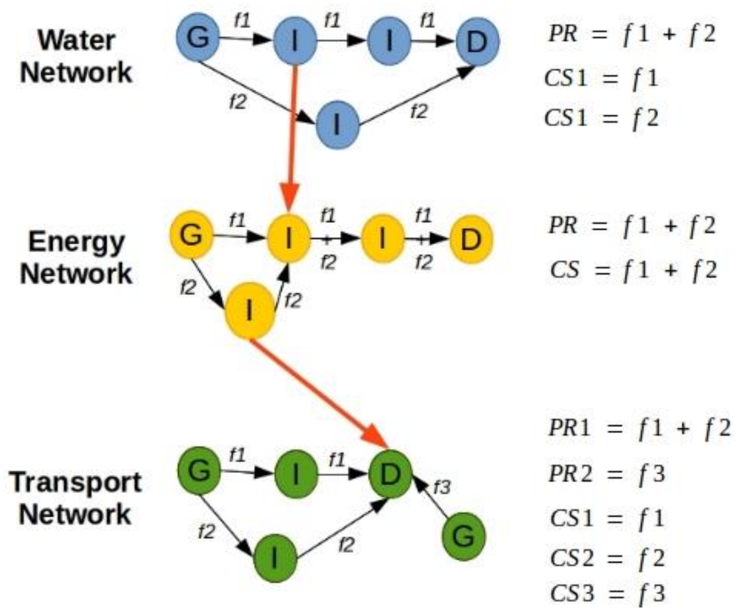


Figure 33: Three type network representation

3.5.2 Asset / Network Dynamics during extreme conditons

EU-CIRCLE also accounts for the dynamics of an infrastructure (or in one of its assets), when under stress from a climate hazard. Again this is related to the state of the asset, which can be directly translated to the performance level of the infrastructure. This section is mainly relating to describe the main temporal stages of a hazard.

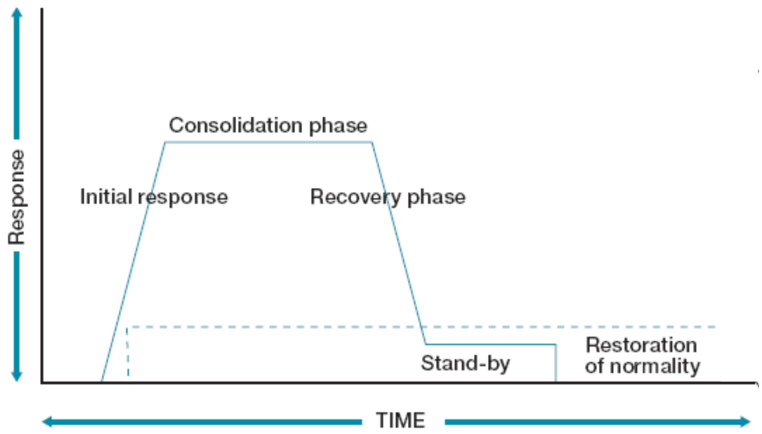


Figure 34: Time stages of hazard

The CI / asset will fall in different states during each of these stages, which according to the EU-CIRCLE procedure are translated into capacity levels or system performance levels.

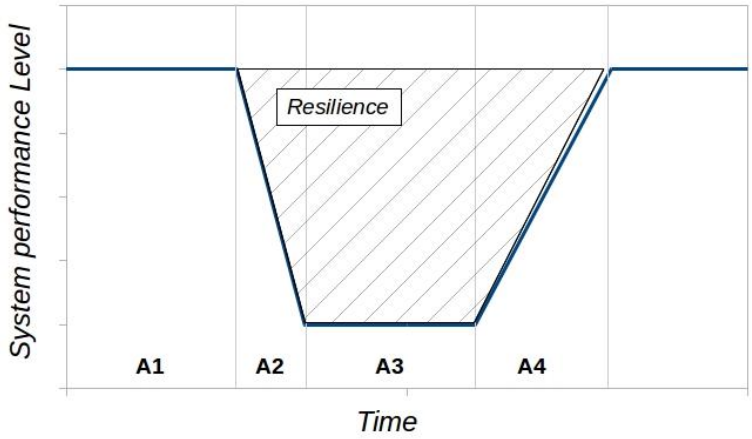


Figure 35: Asset response over time.

This process can be approximated in discrete stages, prevention stage, damage stage, response and assessment stage, recovery stage and restoration to normality. These three stages can be an inherent reflection of the resilience capacities (see D4.1 EU CIRCLE CI Resilience Framework to climate hazards – first version) of the system. Overall the system's present resilience is defined/quantified as the area of the inverse trapezoid in Figure 35. In detail:

- A1 (normality) depicts the normal state of the CI during which the system shows no degradations. The incident may happened or not but the CI remains unaffected.
- A2 (absorb) depicts immediate post-incident time interval during which the system shows performance degradations. This is the phase of the plastic degradation of service-supply, in the sense that the system would not be able to recover its full functionality without human intervention. If a time dependent simulation is chosen (Section XX), then caution should be made that the CI maximum capacity reduction limts (e.g. due to damages) are reached for the hazard under examination, before proceeding into the next interval.
- A3 (response) depicts the interval of time during which the degradation of the system performance is stabilized. No additional degradation is observed but the recuperation of the system functionality is not observed either. During this stage, copingwith the catastrophic events occurs and alternative options to maintain or/and replace the services materialize.
- A4 (recovery) depicts the interval of time during which the recovering actions are progressively undertaken. This is related to the ability of a CI to continue services and reconnects with its operational environment.

This concept has been also used in Ganin et al. (2016), Bruneau and Reinhorn (2007) and Cimellaro et al. (2009) that introduced the time element in the CI modeling process. The element of recovery time was introduced by (Porter et al. (2001); Bruneau and Reinhorn (2007); Cimellaro et al. (2009), (2010)), indicating the period necessary to restore the functionality of a structure, and infrastructure system to a desired level that can operate or function the same, or close to, or better than the original one.

For the purposes of EU-CIRCLE, each stage for each asset and hazard can be modeled through a first order approximation requiring only the rate of capacity change (either negative for the disaster stage or positive for the restoration) and a time interval. It is possible that stages A3 and A4 could be merged, or a different approximation is used.

3.5.3 Interdependency analysis

For the purpose of the EU-CIRCLE project a generic syntax for the description of a specific network state is used, as denoted in the previous section . This generic variable, $S_i(t)$, with property k, referring to the node i of the network j is defined as:

$$S_{i[\text{Node}],j[\text{Network}]}^{k[\text{property}]}(\text{t})$$

The diffusion of relevant information, such as the present state of operation, between interdependent networks is a key component of the network analysis. In more details, the interconnection links are characterized by a function that expresses the way the one network influences the operation of the interconnected networks. In general terms, it is defined as:

Formula 3
$$NS_{i,j} = function\left(PS_{i,j}, PS_{i',j'}, interconnection\ type\right)$$

$NS_{i,j}$ denotes the Network State of node i of the network j, $PS_{i,j}$ stands for Previous State of node i of the network j. Interconnection types according to Rinaldi et al. are used as described in Section 3.4.3. In mathematical terms, the failure of node i due to loss of service LS in a network j is designated as $E_{\text{ij}}^{\text{LS}}$. The event E_{ij} can then be define as the union of the events $E_{\text{ij}}^{\text{LS1}}$, $E_{\text{ij}}^{\text{LS2}}$, …, $E_{\text{ij}}^{\text{LSn}}$.

Formula 4
$$E_{\text{ij}} = E_{\text{ij}}^{\text{LS1}} \cup E_{\text{ij}}^{\text{LS2}} \cup \ldots \cup E_{\text{ij}}^{\text{LSn}}$$

Loss of service incorporates the damages due to a hazard, such as flood, and the non-functionality due to a failure of a node from another network, for example the waste water network (blue dots in Figure 27). By solving each network independently and then considering their interaction the proposed approach analyses a system of infrastructures. Infrastructure networks can be seen as layers which overlap each other and share some nodes which are presented in both networks and are connected by inter-infrastructure edges. This approach brings many benefits:

1. It discerns the analysis and results of layers and interdependencies and aids the understanding of where critical points are located and which are the tighter and more stressed inter-links. While the single infrastructure assessment is mature, the interdependency studies are still at a development stage.
2. Moreover, giving the possibility to each infrastructure manager of running the model of a given layer and then controlling the interaction between the different layers at a higher level is closer to the professional practice adopted during an emergency response phase.
3. In the end, the diffusion of informatics tools, like Geographic Information Systems (GIS), in both the emergency response and the risk planning sector, suggests the adoption of a unified methodology. The GIS platform has great potentialities and it can be effectively used to organize input data and visualize outputs. Their relational databases are shaped with a layer structure which is in accordance with the one proposed above.

3.5.4 Example

For example, a step by step description of the horizontal analysis is shown in Figure 36. The different types of network (water, energy and transport) are solved independently.

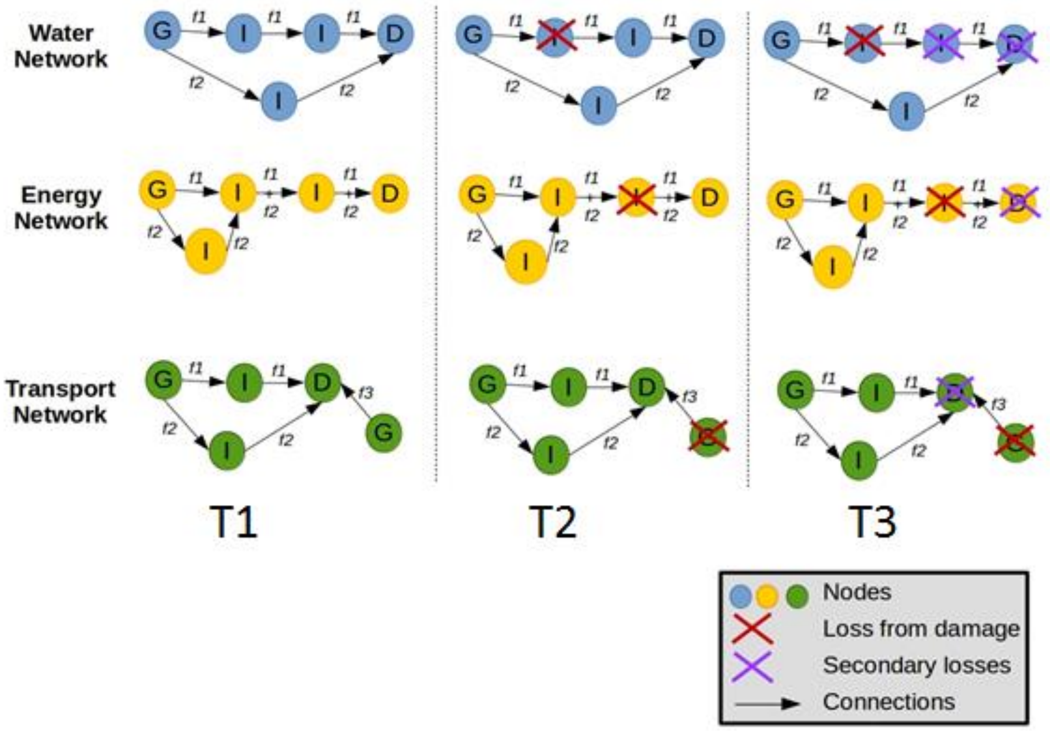


Figure 36: Horizontal network analysis.

In the Water Network a water pump, which is an intermediate node, fails due to a hazard (middle part in Figure 36). As a result, the flow path, after the failed node, is disrupted from the network (right-most part in Figure 36). In the same way, a substation fails in the energy network and the main railroad station in the transport network. Next, the vertical analysis takes place.

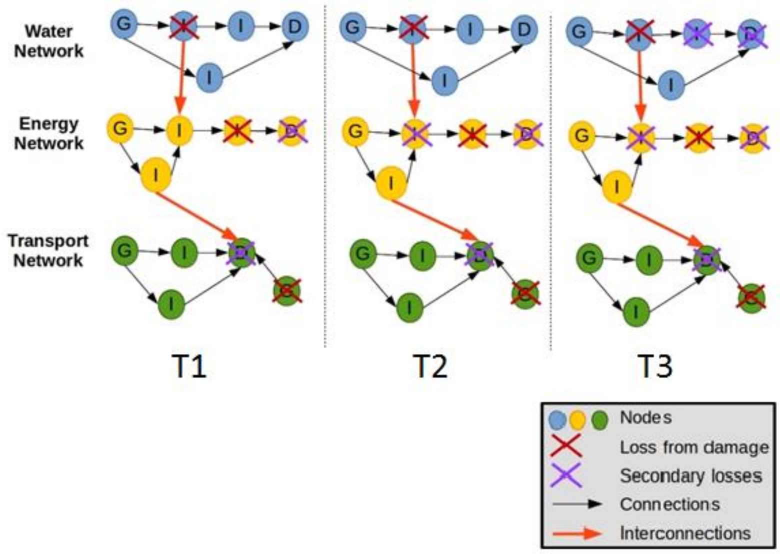


Figure 37: Vertical network analysis.

As a result of that a revaluation of the CI properties must be performed after each analysis. Afterwards a simulation is performed first to the 1st network (electricity network) and then to the water network, parts of the interdependent network (electricity and water network). At the same time of the preliminary analysis, damages-impacts are placed into nodes-links of the interconnected network, while in the last step, an analysis of the new already modified interdependent network is performed comparing the results with those of the basic scenario analysis, in order to define on the one hand which assets are affected in terms of supply & demand, capacity, aging etc. while on the other hand to predict network functionality.

The failure is passed between networks according to the interconnection structural information. The network pump affects the cooling system of an electrical substation and as a result the substation goes off-line (step 2 in Figure 37). In addition, a railroad station fails to perform due to a loss of node in a horizontal analysis. As a result, the need for energy is diminished and the flow of power from the energy network is diminished too (step 3 in Figure 37).

3.5.5 Minimum cost/Maximum flow solutions

A critical infrastructure can be viewed as a collection of interconnected components that work together as a system to achieve a particular, domain specific function. Modeling the system as such, the response of the CI to hazard could be described as an optimization problem of minimum cost and maximum flow problem.

Formula 5

$$min\left(\sum_{j=1}^{N}\sum_{i=1}^{N} flow_{ij}\, cost_{ij}\right)$$

$$0 < flow < \max \quad capacity\ of\ generation\ node(s)$$

That approach provides a general description for all types of networks and a solution of interdependency analysis. Below two approaches are described, based on a time evolution of the hazard:

- Time independent analysis(TI),
- Time dependent analysis(TD)

3.5.6 Time independent analysis (TI)

Under this approach, any specific hazard E which is associated to physical quantities (water depth, floods, forest fires, extreme temperatures etc.) and has large spatial extend, can impact various part of the infrastructure with different intensities.

The vulnerability of exposed assets (nodes and links) is represented by the fragility curves, which define the probability of failure of each node depending on the type of hazard considered. Therefore, for each node there are as many fragility curves as the type of hazard acting. The probability of state change P_{ij} of a node under a specific event E, is obtained by inserting the value of the E into the node fragility curve. The assignmentassign of probabilities to the nodes and how they change their state if the event affects them, is part of Structural and Operation Analysis (SO).

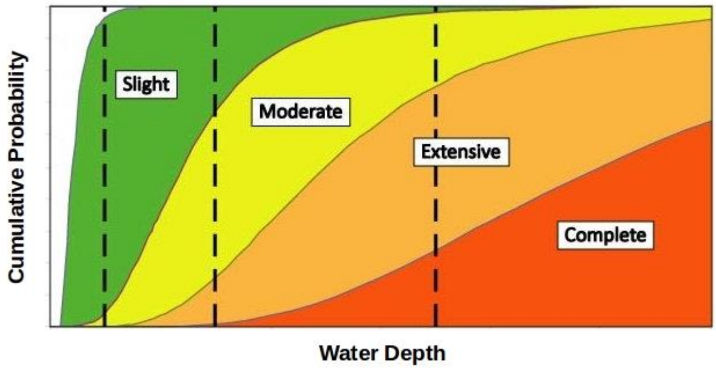


Figure 38: Fragility curve.

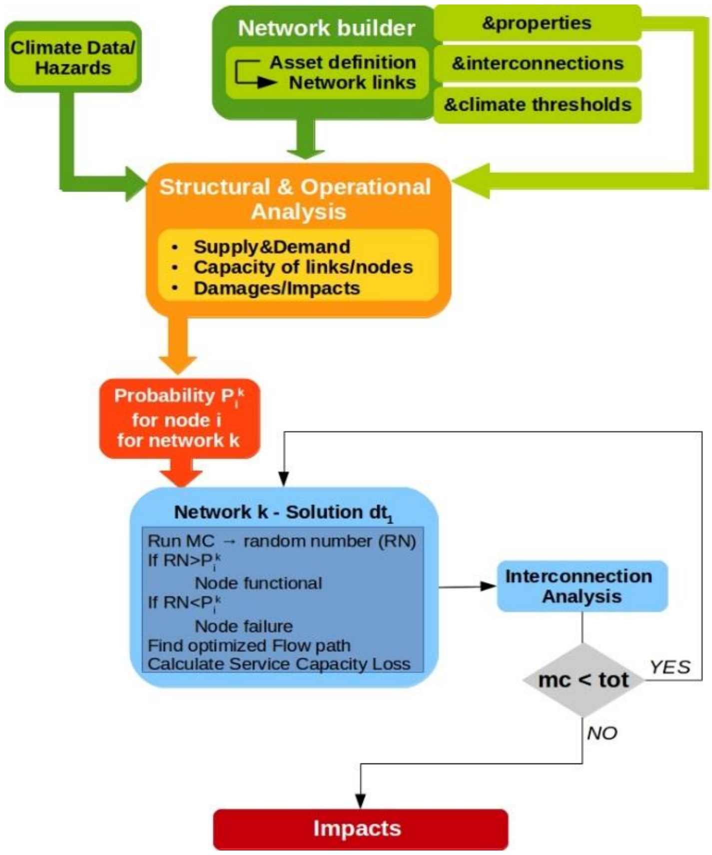


Figure 39: Standard Probabilistic Network Analysis flow chart.

This operation creates a value for each node that expresses the service loss of a node due to a hazard. Then, a network analysis solution takes place, as described below:

1. Determine which nodes are going to change state.
2. Calculate new flow and cost values of the network creating thus a new network affected by the hazard.
3. Solve a minimum cost and maximum flow optimization problem for each type of network.
4. Conduct an interdependency analysis.
5. Repeat steps 1 to 4 for a predefined number of steps.
6. Perform impact analysis.

A very useful information for the CI operation, is the time that the network will gain back part or total operation, after the extreme event. In order to assess that, CIRP introduce a restoration time value for each asset, that can be utilized in the impact analysis and calculate the average time that the network will be fully operational.

3.5.7 Time Dependent Network Analysis (TD)

The spatial evolution of an exteme event can affect the types of CI networks differently and thus, the solution may differ from a "instant" enforcement of the hazard. In addition, it is very useful and interesting to know the behavior of the CI during the duration of extreme events. In order to take into account time evolution scenarios, a Time Dependent Network Analysis is proposed.

The first step in the TD analysis is to discretize time according to the evolution of the hazard. Then, the different time periods are inserted as inputs, in the Scenario Development step. CIRP calculates the maximum intensity during the event for each asset and the time step that is reached. That value is used in order to assess the point that the recovery process can start. Each type of asset has a recovery time value as described in Section 3.5.6. If the maximum value of the hazard has been reached, the asset begins to recover during the next time steps based on a restoration curve/function that is defined using the recovery time value of the asset. That method incorporates the recovery process in the Network analysis step, and permits a dynamic function of the nodes of the network over time, where nodes can lose or restore service. The analysis begins sequentialy from the first time step by performing a network analysis as described in Section 3.5.6 taking into account the restoration process of the asset.

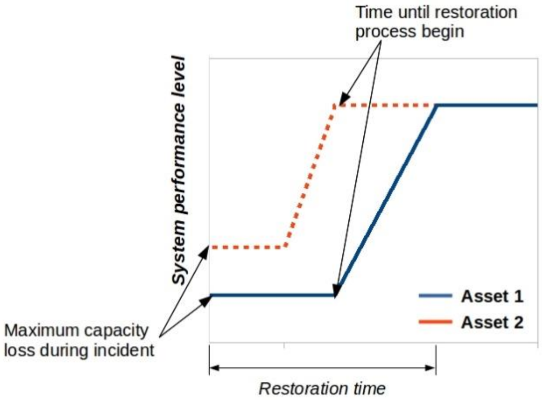


Figure 40: Restoration curve

The result is a new network state matching the hazard at a specific time period. The next time period initializes with the new network state together with the next time step of the hazard. The procedure is being repeated sequentialy for all the time periods that were determined at the first step.

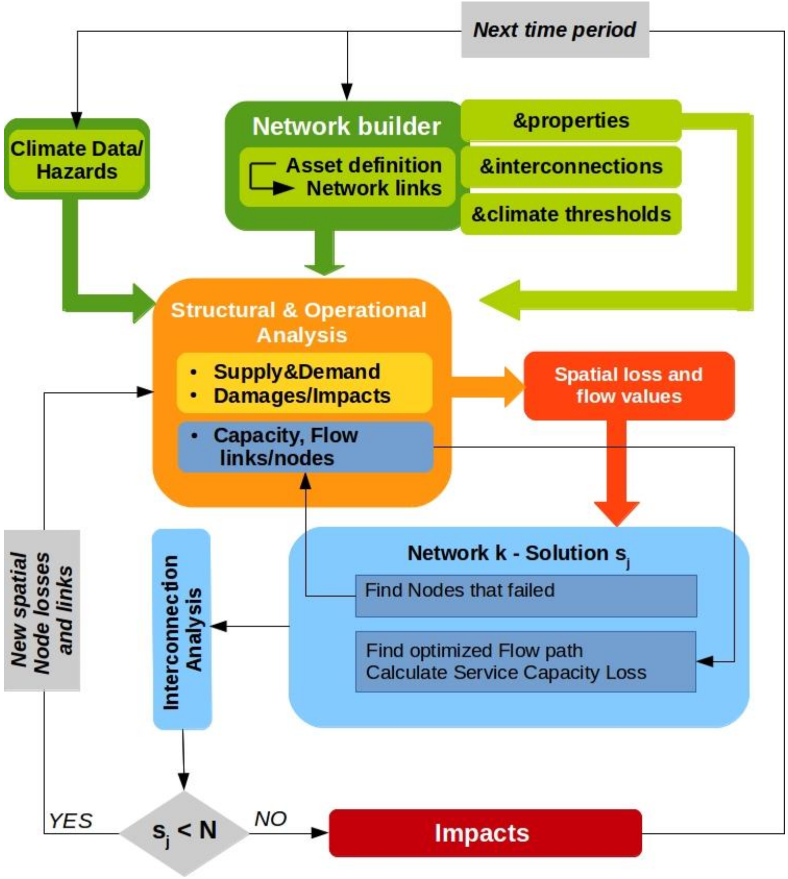


Figure 41: Resilience Factor Network Analysis flow chart.

The steps that TD follows are:

1. Discretization of time according to hazard
2. Solve as TI
3. Perform impact analysis
4. A new network state is determined
5. Run the next time period with the new state of network as initial step
6. Repeat for all time periods (N in total)

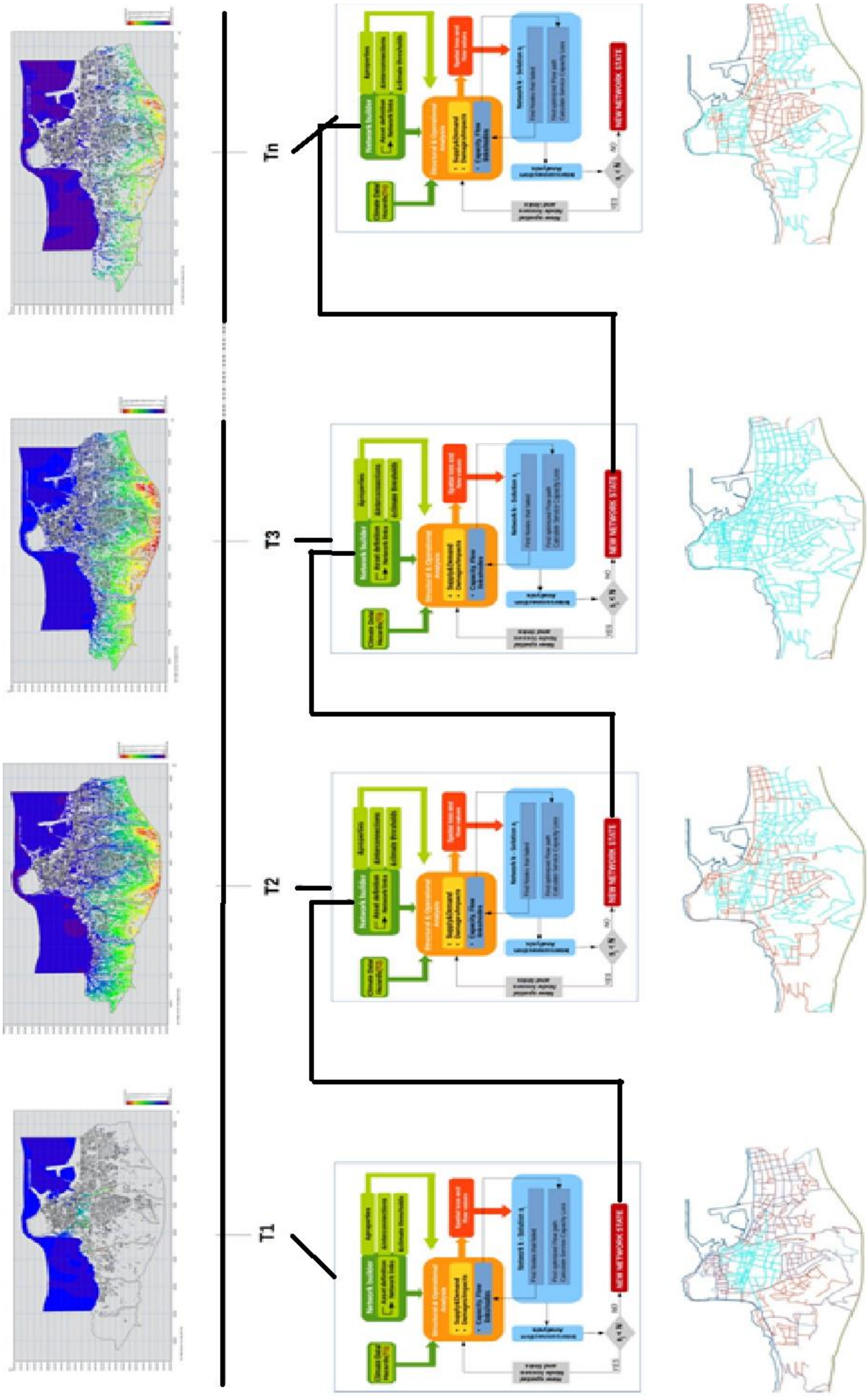


Figure 42: Time Dependent Network Analysis example

3.6 Defining impacts/consequences

Consequence of a risk is defined as a measure of the disruption and impact of a climate hazard not only on a single asset, but to society in general and is thus used in conjunction with likelihood to assess its overall severity. Such an approach proposed within the EU-CIRCLE framework for the determination of the incident consequences will build upon a two level hierarchy. The proposed analysis within EU-CIRCLE tries to incorporate two conceptually different but highly interrelated types of impacts that clearly identify the influence of interconnected critical infrastructures on society and its functioning.

Thus a two tier approach is proposed where

- ***Direct impacts*** to the interconnected CI network are identified, and described and quantified through different indicators and
- ***Indirect impacts*** to society, that are directly resulting from the CI not being able to function according to their intended scope

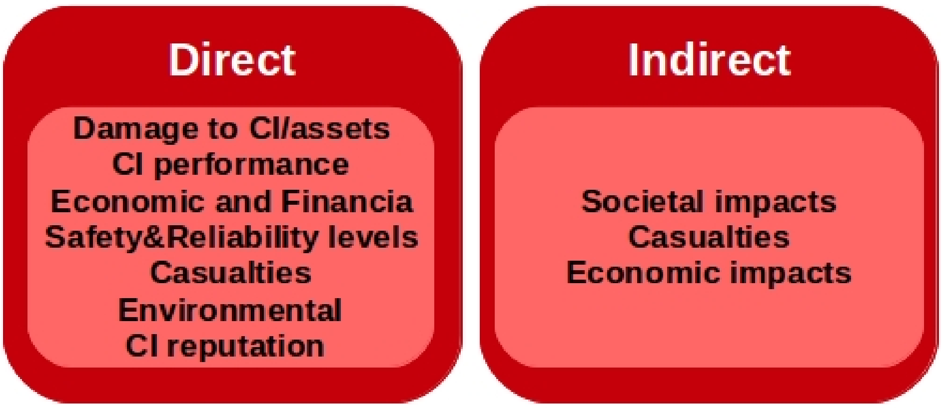


Figure 43: Proposed direct and indirect impacts (selection)

3.6.1 Direct impacts

This category of impacts directly affects the CI (or the interconnected network of CI), in multiple pathways which are presented in the following points:

i. Damages to CI assets

Assets that are completely or partially damaged (significant destruction from its as-builtbuild state) due to a climate hazard. The enumeration of this category could be through different indices such as:

- number of assets fully damaged (beyond reparability)
- number of assets partially damaged
- number of assets with a [over] certain per cent (%) or range of damages
- highest per cent (%) of damage per network
- average damage per network
- Enumerated damage per [asset / network]. Value depending on network specific properties (e.g. km of roads destroyed, km of railways, km of water pipelines, km of electricity transmission network, etc.)

ii. CI performance

This category refers to the change of the capacity of the CI network (or interconnected networks) to maintain its fully functional performance level, as identified in the baseline category of normal operation. The following parameters could be relevant:

- Flow reduction in network asset (node / link)
- Changes in network generation capacity
- Changes in network demand capacity
- Changes in network links capacities due to climate hazards
- Time that CI is not able to serve its intended function
- Total time that person is left without any CI services
- Total time that person is left without two or more CI services

The network simulation solutions that were described in section XX (3.4), could be used to derive performance related indicators as follows:

Connectivity Loss (CL)

Connectivity Loss is a measure of the ability of every distribution node to receive from a generation node and it is defined as:

Formula 6

$$\mathrm{CL} = 1 - \sum_{\mathrm{j}=1}^{N} \frac{G_j^{\mathrm{ap}}}{G_j^{\mathrm{af}}}$$

where N is the number of distribution nodes, G_j^{af} denotes the number of generation nodes able to feed flow to the j distribution node, and G_j^{ap} denotes the number of generation nodes able to supply power to the j distribution node.

Service Flow Reduction (SFR)

Service Flow Reduction (SFR) determines the amount of flow that the system can provide compared to what it provided before the “event”. SFR is defined as:

Formula 7

$$\mathrm{SFR} = 1 - \sum_{\mathrm{j}=1}^{N} \frac{\mathrm{PR}_j}{\mathrm{CS}_j}$$

where PR_j denotes the actual flow at the j distribution node, and the CS_j represents the demand of j distribution node.

Asset / Network Resilience Curve

The estimation of the System Performance (flows , performance levels, …) at different time intervals, can be used to construct the resilience curve of an asset/network which is very useful to quantify the resilience of this system. Overall, according to many different approaches, this is quantified by the area covering the performance reduction and recovery phases (Ganin, et al.

(2016), Cimellaro, et al. (2010), Ouyang & Wang (2015) , Ouyang & Dueñas-Osorio (2012), Bocchini, et al. (2014)).
Additionally, it may be used to examine /compare different adaptive/transformative measures aim at enhancing the CI resilience through strategies that improve the infrastructure's functionality and performance level and that decrease time to full recovery, leading to a reduction of the area covered by the "inverse trapezoid" .

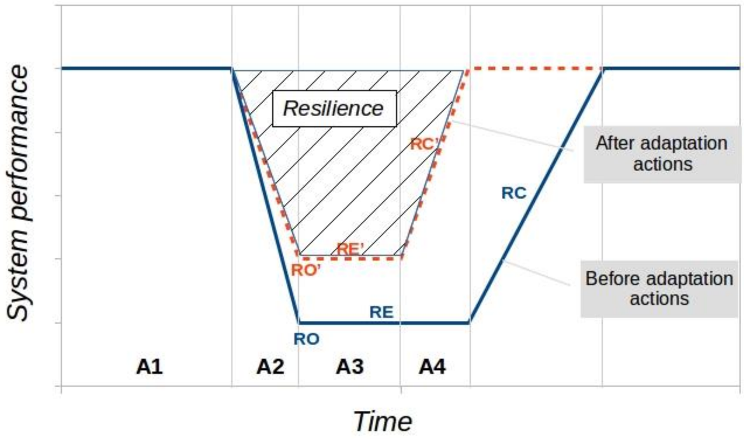


Figure 44: Asset/CI constructucted resilience curve.

From the Figure 44, the following indicators may be obtained, which are also analysed in D4.1:

- **Resistance & Reliability (Robustness):** the ability of systems, system elements, and other units of analysis to withstand disaster forces without significant degradation or loss of performance. Successive adaptation measures could result in RO':
  - reduce the duration where the CI is exposed to a hazard
  - build better defenses to reduce the consequences
  - to maintain a higher performance level
- **Redundancy:** the extent to which systems, system elements, or other units are substitutable, that is, capable of satisfying functional requirements, if significant degradation or loss of functionality occurs. Successive adaptation measures could result in RE′:
  - shorter time for response
  - operation of alternative options to maintain service
- **Response:** the ability to diagnose and prioritize problems and to initiate solutions by identifying and mobilizing material, monetary, informational, technological, and human resources. Successive adaptation measures could result in RS':
  - shorter time for acquiring all necessary resources
  - minimization of economic cost
- **Recovery:** the capacity to restore functionality in a timely way, containing losses and avoiding disruptions. Successive adaptation measures could result in RC':
  - faster restoration of services

iii. Safety Indices

Taking into account the importance of the effectiveness of the safety and operating processes of interconnected infrastructures and the change of behaviour due to climate stressors, the safety and reliability states can be used as an impact indicator. As such the following indicators may be used:

- the critical infrastructure component safety function
- the mean lifetime of the component / asset in the safety state subset $\{u, u+1, ..., z\}$
- the standard deviation of the component / asset lifetime in the safety state subset $\{u, u+1, ..., z\}$
- the intensity of ageing of the critical infrastructure component Ei/the intensity of critical infrastructure component Ei departure from the safety state subset $\{u, u+1, ..., z\}$
- the critical Infrastructure mean lifetime $T(r)$ up to exceeding critical safety state r
- the standard deviation of the critical infrastructure lifetime $T(r)$ up to the exceeding the critical safety state r
- the moment τ of exceeding the acceptable value of critical infrastructure risk level δ
- the intensity of ageing of the critical infrastructure, the intensity of critical infrastructure departure from the safety state subset $\{u, u+1, ..., z\}$

Annex 1 presents a multi-state methodological approach on how to identify multi-state safety functions of interconnected critical infrastructures

iv. Casualties

Casualties include fatalities and injuries to employees of the CI operation and also to those using the infrastructure at the time of the incident (related only to transportation networks and governmental services, health sector). Casualties can be quantified using two approaches:

- **Numerically**, in an absolute manner, such as the number of people exposed,
- **Person years lost.** (Klaver, et al., 2008) define this index as the sum of: a) Half the life expectancies of the people who lost their lives, b) The total period that people are hospitalized and in recovery, the percentage unable to live a normal life times the period affected, and the decrease in life expectancy

v. Economic and Financial Perspectives

Economic losses are estimated on the network (and/or interconnected networks) where the incident occurred and accounts for the following elements:

- Costs of damaged assets
- Loss of income as a result of not servicing demand
- Loss due to possible penalties from violating service level agreements with buyers
- Costs for replacements of services
- Restoration and recovery costs
- Maintenance costs after hazard

Total economic costs and losses can be calculated as follows, with reference to the intervals identified in 3.5:

total economic costs & losses =
[cost of economic losses & costs damaged assets] @ (the damage absorption stage A2) +

[cost of economic losses + cost of response + cost of replacement] @ (the response stage A3) +
[economic losses + recovery cost] @ (recovery stage A4) +
[loss of income from not servicing + maintenance costs] @ (all stages of this incident)

Additionally, the risk premiums to a specific CI maybe alternated in the light of changing climatic conditions and exposure to increasing levels of risk.

All economic effects shall use the same metric, preferably in a common currency. Furthermore, due to the change of the monetary value over time all losses that last more than a year should be annualized using the Net Present Value (NPV) method.

vi. Environmental Losses

As CI operation is expected to have an impact on future climate, especially the operation of highly susceptible infrastructures such as energy, the production of Greenhouse Gases can also be considered as an impact within the proposed approach. The following types of pollutants are considered, the estimation of which will be done based on emission factors from existing international databases

- Air pollutants affecting local air quality (NOx,SOx, CO, PM of various dimensions, VOC) and toxics (EMEP/EEA air pollutant emission inventory guidebook 2013)
- Green house gases (http://www.ghgprotocol.org/Third-Party-Databases/IPCC-Emissions-Factor-Database)
- Hazardous materials & toxics, that may be classified according to the chemicals danger classification obtained from the related web site of the Globally Harmonized System of Classification and Labelling of Chemicals (http://www.unece.org/trans/danger/publi/ghs/ghs_rev01/01files_e.html)

In case of spills and leak of chemicals and hazardous materals involved in the incident a series of indices can be used to stress the impact of the substance on the environment. Once the amount of the material is quantified then a dispersion model (from the simplest Gaussian one and towards more complex models) could be applied to define the impacted area.

Environmental/ecological effects can be expressed in terms of the size of the impacted area, an indication of severity based on recovery time needed to fully restore the state of the environment in its previous state and as an indicator of the ecosystem and biodiversity that is at-risk. The latter is critically important if the location of the natural hazard on the CI network is under a protected area (NATURA 2000, RAMSAR treaty etc.).

vii. CI reputation

This type of impact is related to the reputation of the CI (can be classified in a categorical way) in a subjective-quantitative estimate from subject matter experts-CI operators.

3.6.2 Indirect

This category pertains to the impacts affecting society that is served by the CI. As such they correspond to impacts on diverse groups of people accounting for a holistic assessment and quantification of the role of CI.

i. Impact on societal groups

This category accounts for the part of society whose demand for CI services is not (or is partially) met due to the CI not being able to meet the required demand. This can be further expanded into the following elements

- Number of people exposed / affected
- Number of in-need societal groups (in people) not-served, such as infants, elderly, patients, etc.
- Number of houses not-served
- Number of enterprises not-served
- Number of special facilities not-served (elderly care, kindergarten, schools, etc.)

Additionally, psychological effects can be accounted for, as a measure of the citizen confidence in the CI network and is directly related to their motivation in continuing using the network in the future. The psychological impacts are classified as:

- Annoying: Irritating for the individual, but not disruptive for his/her daily routine
- Disruptive: The individual will have to adapt his/her daily routine
- Disturbing: The individual will have to make significant alternations to his/her daily routine
- Dysfunction: the individual is no longer able to continue his/her daily routine

Considering risk assessment of **political** effects, it is obvious that only those political aspects can be considered that can be assessed beforehand. Risk assessment cannot and shall not take into account heightened political sensitivities between parties such as that during an election period or sequences of events which may have led to a political change, unless it considers the re-evaluation during or just after an incident. The only political effects that can be qualitatively assessed are the risk of policy changes that affect the process or structure of the business or the sector after an incident and the continuation of governmental operations at all levels of government.

ii. Casualties

Casualties include fatalities and injuries to the society caused due to the CI not being able to perform an agreed level of operation. Casualties can be quantified using the same two approaches as for the direct impacts. Also accounting for possibly displaced people.

iii. Economic impacts

Economic losses are estimated for the economic activity of the society that is affected by the climate hazards on the network. The Critical Infrastructure Network (CIN) is considered as an integrated production system consisting of different assembly lines/economic activities. In other words the CIN is an economic entity composed by district economic activities while is incorporated in a total economic system at regional or/and national level. The time dimension will be taken into account by implementing ex-post and ex-ante (hazard/disaster) methodologies in order to cover at highest level the risk assessment and management in CI.

The impact of the security incident on the economic system of a country, region or area may be defined from the Input – Output Matrix, using the Leontieff framework. The fundamental information used in input–output analysis concerns the flows of products from each industrial sector, considered as a producer, to each of the sectors, itself and others, considered as consumers. This basic information from which an input– output model is developed is contained in an interindustry transactions table. The rows of such a table describe the distribution of a producer's output throughout the economy. The columns describe the composition of inputs required by a particular industry to produce its output (Miller, et al., 2009).

		PRODUCERS AS CONSUMERS								FINAL DEMAND			
		Agric.	Mining	Const.	Manuf.	Trade	Transp.	Services	Other	Personal Consumption Expenditures	Gross Private Domestic Investment	Govt. Purchases of Goods & Services	Net Exports of Goods & Services
PRODUCERS	Agriculture												
	Mining												
	Construction												
	Manufacturing												
	Trade												
	Transportation												
	Services												
	Other Industry												
VALUE ADDED	Employees	Employee compensation								GROSS DOMESTIC PRODUCT			
	Business Owners and Capital	Profit-type income and capital consumption allowances											
	Government	Indirect business taxes											

Figure 45: Input-Output Matrix.

Input-Output Model:

X=Ax+Y,

Where: X= Production Y= Final Demand, A=Technical Coefficient Matrix

Each element of A (Technical Coefficient Matrix) represents the quota of each sector's production:

$a_{ij} = X_{ij} / X_j$

I.e, the technological factor a_{ij} shows the share of x_i industry in the total output of industry j.

Assuming each CI of the network (system) as a productive sector of this system that is interdependent with other CIs (sectors) we could find the extention of this direct and indirect interdependency across all CIs. This assumption is not far from the reality, taking into account that according to EUROSTAT's National Accounts (based on I-O framework) the most of CI are separate economic sectors (i.e. Energy Sector, Transport Service Sector). More specifically, a unitary impact on the CI network activity class (input) **y**, would result in an analogous impact estimate $\mathbf{x} = (\mathbf{I}-\mathbf{A})^{-1}\, \mathbf{y}$, where x (output) are economic values on an economic activity level, and $(I-A)^{-1}$ is the inverse Leontief Matrix which shows the direct, indirect and induced interdependencies of all production sectors.

Therefore, the system's solution is:

$X = (I-A)^{-1}Y$

Under the proposed scheme, the economic costs account not only for the costs of the public sector or the infrastructure operator, which is currently practice, but will also account for the economic costs to the private sector.

Again, all Economic effects shall use the same metric, preferably in a common currency. Furthermore, due to the change of the monetary value over time all losses that last more than a year should be annualized for instance by means of using the Net Present Value (NPV) method.

3.7 Risk indicators and categories

This section tries to demonstrate the modularity and capacity of the proposed approach to be compatible with the main methodological that exist. Thus using the EU-CIRCLE risk framework, it is possible to account

3.7.1 Indicators of Sendai Framework

In order to measure the progress of the implemntation of the Sendai Framework and its seven targets, an open-ended intergovernmental expert working group on indicators and terminology relating to disaster risk reduction has been tasked with developing the relevant indicators. The working group has released a Collection of Issue Papers on Indicators for the Seven Global Targets (UNISDR, 2015), which puts forward a basic set of requirements for recording and reporting disaster loss to UNISDR in order to monitor the Targets (a) through (d) (released as part of Technical Review). Particularly relevant for EU-CIRCLE is ***the newly introduced Target D of the Sendai Framework which deals exclusively with Climate Change impacts to Critical Infrastructure***. Based on the working version of **Global Target D which is to: Substantially reduce disaster damage to critical infrastructure and disruption of basic services, among them health and educational facilities, including through developing their resilience by 2030**, the following indicators have been proposed by the working group. They are tabulated and linked to the impacts/consequence definitions of EU-CIRCLE as these were analysed in Section 3.6.

Table 8: Impacts indicators as defined by Sendai Framework Target D.

Sendai Framework Target D proposed indicators[3]	**EU-CIRCLE impact**
D-1 - Damage to critical infrastructure due to hazardous events.	Direct impacts – damages to CI assets
D-1 bis. - Number of electricity plants and transmission towers destroyed or damaged by hazardous events	Direct impacts – damages to CI assets focus on energy networks
D-2 – [Number / percentage] of health facilities destroyed or damaged by hazardous events	Direct impacts – damages to CI assets focus on health infrastructures
D-3 - [Number / percentage] of educational facilities destroyed or damaged by hazardous events	Direct impacts – damages to CI assets focus on govermental services
D-4 - [Number / percentage] of [major] transportation [units and] infrastructures destroyed or damaged by hazardous events[4]	Direct impacts – damages to CI assets focus on transportation sector

[3] working text on indicators based on negotiations during the second session of the open-ended inter-governmental expert working group on indicators and terminology relating to disaster risk reduction held in Geneva, Switzerland from 10-11 February 2016, issued with factual corrections on 24 March 2016

[4] the indicator measures (1) road (in kilometres of paved/unpaved), (2) railway (in kilometres), (3) port (number of facilities) and (4) airport (number of facilities)

D-4a. – Extent of damage to ports and airports	Direct impacts – damages to CI assets
D-4b. – Kilometres of road destroyed/damaged by hazardous event	Direct impacts – damages to CI assets
D-4c. – Number of bridges destroyed/damaged by hazardous event	Direct impacts – damages to CI assets
D-4d. – Kilometres of railway destroyed/damaged by hazardous event	Direct impacts – damages to CI assets
D-4e. – Number of days airport(s) have been closed due hazardous event	Direct impacts – CI performance transport sector
D-4f. – Number of days port(s) have been closed due hazardous event	Direct impacts – CI performance transport sector
D-4g. – Number of days telecommunications breakouts have been experienced due hazardous event	Direct impacts – CI performance ICT sector
D-4h. – Number of days power breakouts have been experienced due to hazardous event	Direct impacts – CI performance energy sector
D-4i. – Number of days without water supply due to hazardous event	Direct impacts – CI performance water sector
D-4j. – Number of days without sanitation services due hazardous event	Direct impacts – CI performance health sector
D-5 – [Number / Length / Percentage] of [time / days / person days] basic services have been disrupted due to hazardous events[5]	Direct impacts – CI performance collective assessment
D-7 - [Number / percentage] of security service structures destroyed or damaged by hazardous events	Direct impacts
D-10 – Number of communication infrastructure destroyed or damaged by hazardous events	Direct impacts – damages to ICT sector
D-14 – Number of water and sanitation infrastructures destroyed or damaged by hazardous events	Direct impacts – damages to CI water sector
D-15 – Number of days financial services have been disrupted due to hazardous events	Direct impacts – CI performance financial sector

3.7.2 European Programme for Critical Infrastructure Protection EPCIP

Council Directive 2008/114/EC has identified three different cross cutting criteria for the identification of impacts to the European Critical Infrastructures. Their correspondence to EU-CIRCLE indicators can be found in the following Table

[5] Sectors monitored include healthcare services, education services, transport sector, ICT, water supply, sewage system, solid waste management, power/energy system and emergency response.

Table 9: Impacts as defined by EPCIP.

EPCIP Programme (Theocharidou & Giannopoulos, 2015)	**EU-CIRCLE link**
Human impacts	Direct Impacts – casualties
- Quantitative (in no. of affected people). e.g. number of deaths, number of severely injured or ill people,	Direct Impacts
- number of permanently displaced people	Indirect Impacts - casualties
Economic and Environmental impacts	Direct Impacts – economic & financial AND environmental losses
- e.g. immediate or longer-term emergency measures	Not accounted
- Restoration	Resilience Curve
- Environmental costs	Direct Impacts – Environmental Losses
- Costs of disruption of economic activity,	Direct Impacts – Economic and Financial impacts
- value of insurance pay-outs	Direct Impacts – Economic and Financial impacts
- indirect costs on the economy	Indirect – Economic Impacts
- indirect social costs	Indirect – impacts on societal groups
Political/social consequences	Indirect – impacts on societal groups

3.7.3 National Risk Assessment Plans

According to the Commission Staff Working Paper on Risk Assessment and Mapping Guidelines for Disaster Management (European Commission, 2010), Member States are engaged in a process of describing and cataloguing risks and risks scenarios. Many EU Member States have used a different set of criteria for assessing risk, which are linked to the EU-CIRCLE approach.

The information used within the NRA to consider the likelihood of events is:

- frequency of one or more incidents in various time scales (CZ, IE, LT, NO, PL, HU)
- probability of occurrence within 1 year (EE, EL)

With regards to consequences all MS have used a 5 distinct categories approach, but different criteria have been employed for each one. Concerning the potential for loss of critical infrastructure, which is the scope of EU-CIRCLE, this threat has been specifically identified as a cascade effect of most of the other risks addressed in this review. There is also an additional risk of direct malicious and non-malicious interference to the normal operation of critical infrastructure. The impacts arising from a loss of critical infrastructure, are the disruption to, or complete cessation of, the delivery of essential services to large sections of the public.

Essential services include the provision of energy, water, food, communications, health and emergency response services, transport and finance. The effects on citizens arising from disruption or cessation of any of these essential services will depend on the duration of the disruption, the time of year, the resilience of the service, and the response by the authorities, but will probably involve a societal effect, economic consequences, and in extreme cases casualties. The following table presents a linkage between identified CI risks by MS linked to EU-CIRCLE approach

Table 10: Linkage between CI threats and EU-CIRCLE.

Country	Threat	EU-CIRCLE
CZ , IE	Critical infrastructure disruption	Direct impacts – Damages to CI assets & CI performance
DE	Outage of critical infrastructure	Direct impacts – CI performance
PL	Disruption of electricity supplies, of fuel supplies, of natural gas supplies	Direct impacts – Damages to CI assets & CI performance (energy, chemical sectors)
NL	National power failure	Direct impacts – Damages to CI assets & CI performance (energy sector)

Additionally, within the NRA different criteria have been used for assessing impacts, their link to EU-CIRCLE approach is shown in the following Table

Table 11: Impact criteria of NRA and link to EU-CIRCLE.

Country	Impact	EU-CIRCLE
All	Humans – injuries - fatalities	Direct & indirect impacts - casualties
All	Assets – economic damage (euros)	Direct & indirect impacts – economic criterion
EE, EL	Vital service: disruptions, direct losses	Direct impacts – damages to CI assets, CI performance
IE	Infrastructure: economic losses	Direct impacts – economic criterion
IE	Social: disruption to community services or infrastructure	Indirect impacts- impacts on social groups
LT	disturbances of supply or outage of energy; traffic burdens	Direct impacts – damages to CI assets, CI performance (energy & transport sectors)

3.8 Uncertainty estimation in the EU-CIRCLE process

A critical element of EU-CIRCLE to to estimate the uncertainty of the risk estimation process, that consists of the error that the whole framework incorporates. In-line with the risk modeling process, the uncertainty of every model phase can be quantified with a mathematical function and be classified in a cardinal scale. Alternatively, and in the case of the use of categorical information directly, it can be categorized to the same scale by the same "expert's opinion". The latter involves cases where a strict mathematical approach cannot be applied, but an expert with years of experience may assess the data and classify them to a scale.

In the end of all model phases, the whole uncertainty of the process may be calculated as the weighted average. The scale that the uncertainty of each model phase is categorized , consists of five(5) classes from very low to very high uncertainty, similar to the risk estimation.

VERY LOW	LOW	MEDIUM	HIGH	VERY HIGH

The different levels of uncertainty can be broadly expressed as:

- ✓ Very High : high modeling error >80% or relative terms & estimate based upon no supporting scientific evidence.
- ✓ High : Expert view based on limited information, e.g. anecdotal evidence, & modeling outcomes with important error 60-80% on relative terms.
- ✓ Medium - Estimation of potential impacts or consequences, grounded in theory, using accepted methods and with some agreement across the sector, quantified modeling error between 40-60% in relative terms
- ✓ Low - Reliable analysis and methods, with a strong theoretical basis, subject to peer review and accepted within a sector as 'fit for purpose', quantified modeling error for a specific process between 20-40% in relative terms
- ✓ Very Low - Comprehensive evidence using the best practice and published in the peer reviewed literature; accepted as an ideal approach (no risks, received a very high confidence score)

For example the uncertainty of historical and simulation climate date can be calculated with mathematical equation, but the theoretical response of an asset in a hazard (damage function) is not tested , thus, the uncertainty is an “expert’s opinion”. In the case where some inputs are not fully known, or the source that they have been taken from, is not trusted, an experience user can estimate the error, hence, the uncertainty of the process and insert into CIRP. The proposed approach ensures that the risk assessment process described previously, is precisely followed by the uncertainty estimation using a combination of precise estimation of uncertainty (if available) and expert’s opinions.

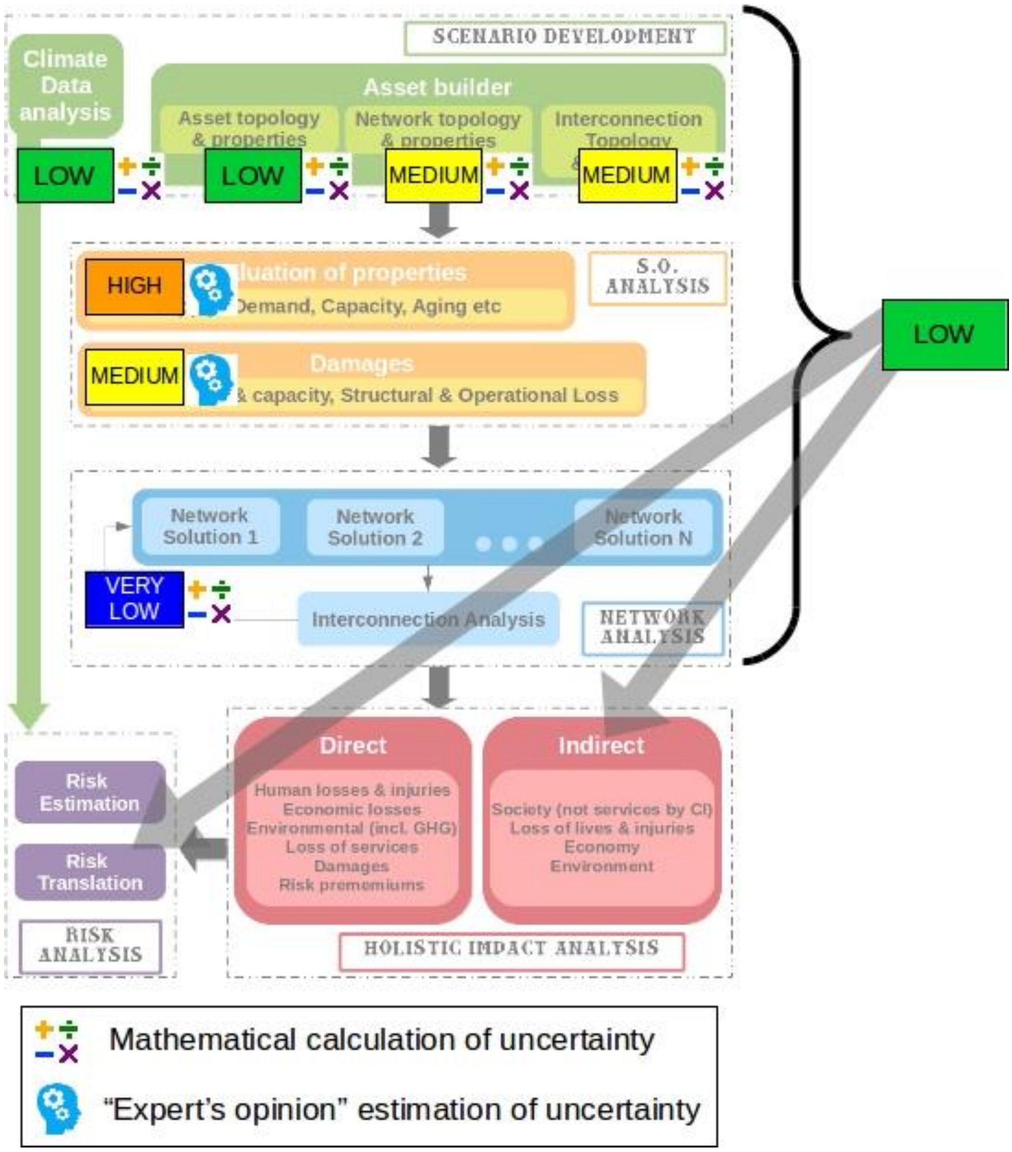


Figure 46: Example of uncertainty calculation

4 Introduction to EU-CIRCLE case studies

According to the DoW, we foresee the following strategy to conduct the case studies with reference to the proposed rik assessment modeling framework.

1) Setup – scenario specification design. This task will result in an initial scenario specification which will guide the initial stages of the case study in the quest for the most suitable models and fitting climate / weather data and CI asset definition.
2) Model implementation and customization, will result in a very specific elaboration of the web-based tool using CI models, systems and climate / weather data required to perform each case study.
3) Case Study Description and preparation, where a specific scenario will be derived, with discrete events and their timeline, CI description, targets and envisaged application of the EU-CICLE framework. During the course of the actual demonstration different variations of the case study may be demonstrated, for example different climate hazards, timescales introduced, adaptation measures and their comparison and validation etc.
4) Data collection. This task involves the collection and processing according to the EU-CIRCLE defined standards of the necessary data in order to conduct the case study. This task will involve particularly CI assets / networks and auxiliary data (e.g. population, land use / land cover, socio-economic, adaptation technologies costs) which are required in order to smoothly execute the envisaged case study.
5) National training course (1 day before case study). Participants to the case study will be have the opportunity to familiarize themselves with the EU-CRICLE web-based tool and holistic resilience framework.
6) Execution of the case study, conducted for 1 day at the local organization premises, with active participation of local End Users and CI stakeholders
7) Validation by End Users. In the last part of the case study day, the participants will provide an independent evaluation of the EU-CIRCLE, according to the validation framework analysed in Task 6.1
8) Summary Report of each case study including all the activities and external experts responses.

An important aspect to decide within the analyses is the granularity of infrastructure analysis. A transport network can be either represented as an abstract and hence coarse node-edge model characterised only by a certain traffic throughputs or – on the opposite side - as a fine grained model where every component is considered in detail, e.g. each road segment with traffic lights, pavements etc.. The final selection depends:

- from the use case and the associated policy questions the end-users want to answer with the EU-CIRCLE CIRP
- the available infrastructure data.

The modelling itself will be flexible enough to facilitate different granularity levels, however, in the envisaged case studies, there seems no need for fine granular modelling and there for a rather coarse approach with lower date demand is recommended for EU-CIRCLE.

During the Consolidation Workshop in Milano, the case studies were presented and discussed. he discussions focused on the:

- Policy questions and time frames for considerations
- Meaning of “resilience” within the case study
- Data availability
- End-users involvement

In the following sections a brief overview of the case studies are presented.

4.1 Case Study 1 - Dryness and Forest fires on transport & electricity networks

Introduction: Case Study 1 involves a scenario on dryness and forest fires that impacts transport and electrical networks. The case study area in southern France covers around 31,000 km², and has a population of five million. Inhabitants. Due to the mediterranean climate, it is a fire prone area. In recent years, there have been several incidents where many dwellings lost electricity, e.g.:

- May 2005: 1 500 000
- July 2009: 1 200 000
- December 2009: 2 100 000

The case study occurs during the summer, when the population highly increases due to the presence of tourists, leading to an overloaded flux of people on the railways and highways networks. Moreover, with the presence of tourists during this high risk area period, the fire ignition propapability increases too.

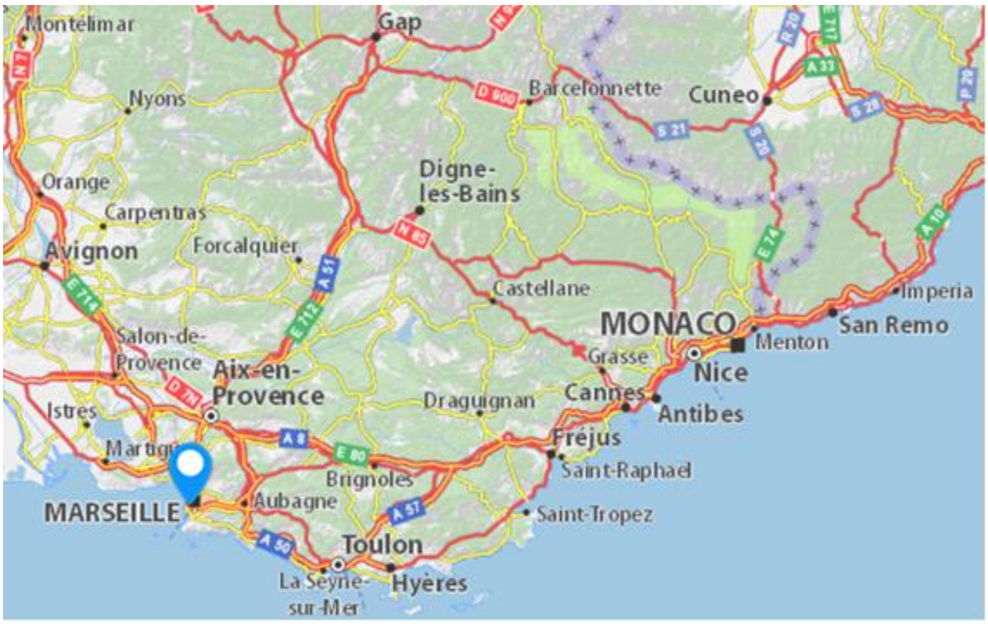


Figure 47: Area of case study 1 - Dryness and forest fire in southern France.

In order to limit the fire extension, the following measures are frequently under consideration:

- Specific plans against natural hazards, especially clearing

- Operational procedures to limit fire evolution along the railways, highways and electric networks
- Fire detection systems
- Sprinkler systems
- Conventions to cut very high voltage lines (up to 60% of 400 kV lines) in order to ensure the functioning of critical infrastructures as hospitals, nuclear plants, airport, railway, safety services
- Operational procedures for electricity network to prepare for unbalanced loads in case of line-cuts, put in operation the secondary hydroelectric power plants

The policy objective is to maintain the infrastucture activity during the event. A focus will be on prevention processes such as clearing along highway and railways networks or high voltage line to limit the power of the fire front. Another important aspect are protocols to restore to normal operatations in a safe way for public and rescue services. The case study will elaborate on the following:

- Analysis of current prevention plans, interconnections between CI, inter-services collaboration, alert systems, legacy tools
- What are the weak points of the actual organization processes?
- How can we take into accout the climate change impact in prevention plans?
- Identification and evaluation of measures to increase resilience of CI, avoid activity disruption and domino effects.

An meaningful time horizon is 20 years. Relevant key words related to resilience raised in the consolidation workshop were: save lives, save valuables and: return to service.

4.2 Case Study 2 - Baltic Sea maritime scenarios

This case study foresees two distinctive scenarios:

Oil Transport in Port: The oil piping transportation system is operating at one of the Baltic Oil Terminals that is designated for the reception from ships, the storage and sending by carriages and cars the oil products. It is also designated for receiving from carriages and cars, the storage and loading the tankers with oil products such like petrol and oil. On the basis of the piping system operation and safety statistical data coming from its operators its safety will be modelled, identified and predicted. The examination of the climate-weather change influence on the port oil transportation system safety will be performed within:

- The area in the neighbourhood of the port oil piping transportation system.
- The port oil piping system which has a length of 25 km.

The considered port oil piping transportation system and the alignment of the most important “experimental points” are shown in the following figure.

Figure 48: Port Oil Piping Transportation infrastructure - Land side (map source: maps.google.com)

Under the assumption of the increasing stress of weather influence on the operation conditions in the form of maritime storm and/or other hard sea conditions, the piping system safety will be examined and the results will be compared with safety under current conditions. The piping system safety and operation optimization will be performed and practical suggestions and procedures improving its safety will be worked out. Within the focus of the examination are the following aspects:

- piping safety structure and its parameters,
- number of piping and its components safety states,
- piping components safety states changing and
- number of piping components leaving the safety state.

Chemical Spill Due to Extreme Sea Surges: The sea transport of dangerous chemicals is pretty safe in normal environmental conditions. However, the transported goods may be swept overboard as a result of bad weather and hard sea conditions. The released chemicals may create the threat for the crew and the ship as well as pollute the seawater and the coast. The Baltic Sea and nearby ecosystems are vulnerable to pollution and contamination as a result of an accident at sea during the dangerous goods transportation. Today, one major accident at the Baltic Sea happens every year approximately. There are more than 50,000 ships entering and leaving the Baltic Sea every year and about 2,000 vessels are at the Baltic Sea at any given moment. Experiment area dimension:

- The area in the neighbourhood of the maritime ferry route.
- The approximate length of the maritime ferry sea water route is equal to 250 km.

On the basis of the statistical data coming from reports on chemical accidents at sea, the risk of dangerous chemical accidents at sea and their dangerous consequences will be modelled, identified and predicted. Under the assumption of the stress of weather influence on the operation conditions in the form of maritime storm and/or other hard sea conditions existence, the risk of chemical spills at sea will be examined and the results will be compared with the previous results. The risk of chemical spills at sea the environment degradation optimization will be performed and practical suggestions and procedures decreasing the risk of the environment degradation will be worked out. Within the focus of the examination are the following aspects:

Ferry safety states changing process data parameters:

- ferry technical system safety structure and its parameters identification
- number of ferry technical system and its components safety states and their definitions
- numbers of ferry technical system components leaving the safety state

Critical infrastructure accident consequences will be considered by realizations of three interacting and interdependent processes:

- the process of initiating events
- the process of environment threats and
- the process of environment degradation

The time horizon for the consideration are up to 100 years. Relevant key words related to resilience raised in the consolidation workshop: strength, elasticity, insight (awareness).

4.3 Case Study 3 - Coastal flooding

Torbay Borough is located in the South West of England and covers an area of approximately 62 km^{2}. The main settlements within Torbay are Torquay, Paignton and Brixham. The main economic driver for Torbay is the tourism industry which has developed around the coast line. The region has suffered flooding over many years, from different sources including surface water runoff, highway flooding, sewer flooding, main river and ordinary watercourse flooding during intense rainfall events. Coastal areas of Torbay suffer coastal flooding due to overtopping of sea defences during high tides that coincide with easterly winds. All sources of flooding in the low lying areas of Torbay are exacerbated during high tides and heavy rainfall when capacity of outfalls discharging to coastal waters are reduced.

Historically flooding events have resulted in many residential and commercial properties being flooded throughout Torbay. In addition, numerous roads are affected during the flooding incidents and the main coast road linking Torquay to Paignton and Brixham has to be closed on a regular basis due to overtopping of the sea walls. The most severe flooding event over the last 20 years occurred on the 24th October 1999 when over 200 properties were flooded, many roads had to be closed to traffic and critical infrastructure was disrupted. As Torbay relies on tourism for its economy, flooding has a very significant economic impact.

Figure 49: Area of case study 3 - Torbay borough.

Another example of damage to critical infrastructure as a result of storms was in 2013 when during a severe storm the sea wall at Livermead in Torquay was breached. As a result of this breach, the main highway linking Torquay to Paignton had to be closed and the sewage system that transfers all of Torquay's sewage to the sewage treatment works failed. Also, a high pressure gas main was damaged however failure of the main was averted by the installation of sheet piling to protect the main from further damage. If this had not been successful, all residents and businesses within a larger radius would have had to be evacuated.

As sea level rise is predicted to rise over 1 m in the next 100 years, both: frequency and impact of overtopping will increase resulting in more infrastructure and properties being affected by flooding. Also, more intense rainfall causes more surface runoff increasing localised flooding and erosion Existing drainage systems already have hydraulic capacity issues and therefore more intense rainfall will increase the flood risk from these systems. Multiple approaches for improved mitigation are in the discussion, among them:

The identification of Torbay as a critical drainage area

- Control of development within Torbay
- Sustainable drainage considered first
- Only if sustainable drainage is not viable and/or limits discharge to a watercourse, main river or sewer be considered. The discharge will be limited to the 10year greenfield run off rate for the development site.

- By implementing this control on development it will be possible to reduce flood risk

Coastal defence study

- Assess current performance criteria
- Assess future requirements for 20 years,50 years and 100 years of sea level rise

Flood alleviation schemes

- Reduce impact of climate change and resolve historic flooding problems

Local flood warnings

- Network of rain gauges and depth gauges providing automated alarms for local community
- Infoworks ICM Live hydraulic modeling could be used to provide a fast, accurate forecast of flood risk at property level. This tool can be used to provide alarms for preset flood warning triggers. Simulations would be re-run based on rainfall forecasts at between 60 and 15 minute intervals depending on the intensity of the rainfall forecast. Accuracy of this modeling can be improved using the "hindcast" period.

In the course of EU-CIRCLE case study 3, effects of climate change will be further elaborated:

Rising sea level

- Increased risk of overtopping
- Restricting outfall discharges

More intense rainfall

- Increased surface runoff
- Increasing risk of localised flooding
- Reduced hydraulic capacity of drainage systems

The following outcomes are expected from the case study:

- Identify infrastructure at risk due to climate change
- Identify future mitigation works
- Produce a plan to allow resilient development

During the consolidation workshop discussion took place with regards to the time horizon that should be used during the case study and it was agreed that three time periods should be considered in order to be adaptive. These were 20years, 50 years and 100 years.

Relevant key words/phrases related to resilience raised in the consolidation workshop were: interaction of all sources of flooding, risk acceptance criteria and building the capacity.

4.4 Case Study 4 - Rapid winter flooding

Introduction:

The Free state of Saxony is a densely populated region and has borders to Czech Republic and Poland. The City of Dresden, with a population of > 500 Thousand inhabitants is its cultural, scientific and industrial center. Many smaller cities and towns are nearby in the main development area along the valley of the river Elbe. The topography is hilly (sea level between 100 m and 1,200 m). Many water bodies from the mountains are directed to the valley of the river Elbe. In the past, there have been severe floods of the river Elbe, especially in 1845 (Mar/Apr), 2002 (Aug), 2006 (Mar/Apr), 2011 (Jan) and most recently 2013 (Jun). The GLIDE database recorded for this flood:

*"Thousands of people have been evacuated from several parts of central Europe due to heavy rainfall and consequent flooding, particularly in the Czech Republic, Germany, Switzerland and Austria. Significant **disruption to overland travel** is expected to persist as further rainfall is forecast in the coming days in the region. Further rainfall, which has been forecast across parts of the region in the coming days, is likely to exacerbate the problems caused by flooding, especially in low-lying areas. **Considerable disruption to essential services, including telecommunications and electricity**, should be anticipated in the affected areas until the weather conditions improve and any damaged infrastructure is repaired."*

For the previous flood (2002), damages and losses can be estimated as follows (Kraus, 2012):

- Casualties: 21
- Damage costs: 8,6 Billion EUR
- Damaged buildings: >25,000; 400 totally destroyed
- Damaged roads: 540 km
- Damaged social facilities: 280
- Evacuations from the city of Dresden: 35,000

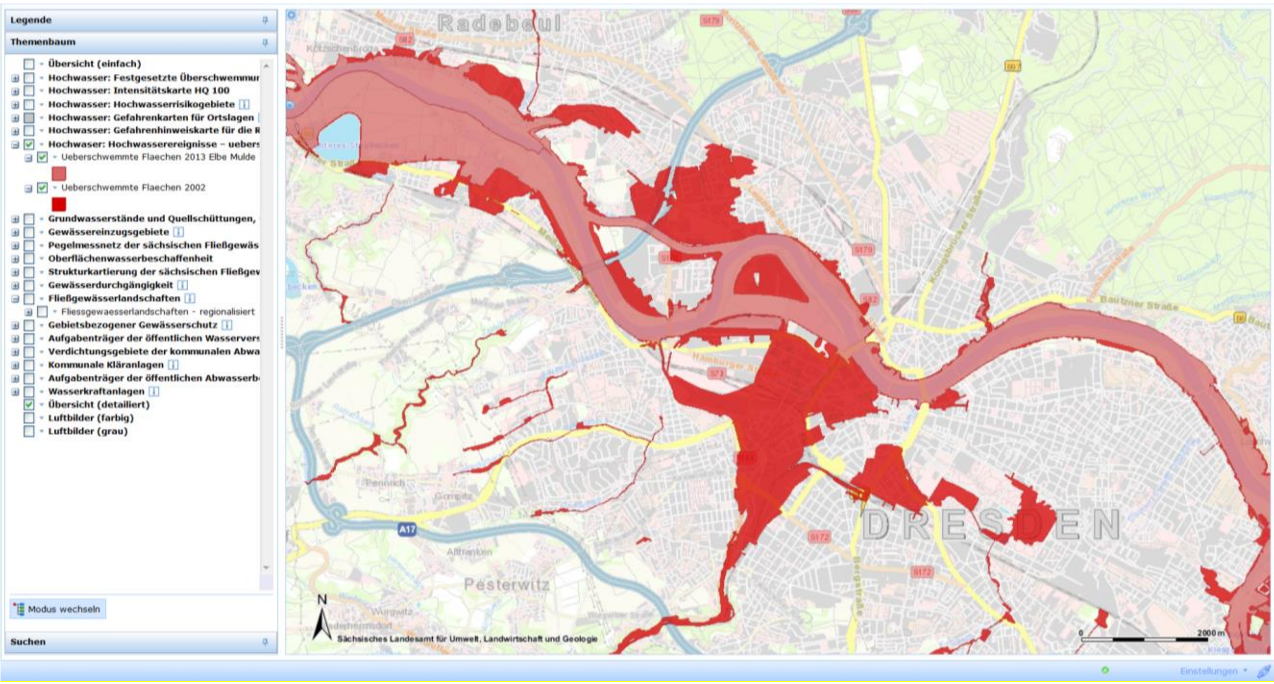


Figure 50: Flooded areas '2002 and '2013 in the City of Dresden. Source: LFULG Sachsen (http://www.umwelt.sachsen.de).

In the aftermath of the recent floods, multiple risk mitigation and adaptation measures were discussed and implemented, such as: flood barriers, new dikes and extension of existing ones, enlargement of discharging capacity of rivers, retention spaces, emergency plans, public warning and information systems and insurances.

During the consolidation workshop, the following policy questions were elicited as relevant to be analysed with EU-CIRCLE CIRP:

- What are the critical infrastructures in the affected area- which contribute to fast recovery?
- How could impacts develop spatialy (e.g. hygienic problems / epedemics as a result of dead animals)?
- What benefit does a new dike/extension of a dike provide?
  - Short term benefits:
    - lowering of evacuation efforts
    - lowering of mobility/transport limitations
  - Long term benefits:
    - agriculture: less pollution with heavy metals
    - faster reconstruction
- Where should emergency resources be placed (powergens, pumps) optimally?
- How many appliances/staff/consumables/vehicles etc. are needed in the future?
- How can cross-border/international help support crises management?
- At which level of the hazard, which area/how many people must be evacuated?
- Where should new settlements/industries be avoided?
- Predict „dimension“ of missions: How many basements must be pumped out?
- Comparisons of strategies: invest in emergency power generators vs. a new dike?
- How can river management / construction be optimized?
- Consider in all analysis different variants: What if:
  - … it rains more frequently/more intensively?
  - … multiple hazards occur simultanously?

As a time-frame for the analysis, the participants mentioned at minimum 2035. Less then 20 years would mean to react to the current situation but not to the likely upcoming developments due to the climate change. Depending on the type of CI, a time horizon of up to the year 2100 might be appropriate since the normative duration for the use of infrastructure is typically 50 years.

Relevant key words related to resilience raised in the consolidation workshop were: adapt, absorb impact and recover quickly to original state.

4.5 Case study 5 – International Case study

The international case study has two elements. One is the exploratory study phase that is targeted at learning of the case study context and the current capacity requirements and capacity development gaps in terms of critical infrastructure resilience. The other phase is the dissemination phase where learning from the EU context is disseminated at various levels as an international dissemination.

Bangladesh is highly vulnerable to climate-induced hazards and disasters and its coastal part are mostly threatened for the impacts of climate change. In broad terms **Cyclone Aila**, which hit Bangladesh in May 2009 is selected as the case study. Torrential rains from Aila resulted in 190 fatalities and at least 7,000 injuries across the **Khulna and Satkhira** Districts. Across 11 of the nation's 64 districts, approximately 600,000 thatched homes, 8,800 km (5,500 mi) of roads, 1,000 km (620 mi) of embankments, and 123,000 hectares (300,000 acres) of land were damaged or destroyed. Approximately 9.3 million people were affected by the cyclone, of which 1 million were rendered homeless. One year after the storm, 200,000 people remained homeless. Total damage amounted to 18.85 billion taka (US$269.28 million).

Figure 51: Area of case study 5.

The main focus of the critical infrastructure impacts will be concentrated within the **Khulna district** on the effect on **roads** and **water infrastructure** (most parts of the district do not have electricity, hence will not be a sector that will be considered under infrastructure), which are key to the survival and sustainability of the community. The area that is affected consists of agricultural land and is highly connected to the livelihoods of the people. Hence **roads and water infrastructure** is importantly linked to the livelihoods of people. Damage data is scatted. Some are at national lead institutes (eg. roads- Local Government Engineering Department (LGED)). The socio-economic data is collected via local government organizations. Discussions with our Bangladesh partners will enable us to determine the area of the case study impact. One of the challenges in linking the socio-economic data to the impact of Cyclone Aila is the regular occurrence of flood events in the country and linking the specific flood event to the socio-economic impact due to the event will be challenging as data is scattered and there are difficulties in linking the data that is available to the specific cyclonic event. This will be discussed further with the local stakehoders within the international case study when it commences.

The broad policy making question addressed within the case study from an EU-CIRCLE perspective is “to provide a validated framework supported by CIRP to enhance cooperation with relevant third countries, regions and international organisations to exchange practices and concepts”. CIRP will be a collaborative environment nurturing scientific and operational collaboration, thus significantly enhancing the uptake of high quality research by the relevant stakeholders with customizable outputs to be produced by CIRP.

5 Data exchange and data transformation

For the analysis, various scenario related data must be gathered, exchanged and stored. WP 3 elaborates on approaches to achieve a "smooth" translation of data between data sources and the EU-CIRCLE modelling framework. This section provides first considerations about WHICH information will be stored and exchanged and also HOW it can be exchanged and stored. In the second year of the project, a further focus will be on meta data (Task 3.6 and D3.6).

5.1 Information to be exchanged

Generally, information must be exchanged related to input data, on the analysis workflows (scenario specific parameters) and related to analysis results (e.g. probability of building damage, costs to rebuild). This comprises amongst others information about:

- Exposed objects, e.g.:
    - Population
    - infrastructure assets such as transport and electricity facilities,
    - environment
- Attributive information about these objects (e.g. IDs, names)
- Dependencies between infrastructure assets (topological information)
- Hazard information (e.g. intensitiy, frequency)
- Fragility (sensitivity of objects to hazards)
- Analysis details
    - Input definitions
    - External modules that are involved in the analysis (e.g. for specific network aspects)
    - model parameters (area of interest, time period, hazard intensity etc.)
    - output definitions

5.2 Existing standards

In the following we provide information on common standards or quasi-standards to exchange spatial data, let it be raster, vector or attributive data, structured information on analyses worflows and last but not least also on meta-data. Again, this description can not be exhaustive since the finally utilized data exchange formats depends on the case studies which are an element of the second project year.

ESRI shape-file (*.shp), a popular vector graphic format, contains information on geometry and attributive data. Optionally, it can contain some metadata and information on the projection. Each file can only contain elements of one specific geometry type (points, lines, polygons, etc.). Since it is a rather old data format, restrictions exist regarding the lenths of field names (10 characters) and maximum filesize (2 GB). However, it is well established and most GIS systems are capable to import and export data of this format.

OGC (Open Geospatial Consortium) defines common standards for exchange of spatial information via webservices. The most frequently used specifications are:

- WMS (Web Feature Service) for provision of feature-data (abstraction of any object, e.g. point, line or polygon)
- WMS (Web Mapping Service) for provision of visual presentations of geodata as maps (raster)
- WCS (Web Coverage Service) for provision of coverage files (spatial-temporal raster, points, TIN, mesh data)

OGC Geopackage is an open format for geospatial information developed initially by the US Army Engineer Research and Development Center (ERDC). Frequently described as the “shape file of the future” it is a universal file format for geodata such as vector geospatial features, tile matrix sets of imagery and raster maps at various scales as well as related metadata. From a technical perspective, it is a spatiallite database file (*.gpkg).

ASCII compliant text files: Spatial data can be stored and exchanged as simple text files. It is still very common to store raster information in text files (*.asc). In this case, the first lines of the file are dedicated to specify the geographic location of one corner, the number of columns, the number of cells and the cell width. In the subsequent lines, the raster values are stored with a simple delimiting character (typically blank). Simple text files are also used to store information points. Such files contain a minimum of three columns: one for geographic latitude, one for geographic longitude and one or more additional columns with attributive information on the point object.

INSPIRE (INfrastructure for SPatial InfoRmation in Europe) entered into force in 2007, and since 2013 addressed more then 30 different spatial data themes. Technical guidlines specify data models, handling of coordinate systems and meta data etc. It aims to ease the cross-border utilisation of basic and thematic geodata by means of harmonized formats for data storage and exchange. In more detail, the objectives of the INSPIRE initiative are to:

- document spatial data and services,
- establish more internet based services,
- facilitate access to spatial data by improving interoperability,
- arrange for public authorities to have better access to spatial data and services, and
- improve the structures and mechanisms for the coordination of spatial information. Implementation in EU members stats is progressing.

The implementation review from 2014 found a satisfactory implementation (EEA-JRC, 2014), hence INSPIRE data models might be also used within EU-CIRCLE, especially for input geodata.

XML (Extensible Markup Language) defines rules for encoding information in a way that is both: machine-readable and human-readable. XML files can be displayed and edited with any text editor. Within EU-CIRCLE, XML might be widely used for:

- spatial data (infrastructures, hazards etc.)
- analysis workflows (input, output, procedural steps, parameters etc.)

- fragilities curves for object types (sensitivity of objects to suffer from a hazard)
- fragility mapping (rules to relate fragility curves and objects)

EDXL (Emergency Data Exchange Language): a family of standards based on XML developed by the OASIS International Open Standards Consortium. Primarily for the operational message exchange between organisations involved in emergency managemet). Research projects such as IDIRA and IMPRESS have generated data in this formal that could be relevant for EU-CIRCLE case studies. Two standards appear to be closely related to EU-CIRCLE:

a) EDXL-HAVE (Hospital availability), can be used to communicate information about hospital capacities and their status (bed availability, emergency department status etc.)

b) EDXL-RM (Resource management) exchange on resources to respond to emergency incidents, such as stations, equipment, and people

ACORD (Association for Cooperative Operations Research and Development) develops a family of standards for the exchange of information relevant for insurances. Among the various standards, the ACORD P&C (property & casualty) XML standard may become of interest since it can describe in a very detailed manner property values, insurance amounts etc. (ACORD, 2016). However, due to the detailed level of information, such information is hardly available within the project EU-CIRCLE.

5.3 Data conversion

The available raw data must be adapted to the needs of the subsequent analytical steps. Typical conversions are related to:

- Coordinate reference systems
- Recalculation of units
- Modifications to data structure
- Insertion of IDs to accelerate subsequent processing
- Spatial clipping to actual area of interest
- Merging of attributive data to objects (assets)
- Topological functions
- Cleaning of unnecessary objects

Currently, at least two ways exist to pre-process the data. One approach is to use ESRI ArcGIS which provides multiple functionalities for the aforementioned challenges. Since it is a commercial product, licensing is an issue.

Another option is to use the tool SATROS (Shapefile transformation and processing tool) which has been previously developed by the EU-CIRCLE partner Fraunhofer IVI. SATROS was developed as a tool with a simple to use GUI and the possibility to save all transformation steps for later reuse. A catalogue of transformations for frequently required data schemas can be created. This gives the user the possibility to transform the data schemas and import the data straightforward into the EU-CIRCLE database, without using a complex GIS system with a complex user interface like ArcGIS.

6 Closing remarks

It is obvious, that climate change amplifies risks and creates new risks for people, infrastructure and nature. Within this deliverable, we have drafted a generic approach for holistic risk assessment which is based on scientific validated methods. In the development of our risk assessment framework we took into consideration national and international frameworks on risk assessment, risk management and resilience. Our approach is generic in the sense that it is intended to be applicable to various assessment situations; it is holistic in the sense that it includes a wide variety of direct and indirect impacts.

We have augmented the classic understanding of risk assessment and risk management with aspects of resilience and suggest a three layers' approach: In layer 1 we **assess the current climate related risks for a specific hazard to a single CI, CI network or area of interest with interconnected and interdependent CI**. Layer 2 considers **how key drivers of change may alter in the future due to climate (and socio-economic change)**. Finally, in Layer 3, we **identify climate change adaptation or risk mitigation options and define priorities**.

In order to operationalize the approach, we propose a process consisting of the following steps including:

1) Scenario development (elicitation of the scientific or policy question and on the climate hazards under consideration, e.g. their evolution of probability/likelihood)
2) Critical infrastructure network topology and description,
3) Structural and Operational analysis,
4) Network analysis, taking into account interconnectivity and resilience characteristics and
5) Holistic impact analysis

For all the steps, respectively components, we describe a potential analytical approach and foresee an implementation of these steps within a geographic information system.
This analytical approach will be implemented and demonstrated in the five case studies. An overview of the case studies has thus been presented. We will balance the need for having a common approach in all case studies with the special requirements of each case study such as data availability. We aim to apply - as far as possible – a harmonized approach in all the case studies.

The proposed approach is rather high level and leaves the required room for any adaptation necessary for each specific case study. Also, specific modelling steps may be required and will be conducted outside the EU-CIRCLE CIRP platform, for example in the case of utility infrastructures, data might be proprietary or confidential or if the model requires extensive calibration.

The forthcoming deliverable D3.5 will report in more details on specific topics, experiences of the suggested approach and describe the final approach adopted.

7 Bibliography

ACORD, 2016. *ACORD XML Business Message Specification for P&C Insurance and Surety,* s.l.: s.n.

Alderson, Carlyle & Brown, 2015. Operational Models of Infrastructure Resilience. *Risk Analysis, Vol. 35, No. 4, 2015*.

AS/NZS, 1999. *Risk Management. 4360:1999.,* s.l.: s.n.

ASME-ITI, 2005. *RAMCAP - Executive Summary,* s.l.: s.n.

Balducelli, C., Bologna, S., Di Pietro, A. & Vicoli, G., 2005. Analysing interdependencies of critical infrastructures using agent discrete event simulation. *International Journal of Emergency Management*, Volume 2 (4), pp. 306-318.

Bocchini, Frangopol, Ummenhofer & Zinke, 2014. Resilience and sustainability of civil infrastructure: toward a unified approach.. *J. Infrastruct. Syst.,* Volume 20.

Bruneau & Reinhorn, 2007. Exploring the concept of seismic resilience for acute care facilities. *Earthquake Spectra,* Volume 23(1), pp. 41-62.

Carey, C., 2016. *Quantification of multi-mode risks and impacts.* s.l., s.n.

Carreño, M., Cardona, O. & Barbat, A., 2007. Urban Seismic Risk Evaluation: A Holistic Approach. *Natural Hazards*, Volume 40 (1), pp. 137-172.

Casalicchio, E., Galli, E. & Tucci, S., 2010. Agent-based modelling of interdependent critical infrastructures. *International Journal of System of Systems Engineering*, Volume 2 (1), pp. 60-75.

Cimellaro, G. P., 2016. Urban Resilience for Emergency Response and Recovery Fundamental Concepts and Applications, Geotechnical, Geological and Earthquake Engineering, Volume 41.

Cimellaro, Reinhorn & Bruneau, 2009. Seismic resilience of a hospital system. *Structure and Infrastructure Engineering,* Volume 6(1-2), p. 127–144.

Cimellaro, Reinhorn & Bruneau, 2010. Framework for analytical quantification of disaster resilience. *Engineering Structures,* Volume 32(11), p. 3639– 3649.

CIMNE, 2013. Probabilistic Modelling of Natural Risks at the Global Level - Global Risk Model.

Coles, G. & Casson, E., 1999. Extreme value modelling of hurricane wind speeds. *Structural Safety*, Volume 20, pp. 283-296.

Criado, R. & Garcia del Amo, A., 2006. New results on computable efficiency and its stability for complex network. *Journal of Computational and Applied Mathematics*, p. 59–74.

Crichton, D., 1999. *The Risk Triangle. In 'Natural Disaster Managment '.* London, Tudor Rose.

Crichton, D., 2001. The Implications of Climate Change for the Insurance Industry..

Crowther, K. G. et al., 2004. *Assessing and managing risk of terrorism to Virginia's interdependent transportation systems.,* Charlottesville, Virginia: Center for Risk Management of Engineering Systems.

Crucitti, P., Latora, V., Marchiori, M. & Rapisarda, A., 2003. Efficiency of scale-free networks: error and attack tolerance. *Physica A 320*, p. 622–642.

Davidson, R., 1997. An Urban Earthquake Disaster Risk Index. *The John A. Blume Earthquake Engineering Center, Department of Civil Engineering, Report No. 121*.

DEFRA, 2012. *The UK Climate Change Risk Assessment 2012 - Evidence Report,* London: Department for Environment, Food and Rural Affairs.

DHS, 2010. *Energy Sector-Specific Plan. An Annex to the National Infrastructure Protection Plan.,* Washington: s.n.

DHS, 2013. *Partnering for Critical Infrastructure Security and Resilience. Homeland Security Presidential Directive 7 (HSPD-7),* Washington: s.n.

DHS, 2013. *Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach.,* s.l.: s.n.

EC, 2012. *Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP). SWD(2012) 190 final,* s.l.: s.n.

EEA-JRC, 2014. *Mid-term evaluation report on INSPIRE implementation,* Luxembourg: Publications Office of the European Union.

European Commission, 2008. *Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection,* Brussels: European Commission.
European Commission, 2010. *Commission Staff Working Document on Risk Assessment and Mapping; Guidelines for Disaster Management, SEC(2010) 1626 final.,* Brussels: s.n.
European Commission, 2013. *Europe 2020: Europe´s growth strategy,* s.l.: s.n.
European Commission, 2013. *ommission Staff Working Document - Principles and recommendations for integrating climate change adaptation considerations under the 2013-2020 European Maritime and Fisheries Fund operational programmes,* s.l.: s.n.
European Commission, 2013. *The EU Strategy on adaptation to climate change,* s.l.: s.n.
European Council, 2009. *Council conclusions on a Community framework on disaster prevention within the EU. 2979th Justice and Home Affairs Council meeting, 30.11.2009.,* Brussels: s.n.
European Council, 2011. *Council conclusions on further developing risk assessment for disaster management within the European Union, 3081st Justice and Home Affairs Council meeting, Brussels, 11.4.2011.,* Brussels: s.n.
European Council, 2014. *Commission staff working document overview of natural and man-made disaster risks in the EU, Brussels, 8.4.2014, SWD(2014) 134 final.],* Brussels: s.n.
Eusgeld, I., Nan, C. & Dietz, S., 2011. System-of-systems approach for interdependent critical infrastructures. *Reliability Engineering and System Safety*, Volume 96 (6), pp. 679-686.
Fedeski, M. & Gwilliam, J., 2007. Urban sustainability in the presence of flood and geological hazards: The development of a GIS-based vulnerability and risk assessment methodology. *Landscape and Urban Planning*, Volume 83, p. 50–61.
Frei, C. & Schär, C., 2001. Detection probability of trends in rare events: theory and application to heavy precipitation in the Alpine region.. *Journal of Climate*, Volume 14, pp. 1568-1584.
Füssel, H., 2007. Vulnerability: A generally applicable conceptual framework for climate change research. *Global Environmental Change*, Volume 17, pp. 155-197.
Ganin, et al., 2016. *Operational resilience: concepts, design and analysis. Scientific Reports 6, Article number: 19540 (2016),* s.l.: s.n.
Garcez & Almeida, d., 2014. A risk measurement tool for an underground electricity distribution system considering the consequences and uncertainties of manhole events. *Reliability Engineering & System Safety, Volume 124*, pp. 68-80.
Gardoni, P. a. M. C., 2009. Capabilities-Based Approach to Measuring the Societal Impacts of Natural and Man-Made Hazards in Risk Analysis. *Nat. Hazards Rev.*, pp. 10.1061/(ASCE)1527-6988(2009)10:2(29), 29-37.
Gas Infrastructure Europe, 2015. *Security Risk Assessment Methodology,* Brussels: GIE.
Gas Infrastructure Europe, 2016. *GIE Publications.* [Online]
Available at: http://www.gie.eu/index.php/publications/gie
Gellens, D., 2002. Combining regional approach and data extension procedure for assessing GEV distribution of extreme precipitation in Belgium. *Journal of Hydrology*, Volume 268, pp. 113-126.
Giannopoulos, G., Filippini, R. & Schimmer, M., 2012. *Risk Assessment Methodologies for Critical Infrastructure Protection. Part I,* Luxembourg: Publications Office.
Giorgi, F., 2008. Regionalization of climate change information for impact assessment and adaptation. *WMO Bulletin*, Volume 57 (2), pp. 86-92.
Goodman, J., 1983. Accuracy and efficiency of Monte Carlo method.. *Numerical methods in nuclear engineering Part 1*, p. 587.
Gumbel, E. J., 1958. *Statistics of Extremes.* New York: Columbia University Press.
Haimes, Y. et al., 2008. Risk analysis in interdependent infrastructures. *Critical Infrastructure Protection*.
HM Government, 2011. *Climate Resilient Infrastructure: Preparing for a Changing Climate,* s.l.: s.n.
House-Peters & Chang, 2011. Urban water demand modeling: Review of concepts, methods, and organizing principles. *Water Resources Research,* Volume 47 (5).

IPCC, 2014. *Climate Change 2014 Mitigation of Climate Change Working Group III Contribution to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change,* New York: s.n.
IPCC, 2014. *Climate Change 2014: Impacts, Adaptation, and Vulnerability,* s.l.: s.n.
ISDR, 2005. *Hyogo Framework for Action 2005-2015: Building the Resilience of Nations and Communities to Disasters,* Geneva: s.n.
ISO, 2009. *Risk management – Principles and guidelines. First edition of 2009.,* s.l.: s.n.
Jenkinson, A., 1955. The frequency distribution of the annual maximum (or minimum) values of meteorological elements.. *Quarterly Journal of the Royal Meteorological Society*, Volume 81, p. 58–171.
Johansson, J. & Hassel, H., 2010. An approach for modelling interdependent infrastructures in the context of vulnerability analysis. *Reliability Engineering and System Safety*, Volume 95 (12), pp. 1335-1344.
Jones, R. & Boer, R., 2003. *Assessing current climate risks Adaptation Policy Framework: A Guide for Policies to Facilitate Adaptation to Climate Change.* s.l., UNDP.
JRC, 2012. *Impacts of Climate Change on Transport: A focus on road and rail transport infrastructures.,* s.l.: s.n.
JRC, 2013. *Overview of Disaster Risks that the EU faces,* s.l.: s.n.
Kalos, M. H. & Whitlock, P., 2007. *Monte Carlo Methods.* s.l.:s.n.
Kendall, M., 1938. A New Measure of Rank Correlation. *Biometrika*, Volume 30, 1/2, pp. 81-93.
Kharin, V. & Zwiers, F., 2000. Changes in the extremes in an ensemble of transient climate simulations with a coupled atmosphere–ocean GCM. *Journal of Climate*, Volume 13, p. 3760–3788.
Kim, Y. S. B. E. A., 2008. *Seismic Loss Assessment and Mitigation for Critical Urban Infrastructure Systems.* NSEL-007 ed. s.l.:s.n.
Klaver, et al., 2008. *European Risk Assessment Methodology for Critical Infrastructures. URAM project report.,* s.l.: s.n.
Kleiner & Rajani, 1999. Using limited data to assess future need.. *Journal of AWWA*, Issue 91(7), pp. 47-62.
Kraus, 2012. *Lehren aus 2002 - Erfahrungen und Maßnahmen.* s.l., s.n.
Kumar, P., 2015. Addressing Water Security and Emergent Environmental Risks. *Water Resources Research, 51*, p. 12.
Kyriazis, Pitilakis, Kalliop & Kakderi, 2011. *Seismic risk assessment and management of lifelines, utilities, and infrastructures , 5th International Conference on Earthquake Geotechnical Engineering.* Santiago, Chile, s.n.
Markovic et al., 2016. Assessing drought and drought-related wildfire risk in Kanjiza, Serbia: the SEERISK methodology. *Natural Hazards*, Volume 80, p. 709–726.
Marulanda, M. C. et al., 2013. Probabilistic earthquake risk assessment using CAPRA: application to the city of Barcelona, Spain, ,. *Natural Hazards*, Volume 69, pp. 59-84.
McNally, R. K., Lee, S. D., Yavagal, D. & Xiang, W., 2007. Learning the critical infrastructure interdependencies through an ontology-based information system. *Environment and Planning B*, Volume vol.34, no.6, pp. 1103-1124.
Miller, Ronald & Blair, 2009. *nput-Output Analysis: Foundations and Extensions,* Cambridge: Cambridge University Press.
Mukherjee, A., Johnson, D., Jin, Y. & Kieckhafer, R., 2010. Using situational simulations to support decision making in co-dependent infrastructure systems. *International Journal of Critical Infrastructures*, Volume 6 (1), pp. 52-72.
National Coordinator for Security and Counterterrorism, 2009. *Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of the Netherlands,* s.l.: Ministry of Security and Justice.
Nicola, V., Shahabuddin, P. & Nakayama, M., 2001. “Techniques for fast simulation of models of highly dependable systems. *IEEE Transactions on Reliability*, Volume 50, pp. 246-264.
Nogaj, M., Parey, S. & Dacunha-Castelle, D., 2007. Non-stationary extreme models and a climatic application.. *Nonlinear Processes in Geophysics*, Volume 14, pp. 305-316.
OECD, 2014. *Recommendations of the council on the governance of critical risks.* Paris: s.n.
Ouyang & Dueñas-Osorio, 2012. Time-dependent resilience assessment and improvement of urban infrastructure systems. *Chaos Interdiscip. J. Nonlinear Sci.,* Volume 22.

Ouyang & Wang, 2015. Resilience assessment of interdependent infrastructure systems: with a focus on joint restoration modeling and analysis.. *Reliab. Eng. Syst. Saf.,* Volume 141, p. 74–82.
Oyang, M., 2014. Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering - System Safety*, January, pp. 43-60.
Oyang, M. et al., 2009. A methodological approach to analyze vulnerability of interdependent infrastructuresy. *Simulation Modeling Practice and Theory*, pp. 817-828.
Pant, R., Barker, K., Grant, F. & Landers, T., 2011. Interdependent impacts of inoperability at multi-modal transportation container terminals. *Transportation Research Part E - Logistics and Transportation Review*, Volume 47 (5), pp. 722-737.
Panzieri, S., Setola, R. & Ulivi, G., 2005. *An approach to model complex interdependent infrastructures.* s.l., s.n.
Papathoma-Koehle et al., 2016. A common methodology for risk assessment and mapping for south-east Europe: an application for heat wave risk in Romania. *Natural Hazards*, Volume 82, pp. 89-109.
Pederson, Dudenhoeffer, Hartley & Permann, 2006. *Critical Infrastucture Interdependency Modelling - A Survey of US and International Research,* s.l.: s.n.
Penning-Rowsell, Johnson, Tunstall & al., e., 2003. *The benefits of flood and coastal defence: techniques and data for 2003,* Middlesex: Flood Hazard Research Centre, Middlesex University, UK.
Perimann, R., 2007. *Genetic algorithms for agent-based infrastructure interdependency modelling and analysis.* s.l., s.n.
Porter, Kiremidjian & LeGrue, 2001. Assembly–based vulnerability of buildings and its use in performance evaluation. *Earthquake Spectra,* Volume 17(2), p. 291–312.
Rinaldi et al., 2001. *Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies'. IEEE Control Systems Magazine 21, no. 6 (December 2001): 11–25.,* s.l.: s.n.
Rinaldi, S., 2004. *'Modeling and Simulating Critical Infrastructures and Their Interdependencies', 8 pp. IEEE,* s.l.: s.n.
Rootzen, H. & Katz, R., 2013. Design Life Level: Quantifying risk in a changing climate. *Water Resour. Res.*, Volume 49.
Sandmann, W., 2007. Rare Event Simulation Methodologies and Applications. *Simulation*, 12, Volume 83, pp. 809-810.
Satta, A. et al., 2016. An index-based method to assess risks of climate-related hazards in coastal zones: The case of Tetouan,. *Estuarine, Coastal and Shelf Science*, Volume 175, pp. 93-105.
Schwierz, C. et al., 2010. Modelling European winter wind storm losses in current and future climate. *Climatic Change*, Volume 101, p. 485–514.
Shamir & Howard, 1979. An analytical approach to scheduling pipe replacement. *J. Am. WaterWorks Assoc. 28(3)*, p. 159–161.
Shand, T. et al., 2015. *Methods for probabilistic coastal erosion hazard assessment. Australasian Coasts & Ports Conference 2015: 22nd Australasian Coastal and Ocean Engineering Conference and the 15th Australasian Port and Harbour Conference. Auckland, New Zealand.* s.l., s.n.
Simmonds, W., Whittaker, P. & Harrison, R., 2010. *Security Risk Register: User Guide.,* s.l.: s.n.
Sultana, S. & Chen, Z., 2009. Modeling flood induced interdependencies among hydroelectricity generating infrastructures. *Journal of Environmental Management*, Volume 90 (11), pp. 3272-3282.
Theocharidou, M. & Giannopoulos, G., 2015. *Risk assessment methodologies for critical infrastructure protection. Part II: A new approach.,* Brussels: European Commission.
TSO, 2012. *UK Climate Change Risk Assessment: Government Report,* s.l.: s.n.
U.S. DoE, 2010. *DOE O 413.3B, Program and Project Management for the Acquisition of Capital Assets,* Washington, DC: s.n.
UN, 2013. *Climate Change Impacts and Adaptation for International Transport Networks. ExpertGroup Report.,* New York and Geneva: UN Economic Commission for Europe.
UNISDR, 1994. *Yokohama Strategy and Plan of Action for a Safer World: guidelines for natural disaster prevention, preparedness and mitigation,* New York: United Nations - Headquarters (UN).
UNISDR, 2015. *Global assessment report on disaster risk reduction 2015,* s.l.: s.n.

UNISDR, 2015. *Sendai Framework for Disaster Risk Reduction 2015-2030,* Geneva: s.n.
Utne, I., 2010. A method for risk modeling of interdependencies in critical infrastructures.. *Reliability Engineering and System Safety.*.
Utne, I. et al., 2008. *Risk and Vulnerability Analysis of Critical Infrastructures – The DECRIS Approach,,* s.l.: s.n.
Villagrán de León, J., 2004. Manual para la estimacióncuantitativa de riesgos asociadosa diversas aramzenas. *Guatemala: Acción Contra el Hambre*.
Walshaw, D., 2000. Modelling extreme wind speeds in regions prone to hurricanes. *Applied Statistics*, Volume 49, pp. 51-62.
Wennersten, Sun, Q. & Li, H., 2015. The future potential for Carbon Capture and Storage in climate change mitigation – an overview from perspectives of technology, economy and risk. *Journal of Cleaner Production, Volume 103*, pp. 724-736.
Wisener, B., P., B. & Cannon T., D. I., 2003. *At Risk: natural hazards, people's vulnerability and disasters, Second edition.* s.l., s.n.
WMO, 2009. *Guidelines on Analysis of extremes in a changing climate in support of informed decisions for adaptation,* Geneva: s.n.
Yong Ge, X. X. Q. C., 2010. Simulation and analysis of infrastructure interdependencies using a petri net simulation in a geographical information system. *International Journal of Applied Earth Observation and Geoinformation*, pp. 319-430.
Yusta, M., Correa, G. & Lacal-Arantegui, R., 2011. Methodologies and applications for critical infrastructure protection: State-of-the-art. *Energy Policy 39*.
Zhang, P. & Peeta, S., 2011. A generalized modeling framework to analyze interdependencies among infrastructure systems. *Transportation Research Part B: Methodological*, Issue 45 (3), pp. 553-579.
Zimmerman, R., 2001. Social implications of infrastructure network interactions. *Journal of Urban Technology*, Volume 8, p. 97–119.
Zimmerman, R., 2004. *Decision-making and the vulnerability of interdependent critical infrastructure.* s.l., s.n.

Annex 1. CI Safety Assessment – Analytical Process

In the multistate safety analysis to define the system with degrading components, we assume that:

– n is the number of the system components,
– E_i, $i = 1,2,...,n$, are components of a system,
– all components and a system under consideration have the safety state set $\{0,1,...,z\}$, $z \geq 1$,
– the safety states are ordered, the safety state 0 is the worst and the safety state z is the best,
– $T_i(u)$, $i = 1,2,...,n$, are independent random variables representing the lifetimes of components E_i in the safety state subset $\{u,u+1,...,z\}$, while they were in the safety state z at the moment $t = 0$,
– $T(u)$ is a random variable representing the lifetime of a system in the safety state subset $\{u,u+1,...,z\}$ while it was in the safety state z at the moment $t = 0$,
– the system states degrades with time t,
– $s_i(t)$ is a component E_i safety state at the moment t, $t \in (0,\infty)$, given that it was in the safety state z at the moment $t = 0$,
– $s(t)$ is a system S safety state at the moment t, $t \in (0,\infty)$, given that it was in the safety state z at the moment $t = 0$.

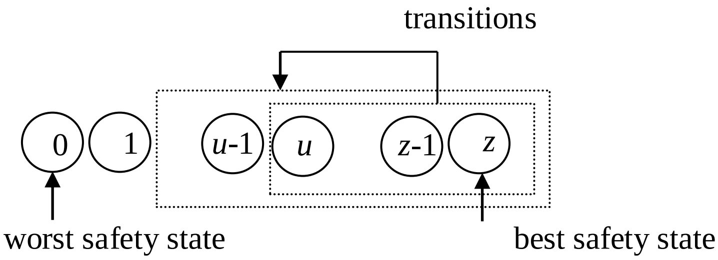


Figure 52. Illustration of a system and components safety states changing

Thus, we assumed that the critical infrastructure is compoced of n *ageing* components/assets E_i, $i = 1,2,...,n$, assuming during time t, $t \in (0,+\infty)$, the safety states from the set of all possible ordered safety states $\{0,1,,,...,z\}$ and we denoted the component E_i, of a critical infrastructure unconditional lifetime in the safety state subset $\{u, u+1,..., z\}$ by $T_i(u)$.

After that, we define the basic critical infrastructure component safety indices:

- **the critical infrastructure component safety function** by the vector

$$S_i(t,\cdot) = [S_i(t,0)=1, S_i(t,1),...,S_i(t,z)],\ t \in (0,+\infty),\ i = 1,2,...,n$$

where

$$S_i(t,u) = P(s_i(t) \geq u \mid s_i(0) = z) = P(T_i(u) > t),\ t \in (0,+\infty),\ u = 0,1,...,z;$$

- **the mean lifetime of the component E_i in the safety state subset** $\{u, u+1,..., z\}$

$$\mu_i(u) = \int_0^\infty S_i(t,u)dt,\ u = 1,2,...,z,\quad i=1,2,...,n,$$

- **the standard deviation of the component E_i lifetime in the safety state subset** $\{u, u+1,..., z\}$

$$\sigma_i(u) = \sqrt{n_i(u) - [\mu_i(u)]^2},\ u = 1,2,...,z,\ i = 1,2,...,n,$$

where $n_i(u) = 2\int_0^\infty t S_i(t,u)dt$, $u = 1,2,...,z$, $i = 1,2,...,n$;

- the intensity of ageing of the critical infrastructure component E_i/the intensity of critical infrastructure component E_i departure from the safety state subset $\{u, u+1,..., z\}$

$\lambda_i(t,\cdot)$ = [$\lambda_i(t,0)$ =0, $\lambda_i(t,1)$, …, $\lambda_i(t,z)$], $t \in (0,+\infty)$, $i = 1,2,...,n$,

that in case the components have the exponential safety functions, i.e.

$S_i(t,u) = \exp[-\lambda_i(u)t]$, $t \in (0,+\infty)$, $\lambda_i(u) \geq 0$, $i = 1,2,...,n$, $u = 1,2,…,z$,

takes form

$\lambda_i(t,\cdot)$ = [0, $\lambda_i(1)$, …, $\lambda_i(z)$], $t \in (0,+\infty)$, $i = 1,2,...,n$.

We denote the critical infrastructure unconditional lifetime in the safety state subset $\{u, u+1,..., z\}$ by $T(u)$ and define **the critical infrastructure safety function (CISI1)** by the vector

$\boldsymbol{S}(t,\cdot)$ = [1, $\boldsymbol{S}(t,1)$, ..., $\boldsymbol{S}(t,z)$],

with the coordinates defined by

$\boldsymbol{S}(t,u) = P(T(u) > t)$ for $t \in < 0, \infty)$, $u = 1,2,..., z$.

The exemplary graph of a five-state (z = 4) critical infrastructure safety function $\boldsymbol{S}(t,\cdot)$ = [1, $\boldsymbol{S}(t,1)$, $\boldsymbol{S}(t,2)$, $\boldsymbol{S}(t,3)$, $\boldsymbol{S}(t,4)$], $t \in (0,\infty)$, is shown in Figure 53

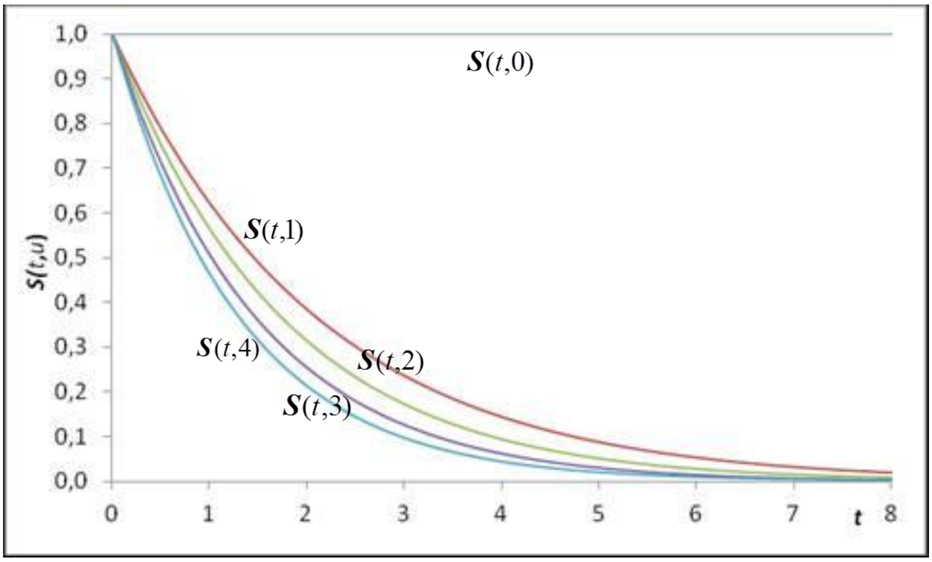


Figure 53. The graphs of a four-state critical infrastructure safety function $\boldsymbol{S}(t,\cdot)$ coordinates

- the critical Infrastructure mean lifetime $T(r)$ **up to exceeding critical safety state** r given by

$\mu_b(r) = \int_0^\infty [\boldsymbol{S}(t,r)]dt$, $b = 1,2,...,\nu$,

where $\boldsymbol{S}(t,r)$ is the coordinate of the critical infrastructure unconditional safety function for certain risk level;

- the standard deviation of the critical infrastructure lifetime $T(r)$ **up to the exceeding the critical safety state** r given by

$\sigma(r) = \sqrt{n(r) - [\mu(r)]^2}$,

where $n(r) = 2\int_0^\infty t\, \boldsymbol{S}(t,r)dt$,

- the moment τ of exceeding acceptable value of critical infrastructure risk function level δ given by $\tau = \boldsymbol{r}^{-1}(\delta)$,

where $\boldsymbol{r}^{-1}(t)$, if it exists, is the inverse function of the risk function $\boldsymbol{r}(t)$ given by (3.37);

- the intensity of ageing of the critical infrastructure, the intensity of critical infrastructure departure from the safety state subset $\{u, u+1, ..., z\}$ **(CISI7)**

$\lambda(t,\cdot)$ = [$\lambda(t,0)$ =0, $\lambda(t,1)$, …, $\lambda_i(t,z)$], $t \in <0,+\infty)$, $i = 1,2,...,n$,

that in case the critical infrastructure have the exponential safety functions, i.e.

$\boldsymbol{S}(t,r) = \exp[-\lambda(u)t]$, $t \in <0,+\infty)$, $\lambda(u) \geq 0$, $i = 1,2,...,n$, $u = 1,2,\ldots,z$,

takes form

$\lambda(t,\cdot)$ = [0 , $\lambda(1)$, …, $\lambda(z)$], $t \in <0,+\infty)$, $i = 1,2,...,n$.

Annex 2. EU-CIRCLE processing of categorical variables

In order to combine different consequence categories, or uncertainty estimates at a categorical level, different approaches can be applied :

- **Mode**: We assign a total impact level equal to the category level that occurs most often in the analysis.
- **Maximum**: This can be thought of as the most "precautious" ("risk-fearing") total impact assessment method since it attributes the highest observed risk rating among all categorical categories to the total impact.
- **Median**: This method calculates the Median value of the categories impact ratings as the value standing in the middle of the impact ratings when we sort them by their impact severity.
- **Weighted Mean**: This is the most flexible method of total assessment and is due to the fact that we can apply weights (0-100% with a sum of 100%) to each categorical category based on their relative significance, map their individual impact rating to ordered numbers and sum them to calculate their weighted mean
- **Majority Rule**: This rule implies that the final metric is estimated as the class that appears the most times within a predefined number of alternatives.
- **At least k times**: This rule is used to define a final class if the corresponding class appears at least k times in the predefined number of alternatives. This rule is considered very useful in the definition of critical events.

Having estimated the impact and likelihood of each risk we can then assess the overall risk contained within a specific network, network of networks or area of effect.. This means that once again the different risk levels need to be mapped to numbers before making the actual calculations and consequently be reverted back to a risk level when a single number is extract by means of rounding to the closest integer representing that level. The methods used to extract that single number are the following:

- **Average risk estimation**: Overall line, network or region risk estimation can be achieved by averaging out the risk estimations for each separate asset and deriving the mean value.
- **Weighted risk calculation**: In an attempt to better calibrate the above proposed method we can apply weights to each of the assets based on their importance or amount of people they serve. The weights are then used to calculate a weighted mean value.

Differences in the two methodologies:

The average risk estimation method can be used in cases where no supplementary information is available or no distinctions need to be made among assets. When this doesn't stand true we can use the weighted risk calculation to fine-tune the estimation to better represent the magnitude of the actual risk. With the above methodology in mind we can calculate the risk found in parts of each CI network, in area selections (using GIS data) or the overall network of networks. In the particular case of the network of networks we can extract our final estimation based on partial estimations from each individual network by re-applying the above methodologies.