Identification and analysis of most vulnerable infrastructure in respect to floods

D 2.1 - Deliverable for Task 2.1

Date: **18 January 2013**

Report Number: **WP2-01-12-04**
Version Number: 1_2_05

Deliverable Number: D01
Due Date for Deliverable: 31/05/12
Actual Submission date: 18/01/13
Task Leader: Damien Serre

FloodProBE is co-funded by the European Community Seventh Framework Programme for European Research and Technological Development (2009-2013)
FloodProBE addresses "Technologies for Improved Safety of the Built Environment in Relation to Flood Events"
Start date: November 2009, duration: 4 Years

Document Dissemination Level PP

PU = **Public**

PP = **Restricted to other programme participants (including the Commission Services).**

RE = **Restricted to a group specified by the consortium (including the Commission Services).**

CO = **Confidential, only for members of the consortium (including the Commission Services).**

CL restricted = **Classified with the mention of the classification level restricted "Restraint UE"**

CL confidential = **Classified with the mention of the classification level confidential "Confidential UE"**

CL secret = **Classified with the mention of the classification level secret "Secret UE"**

Document Information

Title	**Identification and analysis of most vulnerable infrastructure in respect to floods**
Lead Author	Kristina Heilemann
Contributors	Elise Balmand, Serge Lhomme, Karin de Bruijn, Linmei Nie, Damien Serre
Distribution	FloodProBE Consortium
Report Number	1

Document History

Date	Version	Prepared by	Organisation	Approved by	Notes
31/05/2012	1_0_Pn	Kristina Heilemann, etc	SINTEF, EIVP, Deltares		First complete version, harmonising and correction are required
16/07/ 2012	Updated	Linmei Nie, etc	SINTEF, EIVP, Deltares		Updated based on vers. 1.
31/10/2012	Updated	Linmei Nie, etc	SINTEF, EIVP, Deltares		Updated based on 1st round reviewing comments
18/01/2013	Updated	Linmei Nie, etc	SINTEF, EIVP, Deltares		Updated based on 2nd reviewing comments

Acknowledgement

The work described in this publication was supported by the European Community's Seventh Framework Programme through the grant to the budget of the FloodProBE project, Grant Agreement Number 243401.

Disclaimer

Summary

The report presents the work which has been done in the frame of Task 2.1 of the FloodProBE project, which focuses on the vulnerability assessment of critical infrastructure in urban areas with respect to floods.

The work suggests a stepwise approach, from basic assessment to advanced modelling. This approach is oriented towards the stakeholders in charge of critical infrastructure and flood vulnerability in urban areas. The focus is on Critical Infrastructure (CI). The following definition has been adopted: critical infrastructure stands for the infrastructure which is essential for the functioning of society, whose failure would seriously affect many people. The selected approach aims to build guidance on vulnerability assessment on the role of critical infrastructure during flood events. Unlike other types of assessment, the vulnerability assessment incorporates the possible secondary and indirect effects through a well-organised pattern of analysis in three steps: network analysis, analysis of the resistance and resilience of the network elements, and analysis of the effects of element failure on the network. In addition to accounting for secondary effects, the focus of the methodology is on highlighting the interdependency between the infrastructures.

The innovative framework for vulnerability assessment of the various CI consists in four steps which match respectively with four totally different approaches of the flood event. It goes from step 1, a coarse overview, to step 4, the most sophisticated analysis. In case that all the steps are performed, the final result is a thorough insight in the CI, and its vulnerability towards flooding of the area under assessment. The four steps can be defined as following:

- Basic analysis, gathering the stakeholders, first collection of information
- Risk assessment performed on various infrastructures
- Urban flood simulation and risk mapping
- Advanced analysis, FMEA (Failure Modes and Effects Analysis)

Within the frame of FloodProBE, steps 2 and 4 have been tackled, because they are the most important steps to meet the gap in the existing tools. The first tool developed allows fulfilling step 2 (Risk assessment performed on various infrastructures). It consists in a coarse analysis which results in the generation of risk matrices. These matrices are easy handy tools which support the discussion and the decision process for the stakeholders. This first tool only requires basic knowledge of the area under investigation and can be performed by users from different backgrounds. The second tool (step 4) is the most sophisticated one of the suggested stepwise methodology. It is a modelling tool based on Analysis of Failure Modes and Effects Analysis (FMEA). It enables the study of the interdependency between networks subsequently to a disaster. The tool shows how a simple disruption of one network can generate breakdowns on other networks through cascade effects. The output is a failure map of the assessed area, which identifies the most critical sectors. The tool is developed based on GIS analysis.

Contents

Tables

Figures

1 Introduction

1.1 Background and context

Efficient, affordable and reliable systems of communication, power supply and waste management provide the foundations for economic and social development. The target is to ensure that these are accessible to the entire community at all times. Every day millions of people in Europe and elsewhere benefit from the development of a highly sophisticated network of essential infrastructure systems to sustain their communities. Responding to the pace and economics of modern life, the system is expected to work without failure and the level of tolerance towards traffic jams, delays in the railway system and power supply breakdowns becomes lower.

Natural disasters, such as flooding, can cause the failure of entire lifelines in a city or larger area. Even if the flooding is of minor scale it can cause severe damage to infrastructure and critical buildings in which the network control units are located. To implement the right protection measures, communities have to understand the risks from flooding.

Numerous flood hazard, flood vulnerability and flood risk assessments methods exist that produce maps which show the likelihood of flooding from rivers and the sea, the corresponding impacts and risks. However, most of these analyses and maps do not assess the vulnerability of critical infrastructure networks and buildings.

In 2006 the European Commission proposed the EU floods directive in order to reduce and manage the risks that floods pose to human health, the environment, cultural heritage and economic activity. All member states were forced to carry out a "preliminary assessment" to identify flood prone areas close to rivers and coastal areas. In 2013 flood risk maps should be ready. Many tools have been developed to make such maps. An overview of guidelines is provided in "Handbook on good practice for flood mapping in Europe" (EXCIMAP, 2007).

As a next step, the EU Floods directive requires to establish flood risk management plans focused on prevention, protection and preparedness by 2015. These plans require more information than hazards and vulnerability alone: the combined risk is also needed and measures to cope with or reduce risks. Despite the broad variety of tools already existing, there is, up to now, no defined methodology which would be applicable to any area, and which would provide a complete overview of flood risks. Especially, the flood impacts on critical infrastructure are rarely incorporated (Serre et al, 2012).

1.2 Aim

As depicted in the FloodProBE Description of Work report, approved by the European Commission in October 2009, the final title for the present Task 2.1 is "Identification and analysis of most vulnerable infrastructure in respect to floods".

The "most vulnerable infrastructure" is further qualified by the term "critical infrastructure". A special chapter is dedicated to the definition of such a concept. The practical aim of Task 2.1 is therefore *to provide guidance for flood vulnerability assessment of critical infrastructure*.

The **guidance** consists of a framework with methods for vulnerability assessments on different levels of detail. They go from an indicative inventory of hazards and risks for different critical infrastructure types based on expert judgement, to methods for detailed vulnerability analysis including the interdependency of critical infrastructures.

Critical infrastructure (CI), in the present report, stands for the infrastructure which is essential for the functioning of society, and for which the damage would seriously affect many people. The scope of this CI definition includes utility networks, transport networks and (tele) communication networks. This definition is discussed in detail in Chapter 2.

Flood vulnerability is understood as the possibility of negative effects (e.g: harm/damage/casualties) caused directly or indirectly by floods.

The present framework for the risk assessment of CI is meant to support local governments doing risk analysis, but also consultants or researchers studying flood impacts. The framework was developed to fill a gap in flood risk assessment methods, namely the vulnerability assessment of critical infrastructure and their interdependencies.

1.3 Approach

The approach was to develop new elements or new methods based on existing methods and work towards a generic framework.

Concrete actions included literature review, development of tools, and implementation of both fictitious and real case studies. The work was carried out by SINTEF, EIVP and Deltares. HR Wallingford has given comments on the report.

2 Critical infrastructure

2.1 Critical infrastructure (CI) – the definition

Many definitions of Critical Infrastructures (CIs) were found (e.g. Fekete, 2001; Moteff & Parfomak, 2004; Fulmer, 2009; McBain et al. 2010). For example, “Canada’s critical infrastructure consists of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Canadians or the effective functioning of governments in Canada” (Gordon & Dion, 2008). Although no generic definition was found, most definitions are comparable with the Canadian one.

In addition to the definition, the explicit scope of CIs is also important. Most authors identify the following compounds as CIs: electricity networks, water supply and drainage networks, communication related infrastructure, and roads. Some authors also include schools and hospitals, monuments, banks, financial institutes, nuclear power plants, gas supply, or sanitation. Which elements are included depends on the scale (national or regional), the type of hazard considered (terrorists, cyber viruses, natural hazards or others) and the aim of the CI analysis executer. From a national perspective, the focus generally lies on nuclear installations, gas winning, and other sectors of national importance. From a regional perspective, electricity, water supply and wastewater drainage systems, and communication systems, are the most commonly accounted for when considering CIs.

In this report, the focus is on vulnerability of the critical infrastructure to flooding. In the frame of this work, critical infrastructure is defined as follows:

Critical infrastructure includes all networks and buildings that are essential for the functioning of society during the flood event and for the recovery from the flood event. Critical infrastructure is considered ‘critical’ because an outage of the infrastructure has a serious effect on many people over a long period. Criticality can thus be expressed by (Mc Bain et al., 2010);

- the severity of the effect (number of fatalities/wounded or monetary damage),
- the extent of the area or the number of people affected
- the rate of recovery from the outage.

Typically, the following list of CIs is used as a basis for assessment:

- Utility services (electricity, water supply and drainage systems, transportation, telecommunication and gas supply, etc),
- Welfare and social systems (e.g. food distribution centres, financial centres, etc),
- Administrative and emergency service buildings (e.g. fire stations, police stations, flood warning and forecasting office, etc)

Flood protective structures such as embankments are not included in the list, which will be studied in the work package of flood defence rather than critical infrastructures.

Other vulnerable assets such as buildings or shelters are studied in Task 2.2 and WP4 of the project.

2.2 CI Impact assessment

2.2.1 Differences with "common vulnerability assessments"

Vulnerability assessments or damage assessments of CI differ from general damage assessments (De Bruijn et al., in prep.). Whereas general vulnerability assessments focus on direct economic damage and generally only mention possible indirect effects, **criticality assessments** aim at assessing the indirect and secondary effects of infrastructure impairment. Direct damages to the infrastructure itself are of minor importance compared to the indirect effects of their outage. The indirect effects, such as loss of income due to an electricity outage, loss of lives in hospitals due to communication interruptions, broken roads or electricity service interruptions are more relevant than damage to the cables and transformation stations themselves.

Furthermore, when assessing CI, the secondary effects of outage outside the flooded area and interdependencies and cascading effects to other sectors are relevant (see section 2.3). Failure of e.g. the power grid, may affect a wide range of other infrastructures, e.g. water supply and information technology. Vulnerability assessments need to determine the consequences and damages of such interdependencies. For getting a full picture of failure, it is thus necessary to capture second and third order consequences both inside and outside the flooded area (Fekete, 2011).

Since the CIs are different from one land to another, the vulnerability assessment methods are usually different. The methods are discussed in the next sections.

2.2.2 Steps in vulnerability assessment of CI

To assess the flood vulnerability of the CI in a certain city or region, there is first the need to make a rough inventory of the CI and the flood hazards. This can be made by experts and/or municipalities. For those regions were floods may occur and CI may be vulnerable to flooding, more detailed analyses can be carried out (see chapter 3).

The vulnerability analysis of CI involves the following five steps (De Bruijn, 2012.):

1. Network analysis
2. Analysis of the resistance and resilience of the network elements
3. Analysis of the effects of element failure on the network (resilience of network, redundancy)
4. Effect of failure of the network on other networks: interdependency
5. Effects of failure of the networks and the corresponding costs.

Network analysis

First, the CI network in question must be analysed. The nodes (e.g. transformator stations, transformator cabinets etc. in the case of electricity) and connections (electricity cables in the case of electricity) and their links must be identified. Furthermore, the structure can be analysed e.g. with the help of indicators such as redundancy (Lhomme et. al, 2010).

Analysis of the flood resistance and resistance of CI

Flood resistance is defined here as the water depth, velocity and duration of inundation for which the considered infrastructure can withstand without any damage or failure. A CI is *resilient* if, when it comes into contact with floodwater during floods, no permanent damage is caused, structural integrity is maintained and, if operational disruption does occur, normal operation can resume rapidly after the flood has receded. In this second step, for each element and connection of the CI network in question, it should be determined at what water depths, flow velocity or other flood conditions, damage or interruption may occur and how fast recovery of the service is expected after the flood recession.

Analysis of the effect of element failure on the network

In the third step, the effect of failure on the vulnerable elements and connections for the functioning of the network in question is studied.

Analysis of the effect of failure of a (part of one) network on other networks

In the fourth step, the relationship between networks is considered. The clearest relationships are those between electricity supply and other CI. If electricity fails, pumps, communication, traffic control systems and most of the infrastructure will not function, unless they have their own power supply. However, electricity is not the only infrastructure leading to important impacts on other networks: for example, failure of communication services and roads may also strongly affect the other networks.

Effect of disruption on society

Finally, the effect of the failure of networks on society needs to be assessed. This may be done in quantitative terms, such as lost income in euros. However, because this is often very difficult, indicators such as the duration of outage, the area, the number of people affected and combinations of those may be very informative.

The steps can be carried out at different levels of detail: first screening can be done in order to determine for which CI the flood risk may be relevant. Discussion with the municipalities is a good

starting point. If flood risk is found to be relevant, the analysis may be repeated on a more detailed level to determine the scope, data availability and adequacy of existing information and flood risk.

2.3 Interdependencies between critical infrastructure networks

Most critical infrastructure systems interact through direct connectivity, policies and procedures, or geospatial proximity. These interactions often create complex relationships, dependencies, and interdependencies that cross infrastructure boundaries. The modelling and analysis of interdependencies between critical infrastructure elements is a relatively new and very important field of study (Pederson et al., 2006). It illustrates common representations of infrastructures based on the scenario of a flooding event and the subsequent response. There are ties and dependencies within each infrastructure and between the different sectors. The solid lines in crossing sectors and connecting nodes represent internal dependencies, while the dashed lines represent dependencies that also exist between different infrastructures (infrastructure interdependencies).

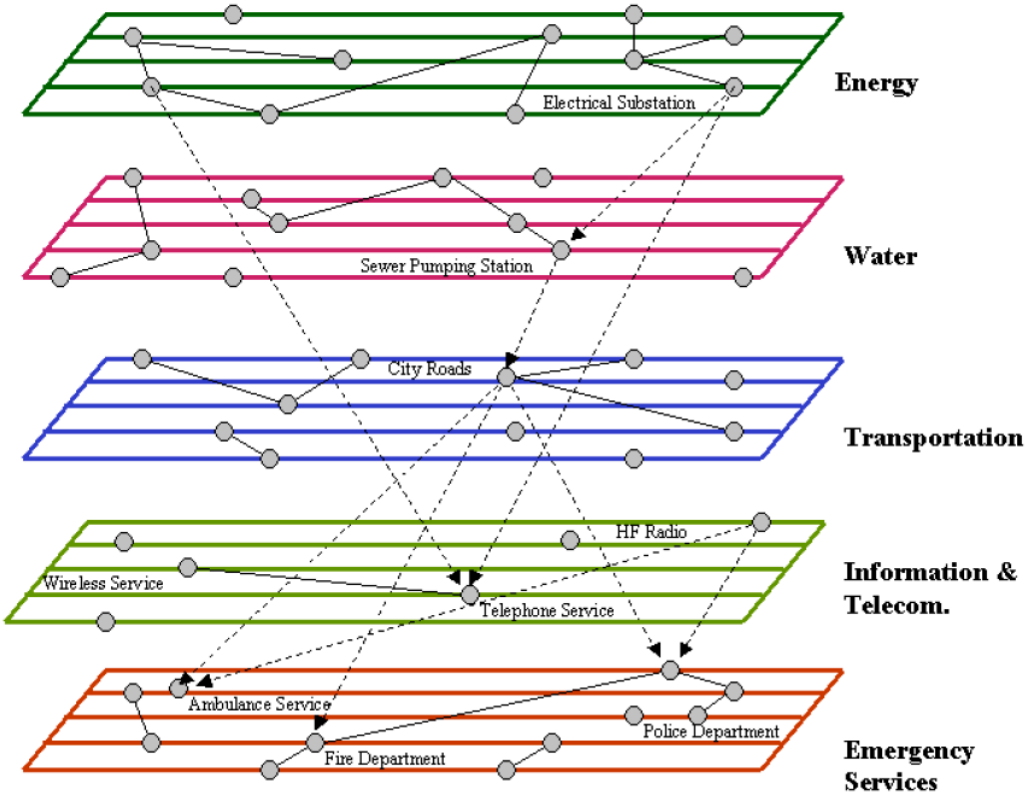


Figure 1 Critical infrastructure interdependency modelling (Pederson et al., 2006)

In order to better understand the importance of critical infrastructure interdependencies and the different issues concerning these interdependencies, an analysis is led based on documents available in the literature.

The cascading effect

The failure of one CI may cause disruption in others. For instance, the utility of traffic control in a municipality is generally provided by a system of three CIs - power grid, telecommunication network, and traffic control boxes. However, the proper functioning of the three CI system components is only a necessary condition for the normal operation of the traffic control system. It alone is not sufficient. The configurations under which the three CI components are bonded together, the nature and magnitude of their bonding (positive and/or negative feed- backs, for example), and the self-regulating mechanisms (power back-ups and surge protections, for example) are all emergent features that are essential to the normal operation of the traffic control system, but which do not exist when the three CI system components are separated (McNally et al, 2007).

The chaos and disorder that overtook New Orleans in the wake of Hurricane Katrina (August 2005) can provide an idea of what a worst-case scenario may look like. Fortunately, CI breakdowns are not necessarily accompanied by the deadly mayhem witnessed in New Orleans. While some breakdowns have cascading effects and can cause great harm, most of them remain isolated events which are quickly remedied (Boin & McConnell, 2007).

Critical infrastructure: a system of systems

CI can be considered as complex systems and complex systems can be defined as follows: ‘‘Traditionally, a system is said to be complex if its attributes are commonly out of the norm, as compared with other systems. Complex systems are characterized by having a large number of dimensions, nonlinear or nonexistent models, strong interactions, unknown or inherently random plant parameters, time delays in the dynamical structure, etc.’’ (Jamshidi, 1983). Additional characteristics of complex systems are an adaptive emergent behavior and feedback loops.

CIs can be seen as a so-called ‘‘system-of-systems’’. ‘A system-of-systems (SoS) consists of “multiple, heterogeneous, distributed, occasionally independently operating systems embedded in networks at multiple levels, which evolve over time’’ (DeLaurentis, 2003). Alternatively, system-of-systems can be defined using the term ‘‘complex systems’’: ‘‘Systems–of-systems are large scale concurrent and distributed systems that are comprised of complex systems’’ (Kotov, 1997). The questions are: how to deal with the complexity? How to model such systems?

Consequently, it is important to draw distinctions between two related but different concepts - a CI system, and a system of CIs. A CI system is an assemblage of functional objects that provides a certain essential good or service. A power supply system, for example, provides electrical service through the synergistic interactions among its components - the power plant, substations, transformers, and transmission and distribution lines. At the same time, a CI system is also a part of an even larger system - a system of CIs, which offers a range of public goods and services through the collaborative operations of, or interdependencies among, its individual CI system components. The behaviour of a system of CIs, as a manifestation of the usually complex interdependencies, cannot be fully described and understood by the behaviours of its CI system components (Rinaldi et al, 2001).

Interdependencies typology

The main dimensions which must be analyzed in order to study interdependency are (Rinaldi, 2004): the technical, economic, business, social/political, legal/regulatory, public policy, health and safety, and security.

Interdependent infrastructures also display a wide range of spatial, temporal, operational, and organizational characteristics, which can affect their ability to adapt to changing system conditions.

The following sections present a short description of various kinds of interdependencies as described by different authors: Input; Mutual; Cyber; Physical; Geographic; logical.

Input: A system requires input from another system. For instance, critical infrastructure systems require information to be able to perform the functions related to process control and management. In case of a failure of the underlying infrastructure (system under control), the operability of the complete system is compromised. The term dependency can be used to describe these unidirectional relationships.

Mutual: At least one of the operations of any infrastructure is dependent upon each of the other infrastructures. This type is given, when two or more systems, where the output of each system is an input to other systems, are discussed. For example, this is the case for a power plant using coal, itself being transported by trains which require power from the plant in order to operate.

Cyber: An infrastructure has cyber interdependency if its state depends on information transmitted through the information infrastructure. The computerization widespread use of supervisory control and data acquisition of modern (SCADA) systems have led to pervasive cyber interdependencies. The state of critical infrastructures is significantly affected by the transmission of information.

Physical: Infrastructures are linked through material output(s). Thus 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.

Geographic: 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: 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. Policy, legal, or regulatory regimes can give rise to logical linkage among infrastructures.

2.4 Methodology used in order to model interdependencies

To understand the cascading failures among infrastructure systems under random incidents, manmade attacks and natural hazards, many researchers have proposed different *methods* for modeling and simulation of interdependent infrastructure systems. These models and methods can broadly be divided into two categories.

The first category corresponds to predictive approaches. Predictive approaches aim at modeling and/or simulating the behavior of a set of interconnected infrastructures in order to, for example, investigate how disturbances cascade between the systems. A wide range of different perspectives and ways of representing the systems of interest exist, including for example Agent Based Methods (ABM), Inoperability Input- output Methods (IIM), System Dynamics Methods (SDM), Network or Graph Based Methods (NBM) and Data Driven Methods (DDM).

In the ***Agent Based Method***, agents represent components in an infrastructure system (such as electric transformers or generators) or some important players (such as government or weather) related to system operation. This method can analyze system responses to different attack scenarios, such as Aspen (name of the agent based model) assessing the impacts of sudden changes or shocks to the economy.

The System Dynamics (SD) approach studies interdependent complex systems by using feedback loops, stocks, and flows. Feedback loops indicate connections and directions of effects between system objects, while stocks represent quantities or states of the system, the levels of which are controlled over time by flow rates between stocks. An SD-based model called Critical Infrastructure Protection Decision Support System (CIPDSS) allows for rapid production of scenarios to compare different types of disruptive events and their impacts across multiple infrastructure systems.

The network or graph based method, which uses nodes to represent different types of system components and links to mimic the physical and relational connections among them, provides affordable and intuitive system representations along with detailed descriptions of their topology and flow patterns. This method can analyze the effects of system topology, element physical fragility, and attack intensity on system performance levels which are measured by connectivity and flow delivery.

The data driven methods, which characterize infrastructure system failure interdependencies based on the data from media and official reports (e.g. post assessments of the events), can complement probabilistic, systems-based and simulation methods and provide empirical understanding on how extreme events within and/or external to one infrastructure system lead to the failures in other infrastructure systems.

Apart from the above methods, there are still some other ***hybrid approaches*** for interdependency studies, such as system-of-systems approaches which can capture the complexities of the interdependencies and model the impacts of human factors, or multilayer infrastructure network approach which can capture the interdependencies among various infrastructure systems with disparate physical and operational characteristics.

The appropriateness of using one model or the other in a predictive vulnerability analysis clearly depends on the purpose and perspective of the analysis.

The second category corresponds to empirical approaches. Empirical approaches aim at studying past events in order to increase the understanding of infrastructure dependencies. Furthermore, the purpose is to identify patterns of interest to policy and decision-making, such as how often failures cascade between infrastructures and patterns related to the extent the society is affected by infrastructure failures caused by interdependencies.

The two categories of approach (predictive and empirical) are complementary, when used as input to risk and vulnerability analyses or as a basis for decisions regarding prevention or mitigation. The predictive approaches can provide important information of the particular systems of interest and facilitate the implementation of a proactive approach to risk management and critical infrastructure protection. The empirical approaches, on the other hand, can provide important information regarding general patterns of infrastructure interdependencies and how failures cascade between different types of systems. Empirical studies are thus very important for the general understanding of infrastructure interdependencies and can provide input both to the predictive models as well as to decision-making and policy.

2.5 Conclusion

For a critical infrastructure, getting dysfunctional is a phenomenon that transcends by far the failure of any, even major, single component. The often incomprehensible cause of system crash stems from the inherent features of the critical infrastructures: they are multicomponent systems, prone to cooperative behavior, and typically responding in a non-linear fashion to stimuli and perturbations. There is an urgent need for appropriate and credible solutions to address such systems in the areas of vulnerability and risk assessment, as a substantial, and indeed critical, component of the contemporary policy making. The challenges for understanding, characterizing and modeling these systems are immense, and the current efforts in this field are still in an early stage. The existing methods and models address the same issue, the impact of interdependencies, but from different viewpoints. In fact, the main issue concerning these methodologies is that they are not exhaustive. Indeed, empirical approaches and predictive approaches are generally not combined in the best way.

3 Framework for Risk Assessment for CI in Respect to Flood

3.1 Introduction to the framework

To offer guidance for the flood vulnerability analysis of critical infrastructure, SINTEF, Norway, EIVP, France, and Deltares, Netherlands developed a framework and two methodologies in strong collaboration with the pilot areas Trondheim, Orleans and Dordrecht (Nie et al, 2011; Lhomme, et

al 2012). This section discusses the framework. The methodologies are described in the following sections.

In the case of flooding it is essential for the functioning of the society to know where the weak points in urban infrastructure networks are. This knowledge is essential for flood risk management and mitigation measures. Some municipalities and other local governments are already well prepared and have a running flood risk management plan; others have not even started with a dialogue between the many people and institutions which are responsible in the case of flood events. The stepwise approach provides a guide for risk assessment from a basic to an advanced assessment process.

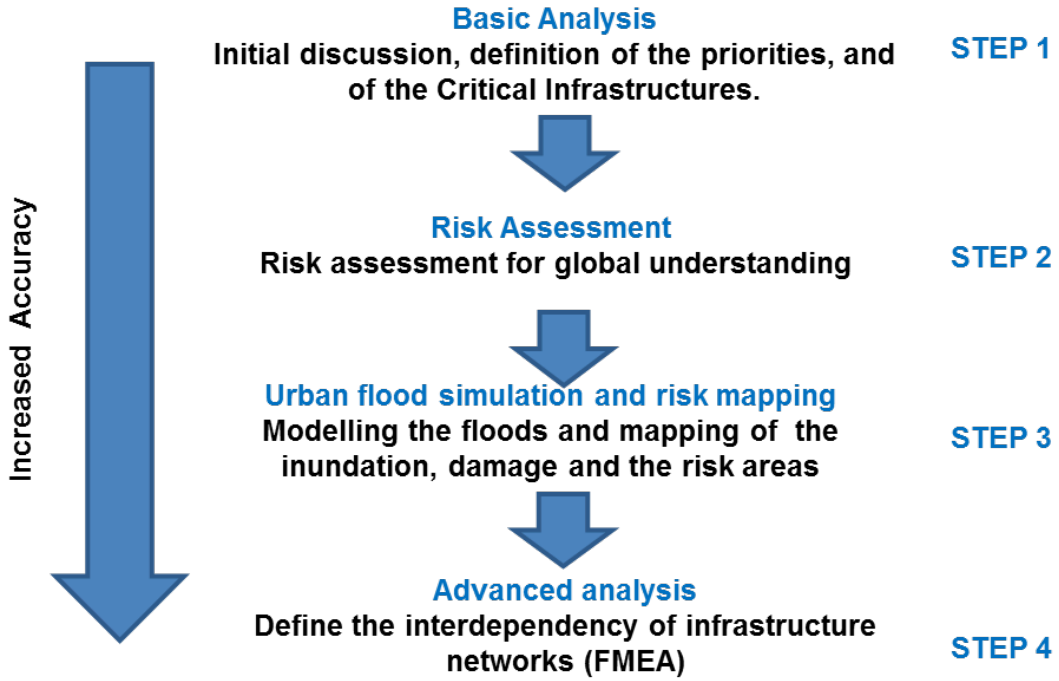


Figure 2 Framework for risk assessment (Lhomme et al 2012)

Starting with simple, generic risk analyses such as the ROS analysis which all municipalities in Norway conduct by now, continuing with a computer based tool showing the weakest infrastructure asset in a municipality (see section 3.2), including existing urban flood simulation and risk mapping (see section 3.3) and concluding with GIS based numerical model and risk mapping (see section 3.4) provides the framework support in the entire assessment process. The first two general approaches increase the awareness of those who are the driving forces for flood risk management and mitigation. Step three, the flood risk mapping, actually the "classical" risk assessment methodology until today, is an essential input for step 4 which shows the interdependencies between critical infrastructures, the weak nodes in the system and sub-system, and the cascading effects.

All four steps can be run independently. Which steps are required depends on the aim of the user and of the outcomes of the first steps. However, if the first steps show that there are CIs at risk from flooding, the latter two steps are needed to provide a full picture of the flood risks for CIs. Step 1 is not further depicted in this report. It is an essential and crucial part (see Part 4), and its success mainly depends on the good will of the stakeholders.

3.2 Step 2: Risk assessment

3.2.1 Risk assessment in Norway

The existing risk assessment tool in Norway supports authorities and infrastructure owners with a quick identification of people, property, buildings and critical infrastructure which are at risk from flooding or other hazardous events.

Vulnerability analyses have been traditionally carried out using empirical methods based on damage vulnerability matrices *(Kappos et al. 1998).* For decades, Probabilistic Safety Analyses (PSA) and Quantitative Risk Analyses (QRV) have been implemented in the safety management of nuclear power plants and in other industrial branches. These analyses, which were conducted by special consultancy companies, required the knowledge of experts and were therefore rather cost-intensive. The public sector and small and medium enterprises were mostly not able to afford such comprehensive analyses. Therefore, a much simpler risk and vulnerability analysis was developed in early nineties in Norway under the acronym ROS ("Risiko- og Sårbahetsanalyse") *(Utne et. Al, 2008).* Based on the initiative of the Directorate for Civil Protection and Emergency Planning the ROS analyses was conducted during the last decade in numerous municipalities in Norway and is today a part of the Norwegian planning and building act.

The purpose of a ROS-analysis is to avoid the risk for harm and loss of life, health, environment, important infrastructure and property and to increase the reliability for the society and area planning processes *(Norwegian Ministry of Environment).* The analyses can be carried out during a planning process, during the construction process or for the evaluation of the risk for existing infrastructure. The analysis supports the taking into account of hazards in the planning process of CI.

The method starts with expert interviews to identify undesired events, their likelihood and the consequences in the case of an incident. These are discussed and registered in a risk matrix. The analysis then provides a first risk picture on a coarse scale. In most cases, more detailed standard risk analyses and model-based risk analyses have to follow. The method is a reliable mapping tool providing an overview about possible causes of risk.

In Norway, risk analyses have been carried out in several municipalities according to the guideline for "risk and vulnerability analyses" (ROS in Norwegian) made by the Directorate for Civil Protection and Emergency Planning (DSB in Norwegian) (DSB, 1994). However, expert-based estimation of potential risks can provide only qualitative results which, in many occasions, are insufficient to support making decision for adaptation and mitigation. Vatn (2007) developed a computing tool - InfraRisk for risk and vulnerability assessment for natural disasters at macro level. Improving and adjusting the tool were made for urban flooding risk analysis (Nie et al., 2009) and is set as a starting point of the present work.

3.2.2 Case study in Trondheim

The Trondheim Municipality is situated in central Norway beside the Trondheim Fjord, in the county of Trøndelag. With around 170.00 inhabitants, Trondheim is the third biggest city of Norway after Oslo and Bergen. Trondheim is exposed to three different sources of flood risk:

- Flooding from the river Nidelva

  Starting from the lake Hyttfossen, just below the largest lake Selbusjøen in South-Trøndelag, the river Nidelva runs about 40 km before it reaches the city centre of Trondheim and discharges into the Trondheim fjord. The catchment area is 3.178 km^2. Six hydroelectric power plants are located along the river. Due to the regulation of the hydropower plants, the maximal discharge has been reduced significantly. However, the occurrence of large flood events should be analysed (NVE, 2001).

- Flooding from the sea during storm events

  Gale-force storms and spring-tides increase the sea-level up to 50 cm in the Trondheim Fjord, which influences the water level in the river Nidelva due to backflow.

- Flooding of urban drainage systems

  The sewer system in Trondheim consists of about 50% combined system built before 1965, 40% separate system and 10% non-active separate system. About 100 combined sewer overflow incidents (reported) pollute the river and the sea during heavy rain and snow melt. On many places in Trondheim, the existing sewer drainage system is not designed for the increased peak runoff discharge caused by climate change and urbanization. The insufficient capacity of the existing sewer system leads often to flooding during intense precipitation events.

Nie et al (2010) carried out a case study of risk and vulnerability assessment for urban flooding in the city of Trondheim, Norway. That report gives more information of the above mentioned different types of floods. The analysis showed that advanced tools are required in order to take into account diverse risk scenarios, the critical infrastructure networks and their interdependence. A sufficient standardised framework assessing the risk and vulnerability of the most critical infrastructures and their interdependencies does not exist by now in Norway and in the rest of Europe. However the municipalities, which are obliged to take measures for "adaptation to climate change", are in need for guidelines in order to handle the topic on a satisfying way.

3.2.3 Methodology of the risk analysis tool of step 2

Based on existing methodology and software tools for risk and vulnerability assessment in Norway (see previous section), a computer based analysis tool has been developed focused on the flood hazard. Vulnerability is calculated as regards to people, environment, and infrastructure (water network, transportation, electricity network, telecommunications). The purpose of the program is to obtain a general overview of the risk associated to different flood scenarios that can harm a defined location. The inputs required are general knowledge and data about the hazards that can threaten a specific geological region. The outputs are presented as several matrices that can be compared to each other, and that allow visualizing the risk events for which action shall be taken.

Risk

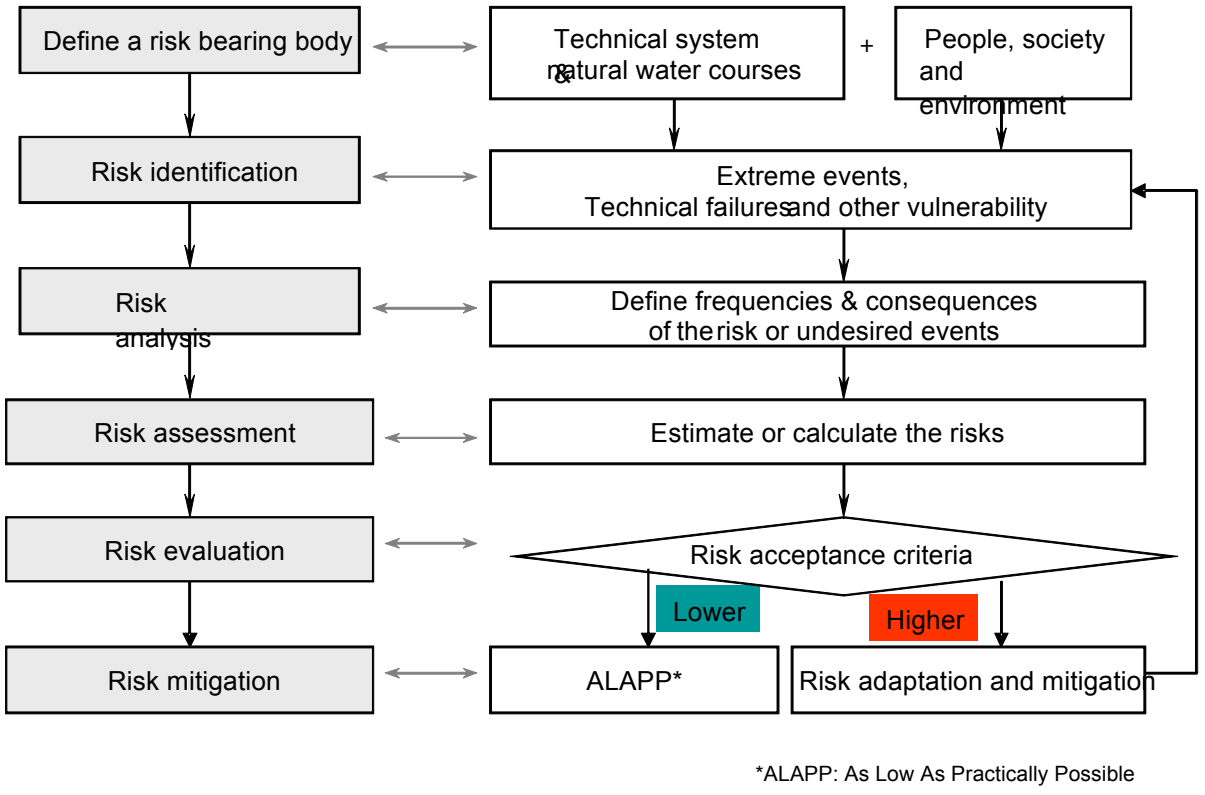
Risk is determined by the frequencies and potential consequences of undesired events. A complete risk analysis should be able to answer the following questions:

1. What are the potential risk events?
2. What are the root causes of these events and contributing factors, i.e. why do they happen and the development chains?
3. How often do they happen?
4. What are the potential consequences?
5. How high are the potential risks?
6. How to mitigate the potential risks?

To assess the risk of a vulnerable body (e.g. a specified object or system), the following four steps should be included:

1. Identify hazardous events and undesired technical defects (also called barriers);
2. Perform frequency and consequence analysis;
3. Assess the potential risks;
4. Evaluate the risk according to the selected risk acceptance criteria, and then planning for adaptation and mitigation measures

Based on risk assessment process, Nie et al. (2009) proposed an approach for risk and vulnerability assessment (Figure 3).



*ALAPP: As Low As Practically Possible

Figure 3 A procedure for risk and vulnerability assessment and mitigation (Nie *et al*, 2009)

Types of data (input/output)

According to the analytical procedures illustrated in Figure 3, the starting point for risk analysis framework is the identification of undesired natural events, in that case floods due to extreme events like intensive precipitation, snow melting, storm surges and higher sea level, insufficient capacities, technical failure events like breaking of dams and water pipes, breakdown of pumping stations due to flood inundation and failure in distribution of electric power. Interdependency of different infrastructure networks and their components, social management capability and collaboration of stakeholders and individuals on floods should be weighed. Thus the following data ought to be collected in order to carry out risk and vulnerability assessment.

Main and basic events

Floods are induced by either meteorological or oceanic extreme events or by combinations of extreme events with poor geological conditions or technical failures in the natural or constructed drainage systems (e.g. dam break or failure in operation of the drainage system components). From this point of view, floods are defined as main events, while other contributing factors such as external extreme natural events or undesired incidents or technical failures are considered as basic events (Figure 4). According to the logic relations of “causes” and “consequences”, risk identification can be carried out by two analytical approaches: Fault –tree is a Top- Down method starting from flood events and proceeding to identify prerequisite conditions and root causes; while Event-tree is a Bottom-Up method starting from the basic events to find out failure modes (Nie, 2004).

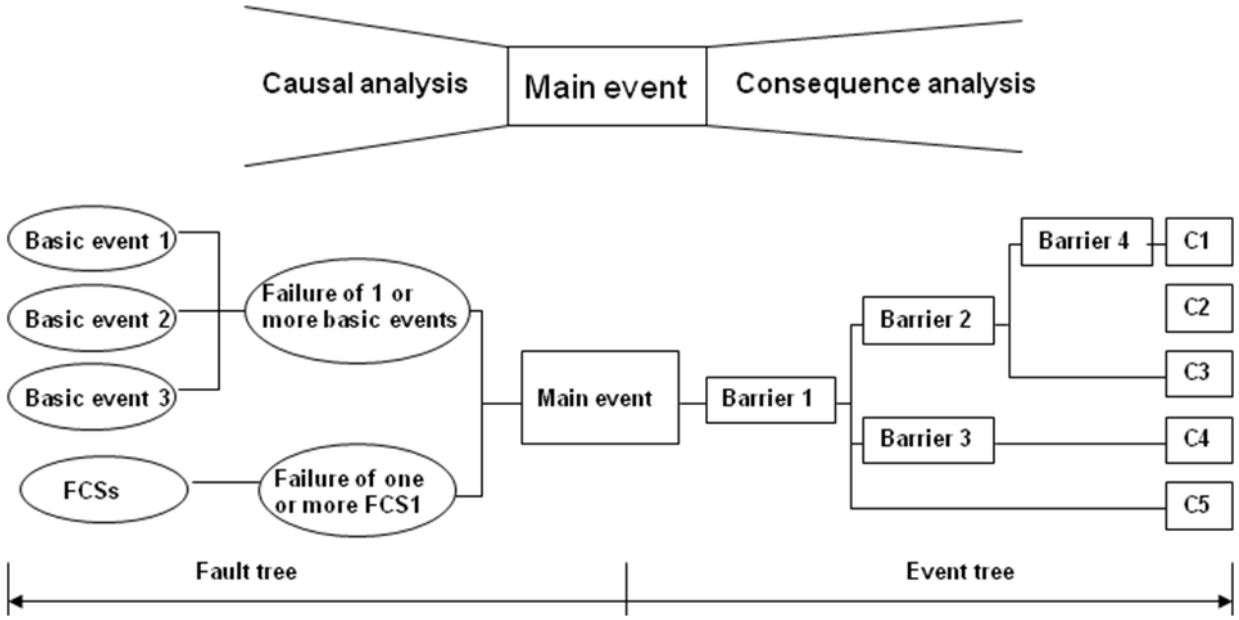


Figure 4 A model of event tree based risk analysis (Nie, 2004)

In addition to the main events, functions of the critical infrastructure, community manageability and behaviour of individuals and their dependency on critical functions will affect the occurrence of

hazardous events and consequences. Any failure in one or more of the infrastructure components, like electric power, telecommunication and transportation system, water drainage system or flood forecasting system or deliver the required service may cause flooding and a chain of failures of the social systems and severe consequences due to floods. In few accidental occasions, flood inundation happened without a drop of rain, e.g. water trunk explosion because of high pressure in the pipes. A terminology of Social Critical Functions (SCFs) is introduced to represent the dependency of flood events with functioning of critical infrastructure and social management networks (Vatn, 2007). Table 1 illustrates how to weigh the impacts of SCFs in compliance to the main events.

Table 1 Relation between the SCFs and the main events

Code	Description	Relation
I100*	Loss of the SCF is the cause for the main event	SCF < before> the main event
B100*	The SCF acts as a complete barrier	
R90*	The SCF is very important for the main event	SCF <before and after> the main event
R60	The SCF is important for the main event	
R40	The SCF is medium import for the main event	
R15	The SCF is not very important for the main event	
R05	The SCF is less important for the main event	
V90*	The SCF is very vulnerable with respect to the main event.	SCF < affected> by the main event
V60	The SCF is vulnerable with respect to the main event	
V40	The SCF is medium vulnerable with respect to the main event	
V15	The SCF is not very vulnerable with respect to the main event	
V05	The SCF is less vulnerable with respect to the main event	

* I, B, R and V represent the relation between the SCFs and the main events, I – initial (cause) to the main event; B – barrier; R – relation of SCF to main event; V – vulnerable degree of the SCFs versus the main events.

Vulnerability influence factors

Vulnerability influence factors (VIFs), unlike SCFs, are a range of factors representing the local environment, which are relevant to the main events. Such vulnerability factors are typically including dimension of the area, geographical location, population density, climate type, time and duration of occurrence of the main events, and preparedness to cope with emergency. These VIFs are important when assessing the consequences of the main events. In the risk assessment, each VIF is measured at five levels from minor to huge according to the influence on consequences of the main events. In addition, the terms of “before”, “before and after” or “after” are used to express the time of occurrence of VIFs in relation to the main events.

Frequency analysis

The frequency is used to describe the occurrence of a hazardous event. For floods induced by extreme weather events, the frequency is usually expressed in terms of return periods, e.g. once in

n years or n times per year; for other flood origins such as technical failures, the frequency of failure is often expressed in terms of expected number of occurrences per year.

To estimate the frequency of urban flooding, it is important to distinguish and integrate the frequency of flooding in rivers which are usually protected by flooding with return periods of 1 time in 100-1000 years or even rarer, and flooding from urban drainage systems which are designed to have capacity to store or drain storm water with return periods equal or rarer than once in 100 years (usually 1 in 10-50 years). According to the Norwegian standards for sewers and rivers (NS-EN, 1998; NVE, 2008), Table 2 represents frequencies for urban pluvial and fluvial flooding.

Table 2 Frequency of urban flooding (NS-EN, 1998; NVE, 2008)

Likelihood	**Return period** **(1 in n in years)**	**Examples of consequences and vulnerabilities**
Rare	Rarer than 1 in 1000 years	People's lives and health are in danger, property downstream may be flushed away or severe economic damages occur. However, hospital buildings and emergency institutions should stay safely for flooding of 1000 years.
Unlikely	Rarer than 1 in 100 years	Buildings, free time-, and farm buildings, industry/ business offices, schools and infrastructures etc. should be safe for 200 years flood.
Occasional	Once in 50 years	Buildings or basements in residential areas, city centres, garages and factory workshops, entrances for underground buildings, shopping and subways may be affected by flooding from sewers. Combined sewer overflow (CSO).
Likely	Once per 1-10 years	Flooding may occur in areas with lower potential for damage (suburb and agricultural areas); Basement flooding or CSO.
Almost certain	Once or several times per year	Basement flooding or CSO due to technical failure.

To model the occurrence of the main event in a chain of dependency of joint events, one can use the Fault Tree Analysis. The functions of calculation consist of three statements of the basic events: "AndGate", "OrGate" and "KooNGate", where the statements have the same meaning as in statistics. The AndGate statement is used when each input to the gate has to occur in order to ensure that the gate occurs. The OrGate statement is used when it is sufficient that one or more of the inputs has to occur in order to ensure the gate to occur. The KooNGate statement is used when the occurrence of K or more out of N inputs ensures the gate to occur.

Consequences analysis

Consequences are adverse results of hazardous or undesired events, which are usually divided into direct and indirect consequences, and are estimated according to tangible monetary damage,

or intangible impacts to people, environment and community manageability as a whole. Examples of typical flood consequences are given in (Table 3).

Table 3 Classification of consequences

Consequences	Tangible damage (may be measured by monetary values)		Intangible loss (difficult to be measured by monetary values)	
	Public sector	**Private sector**	**Public sector**	**Private sector**
Direct	Damage of infrastructure (roads, bridges, dams, pumping stations and other utilities); cost of rescue materials; cost of repairing Cost of lost products, land crops and livestock; cost for medicines and public health care.	Damage of private, commercial, industrial buildings, contents and land products. Cost of cleaning, replacing, repairing the damage articles; cost for healing and medicine care.	Disruption for normal community activities, esp. transportation, power and communication. Pollution of environment; Loss or damage of cultural heritage items or sites	Loss of lives; Health problems or psychological stress caused by current flood.
Indirect	Cost of temporary evacuation and relocation; Cost of post-flood proofing (planning, service and purchasing and storing materials)	Cost of temporary evacuation and relocation; Increasing cost for transportation and communication. Cost of post-flood proofing Loss of income and production losses	Planning, preparing and training teams for emergency actions	Reluctance to inhabit in flood-prone areas, thereby riverine property values going down some amount; Psychological stress caused by possible future floods.

The consequences can be ranked, e.g. in five levels from insignificant to catastrophic (Table 4); or can be expressed by probability (i.e. a number between 0 and 1). The statistic statements of And-, OR- and KooNGate are applicable to calculate the severity of consequences of dependent events.

Assessment of the risks found

The objective of risk and vulnerability assessment is to evaluate the level of the risk, and further, to take appropriate action. Such an objective can be achieved by comparing the calculated risk with a selected risk acceptance criterion (Table 4).

Table 4 Classification and ranking of severity of flood consequences

Rating of consequences	Consequences on			
	Public safety	**Community and infrastructure**	**Property damage**	**Environment**
Insignificant	Appearance of a threat but no actual harm or damage	Minor areas were unable to maintain its current services.	Minor damage on business and private properties.	No environmental damage
Minor	Minor or no injuries, or property damage	Isolated but noticeable cases of decline in service	Minor loss of industrial, commercial goods and materials, and minor damage on business and private properties.	Minor environmental damage.
Critical	Limited number of injuries or accidental loss of lives.	Operation of basic infrastructure (power, water supply and sewage, road and communication systems) is out of function temporarily during or right after the flood event.	Loss of industrial, commercial goods and materials, and some damage on business and private properties.	Isolated but significant instances of environmental damage.
Major	Limited number of lost lives and some serious injuries. Limited number for evacuation.	Operation of basic infrastructure (power, water supply and sewage, road and communication systems) is out of function during or after the flood event for long period.	Little damage on public facilities for social and security and health service, significant damage on important industry or business workshops, domestic and free time buildings, and significant loss of industrial, commercial goods and materials, and private properties.	pollution on environment (surface, receiving waters, or other public areas)
Catastrophic	Limited number of loss of lives or large number of serious injuries.	Basic infrastructure (power, water supply and sewage, road and communication systems are seriously damaged or out of operation).	Serious damage on public facilities for social and security service such as hospitals, schools and emergency buildings and on industrial and private buildings and properties.	Serious pollution on environment (surface, receiving waters), high potential of prevailing disease.

3.2.4 Technical description of the tool

The purpose of the program is to obtain a general overview of the risks associated with the different flood scenarios that can harm a defined location. The input only requires general knowledge about the hazards that can threaten a specific area. The output is presented as several matrices that can be compared to each other, and that allow visualizing the events for which action shall be taken. The program is conveniently based on the Excel spread sheet.

A first sheet allows the user to describe the critical situation under assessment. The input data can be divided into two components:

- Definition of the nature of the triggering events and of their gravity
- Definition of the specific vulnerability associated to the area

For the first component, the program proposes a list of 13 events:

- Natural events: rain, snow melting, wind, exceptional discharge, tsunami, landslide;
- Technical disorders: insufficient sewer capacity, blocked sewer, pumping station out of work, wrong connection between private and public sewer, water pipe breaking, dam break

The user is invited to attribute a frequency of occurrence to each of these 13 events. The entered frequency is estimated by the user himself from his knowledge about the place under assessment. The value of the frequency (inverse of the return period) is directly linked to the gravity of the event: the biggest the return period, the strongest the gravity. Note that the attribution of a "0" value to the frequency/return period is equivalent to not take into account a given event in the generation of scenarios, assuming that this particular event is not relevant for the selected area.

The second component of the input data, defining the specific vulnerability of the location/moment, is then entered. The program distinguishes between 6 different categories, which represent as many perspectives for the calculation of the risks:

- People
- Environment
- Infrastructure:
    - Water network
    - Transportation
    - Electricity
    - Telecommunications.

For each of these 6 categories, the vulnerability is defined by checking the relevant cases.

Once all these parameters are entered, the calculation can be run by clicking on the button "calculate risks". The calculated values of risk are visible in another sheet which presents:

- The explicit name of all the generated scenarios
- The reference number attributed to each of the scenarios (and further used in the matrices)
- The exact calculated values for risks and the so-called real consequences.

The calculated value for risks is a relative value. This means that this value cannot be translated directly in a unit such as euros for example. The risk values are intern to the program, allowing scaling the various generated scenarios, and further locating them into the risk matrix.

The program automatically generates:

- All the single events, with the frequency selected by the user
- Joint events, which are all the couples of 2 events which can be created, based on the input data defined by the user

The matrices show the relation between probability and consequence of each of the scenarios in a visual way, using colourful cells, in accordance to the following scheme (Figure 5):

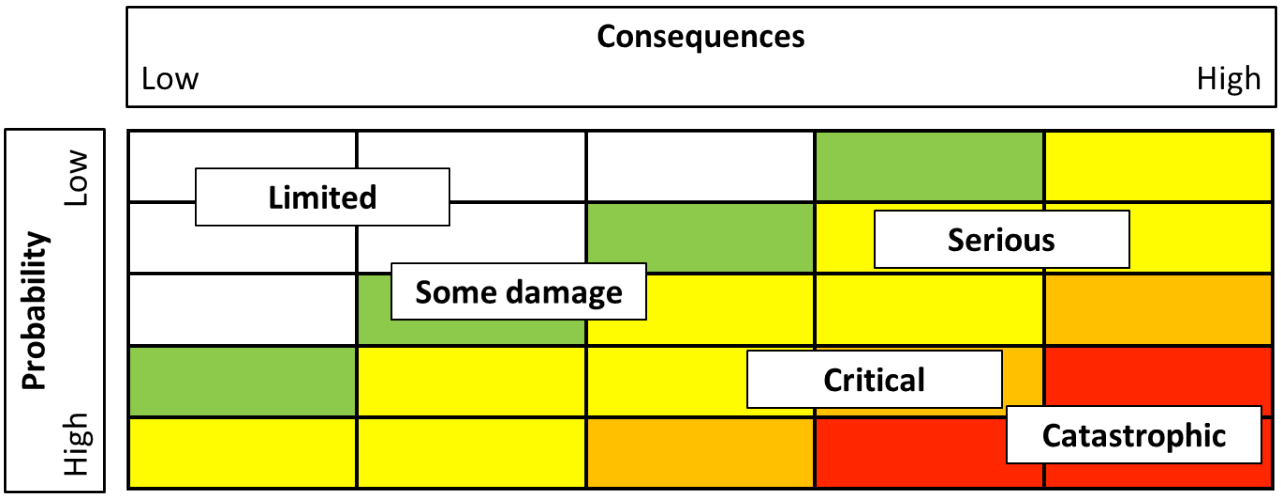


Figure 5 Legend of the risk matrix

The main area of improvement for the stakeholders can be defined by the sections "Some damages", "Serious" and "Critical". In case that the risk calculated for the event is located in the red part "Catastrophic", it should be realized that maybe even the biggest measures for mitigating the criticity of the event are not able to bring a real improvement. In this case, the focus may be rather orientated in the recovery from the extreme event, or in acting on the vulnerability aspect.

The formula used for the calculation is based on the basic equation:

$$Risk = Probability \times Consequence$$

This formula is improved, in order to account for the vulnerability factor, so that the final formula used in the program is as follows:

$$Risk = Probability \times Consequence^{Vulnerability\,factor}$$

The probability factor is an integer that can take the following values: 0-2-4-6-8-10. For the single events, the number is easily deducted from the value set by the user, according to the following Table 5.

Table 5 Link between probability and value used in the risk formula

Calculated probability:	Associated value used in the risk formula:
P=0	0
P<0.00001	2
0.00001≤P<0.0001	4
0.0001≤P<0.001	6
0.001≤P<0.01	8
0.01≤P	10

For joint events, the joint probability is defined by the classical formula:

$$Proba\ of\ simultaneity = P(A \cap B) = P(A/B) \times P(B)$$

In case of independent events, P(A/B) is equal to P(A), thus the probability of joint events is easily directly derived from the single probabilities defined by the user. In case the events are dependent on each other, the value P(A/B) is used. This probability is internally estimated within the program according to simple assumptions. The division between dependent and independent events is also part of the internal routine. The probability of joint events is scaled on the same range as the probability of single events (from 0 to 10), as indicated in the previous table.

The consequences are taken into account in the formula by the use of a factor, scaled in the same range as the probability factor (from 0 to 10). This means that the probability and the consequence are attributed the same relative importance in the definition of risk by the product probability times consequence. The consequences of the events are internally defined for each of the 13 single events. For the single events, the consequences are comprised between 0 and 5. For joint events, the consequences are simply added to one another.

The vulnerability factor is derived from the answers of the user in the first step, where the configuration of the studied area is precisely depicted. An internal routine calculates a number from these input data. This number is further used in the risk formula as the exponent value set on the consequence factor calculated before. This means that in the final formula used for calculating the risk, the consequence has a slightly greater importance than the probability, in conformity with the formula presented below:

$$Risk = Probability \times Consequence^{Vulnerability\,factor}$$

Finally, the results are presented into risk matrices; the snapshot below (Figure 6) gives a view of the output of the program.

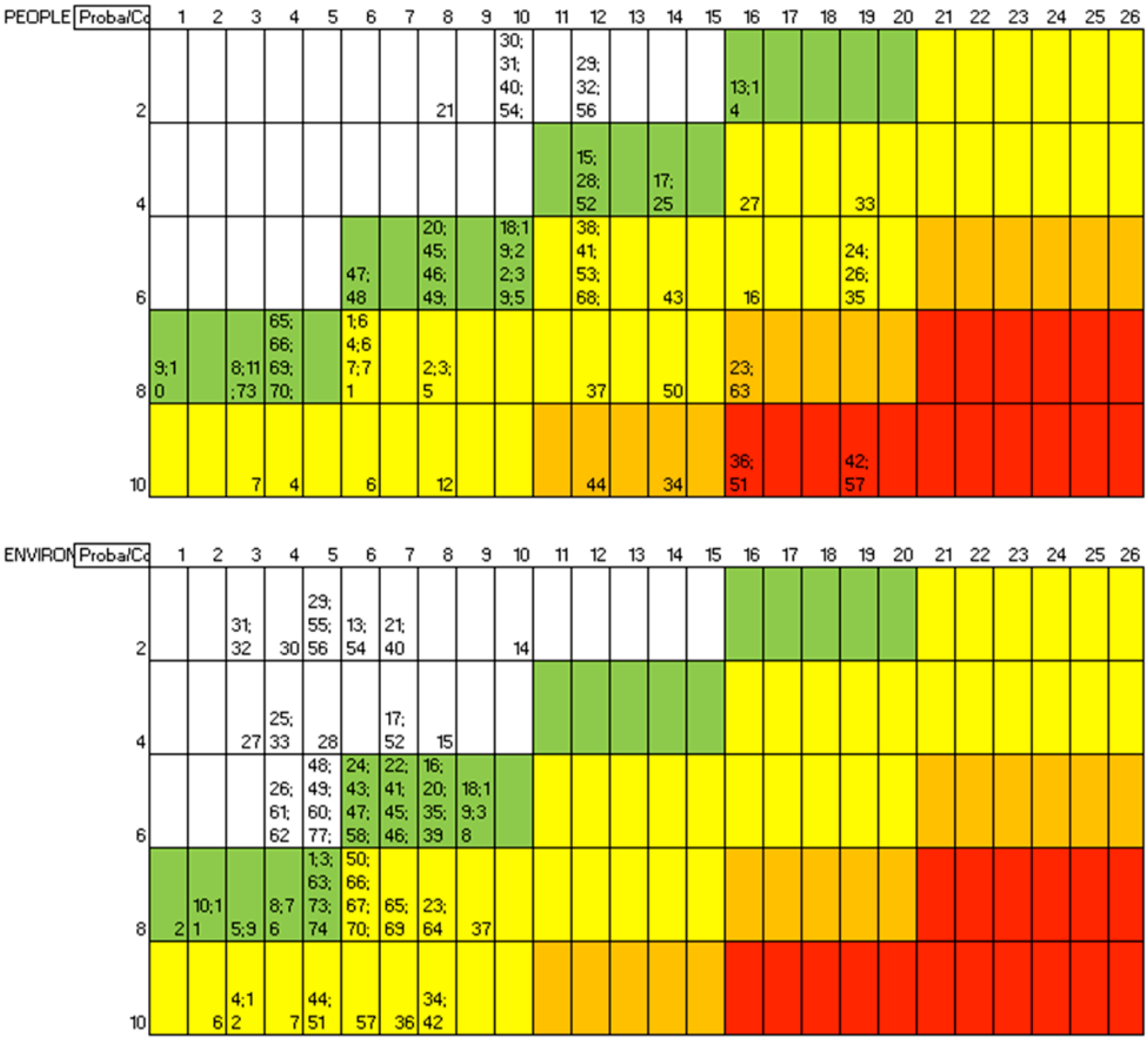


Figure 6 Output of the program

The numbers in Fig. 6 correspond to a given flood configuration. For example, the event numbered 42 is in the red zone for risks on people, but only in the yellow zone when it concerns the environment.

3.3 Step 3- Urban flood simulation and risk mapping

The flood simulation and risk mapping is one of the most important tasks for flood protection. It is incorporated in most flood risk analyses for flood risk management. The present section aims to give an overview of what should be included within the frame of this step III of the stepwise methodology.

3.3.1 Flood risk mapping, the case of Norway

The EU flood directive was mandated in 2007. The directive states that flood risk management plan should focus on prevention, protection and preparedness. The methodology for flood risk management should therefore be developed to include both structural and non-structural measures in different stages. In order to have effective information and basis for priority setting and further technical, financial and political decisions regarding flood risk management, it is necessary to provide information for the establishing of flood hazard maps and flood risk maps showing the potential adverse consequences associated with different flood scenarios and including information of potential pollution to the environment. Flood risk is presented by the product of frequency of flood events and corresponding consequences.

In Norway, the EU Flood Directive (FD) is coordinated by Norwegian Water Resources and Energy Directorate (NVE). NVE performs flood risk analysis for major rivers and river catchments in three stages:

- Carry out preliminary flood risk analysis – The analysis, based on existing hydrological data and gross analysis of consequences for people, environment and economy, and cultural heritage allows deciding where flood risk maps are necessary.
- Make flood risk maps – For areas that are evaluated to have large flood risk, NVE performs detailed analyses of flood hazard maps and consequence maps for three flood scales of medium, large and very large.
- Plan for regional flood management – For those areas that have high potential risk, a flood management plan shall be made. The plan shall be made according to water regions such that it is consistent with EUs Water Framework Directive. Moreover, the flood management plan shall target the risk levels related to people, environment, cultural and economic activities. Changing in flood risk due to climate change and land uses must be taken into consideration in the plan.

3.3.2 Existing methods, models and requirements for data

The two most important processes to evaluate flood risk are the hydrological flood frequency analysis and the hydraulic water level calculation.

The approach of river flood risk mapping includes the following process and data:

1. Data collection of historical flood events

Flood water level marks, flood profiles and areas on photos and papers are important information of historical flood events and for model calibration.

2. Hydrological flood frequency analysis

Flood discharges for different return periods are estimated based on long term discharge observation data and catchment hydrological characteristics.

Common methods for estimation of large flood discharge with rare occurring frequencies are (a) apply the observed discharge data; (b) use discharge data from near stations; (c) Use regional flood frequency analysis and (d) calculate runoff discharge based on rainfall-runoff model and (e) calculate runoff based on IDF (Intensity- Duration-Frequency) curve. The first three methods are

applied mostly to calculate flood discharge for large river basins, while the two last methods (d) and (e) for small urban catchment (< 200 ha) according to NS-EU (1998). Method (a) is the best method to estimate urban flood discharge, however historical data with fine time solutions are usually difficult to obtain. Therefore in most cases, urban flood estimation has higher uncertainty than the results for large river basins.

3. Hydraulic water level simulation

Basic data for hydraulic simulation are surveyed cross sections, discharges based on flood frequency analysis in step 2, observed water levels and records of historical flood events.

Flood water level can be simulated based on 1D or 1D coupled with 2D hydraulic models. For river flood simulation, ID hydraulic model e.g. MIKE 11 and HECRAS or HECGeoRAS (DHI, 2007; HEC, 2010) can be applied in rivers and with delineated cross sections on land surface (Bævre, 2001). To make more accurate simulation of the flood water levels and estimation of flood areas, a 2D hydraulic model can be incorporated with the ID river hydraulic models.

ID sewer model coupled with 2D surface model have been recommended as the best feasible methods for urban flood simulation with concern on the simulation accuracy and for result presentations (Allitt et al., 2009; Maksimovic et al., 2009; Vojinovic and Tuulic, 2009).

4. Flood inundation map

A Digital Elevation Model (DEM) with appropriate spatial resolutions (1-2 m for urban surface and 5-10 m for river catchment) is essential to present the terrain and flood inundation areas. Other elevation data such as elevation for buildings, basic and critical infrastructures should to be included in the DEM in order to estimate and represent the flood risk and vulnerability.

Flood inundation map can be derived based on the DEM and simulated flood water level from hydraulic models.

This flood inundation map describes with as much detail as possible:

- the areas under flood risk
- the depth of water which can be expected at a given location,

It constitutes the starting input to run Step IV of the methodology, and for flood hazard and consequence maps, and finally the flood risk maps.

3.4 Step 4 - Advanced analysis

3.4.1 Introduction

Networks affect the well-being of the people and the smooth functioning of services and, more generally, of economic activities. For instance, over 19 billion tons of freight valued at $13 trillion dollars was moved through the U.S. multimodal transportation system during 2002 (U.S. Department of Transportation 2006). In fact, the economy of a nation or regions depends heavily upon an efficient and reliable transportation system to provide accessibility and promote the safe and efficient movement of people and good (Chen et al., 2002). The transportation system has been identified (Nicholson and Du, 1997) as the most important lifeline in the event of natural disasters such as flood. Yet, it is not so evident, because all networks are interconnected and it is difficult to identify the most important or vulnerable one.

The whole economy of a nation or regions therefore strongly depends upon an efficient and reliable transportation system, but it is also true for other networked systems like electricity, water and telecommunication. For instance, in August 2003 the electrical blackout in North America started with the loss of a single electricity generation plant in Cleveland, Ohio. A cascading failure of interconnected electrical systems commenced, eventually generating a blackout encompassing eight U.S. states, two Canadian provinces, and nearly 50 million people (ELCON 2004). In fact, the most important in a networked system disturbance, it is the potential domino effects on the others systems.

Evaluating network infrastructures for potential vulnerabilities is an important component of strategic planning, particularly in the context of managing and mitigating service disruptions (Murray et al. 2008). Yet, multiple networks that innervate the city are particularly sensitive to flooding, through their structures and geographic constraints. Because societal functions are highly dependent on networked systems, and the operability of these systems can be vulnerable to disasters, there is a need to understand how networked systems are vulnerable.

Moreover, interdependency between different networks tends to increase their vulnerability to flooding. Indeed, this functional dependency between networks may, through a domino effect, lead to failure chain (Fig. 7).

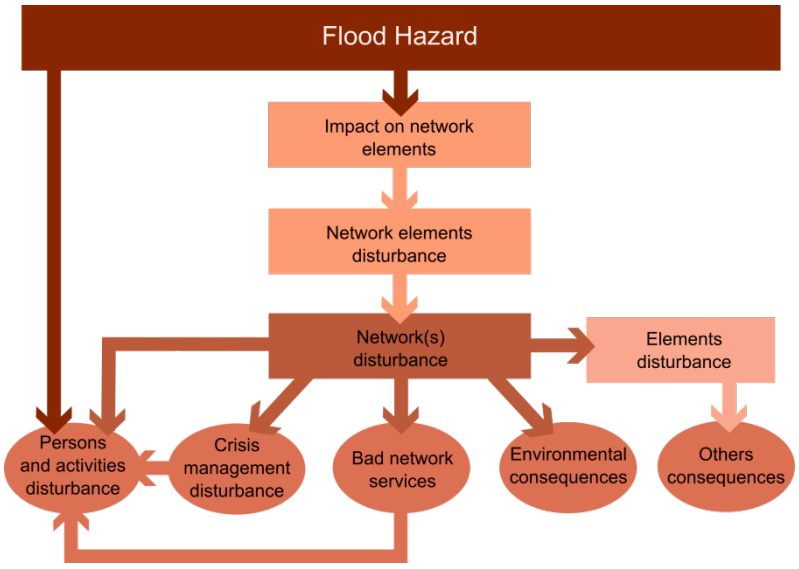


Figure 7 Network domino's effect modelling

The objective here is to design a methodology and tool for advanced vulnerability analyses of networks. These developments represent an example for vulnerability analyses of others critical infrastructures.

The methodology for modelling interdependencies between networks is presented in a first part. Then, in the context of network study, a specific attention to the network properties (particularly redundancy) is needed. Finally, the created web GIS tool is described. This tool is required to implement the overall methodology.

3.4.2 Methodology for interdependencies modelling

The first objective is to design an exhaustive methodology in order to model networks interdependencies. In this way, the use of safety methods is proposed (Lhomme et al., 2011a).

There are several approaches to model interdependencies, which are clearly identified and formalized in the industry (nuclear plant, aeronautic…) and also used in civil engineering (Serre et al., 2008). They can be gathered into two families (Zwingelstein, 1996): internal methods and external methods (Figure 8). Internal methods are based on detailed knowledge of the system functioning. From modeling, it is possible to predict the future behavior of a network and then to analyze the risks. There are two main approaches: physical modeling and functional modeling thanks to safety methods. External methods are used when modeling of the mechanisms (physical or functional) is technically impossible or inappropriate to the level of knowledge, due to system complexity. There are methods based on statistical analysis and those based on expertise.

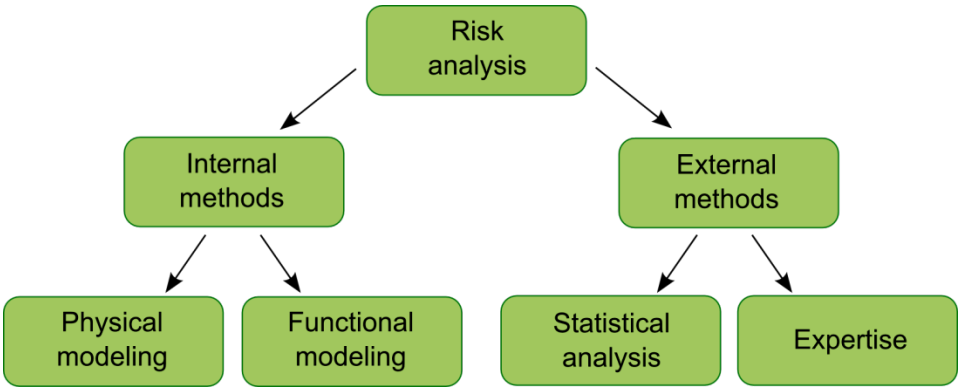


Figure 8 Risk analysis methods (Lhomme et al., 2011b)

The principle of functional modeling is to study the interactions between components of a system and its environment in order to establish a link between the functions failure, their causes and effects. There are various techniques for functional modeling systems: analysis of Failure Modes and Effects Analysis (FMEA), FMEA completed by a criticality analysis (FMECA), the methods of the Tree or Consequences Events. Functional modeling allows better understanding of how the system operates and that is why it allows as well a better understanding of the failure mechanisms.

FMEA is a procedure to identify component failures which have significant consequences affecting the system operations in the application considered. FMEA only provides qualitative analysis. First, FMEA requires breaking down the system into components (structural analysis). Then it is necessary to identify the functional structure of the system and how the components contribute to functions. Then FMEA requires defining failure modes of each component and finishing perform analysis for each failure mode of each component and recording results in Table 6 shown below.

Table 6 FMEA Structure

Network	Components	Functions	Failures	Origins	Effects

After compiling the FMEA data, it is possible to determine the most important failure modes of the systems, their causes and their effects. So, using the FMEA, the failure mechanism model has already been defined, and failure scenarios have been designed thanks to events trees. The events trees analysis was developed in early 1970s for risk assessment of nuclear power plants. The method is used here without quantitative aspects, but this model involves an underlying domino effect induced by networks failure. Indeed, infrastructures and systems do not exist in isolation to one another – telecommunication networks require electricity, as do the sewerage systems. Transportation networks often use sophisticated computerized control and information systems, the generation of electricity requires fuels, etc (Syncera, 2007).

Networks systems failure scenarios are designed by linking failure causes to failure modes, and then to failure effects (Figure 9). In this way, the failure mechanisms are modeled as series of functional failures representing the relevant physical processes taking place within the system and leading to loss or deterioration of functions.

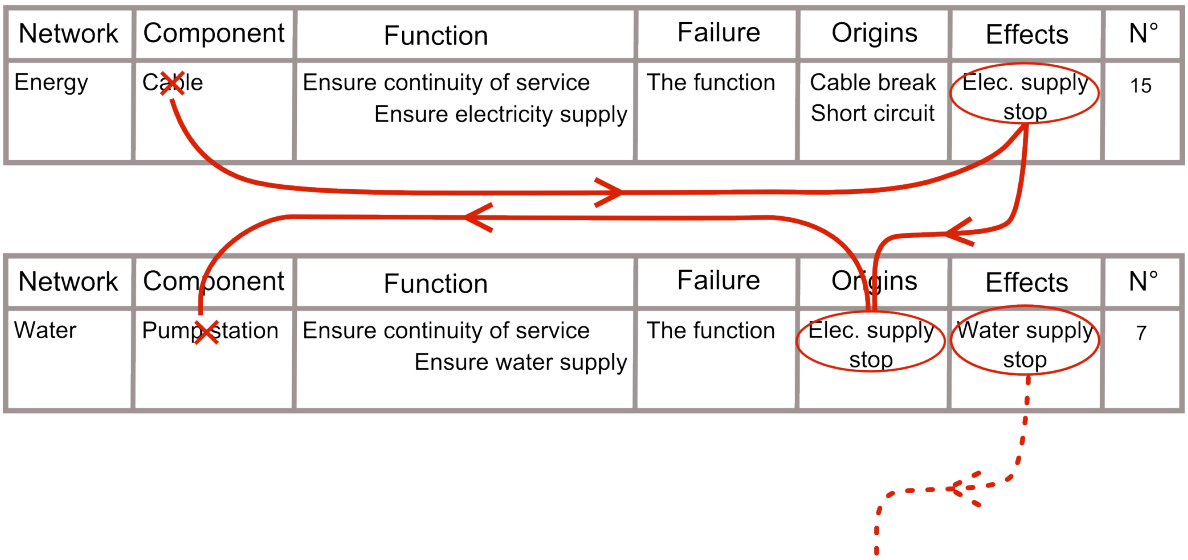


Figure 9 Methodology to produce failure scenarios (Lhomme et al., 2011b)

The methodology for modelling networks interdependencies is summarized below (Figure 10):

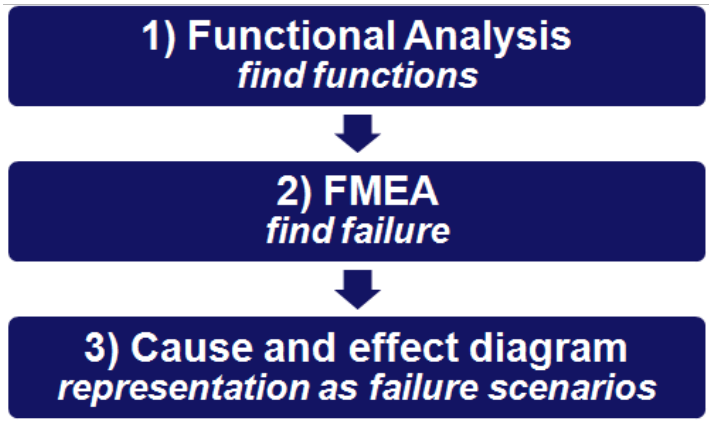


Figure 10 Methodology for modelling networks interdependencies (Lhomme et al., 2011b)

The methodology, presented above, allows producing networks failure scenarios (see example Figure 11). These scenarios may be the most important and plausible ones, thanks to a good knowledge and expertise of the networks, however they do not allow taking advantage of the overall FMEA analysis. Indeed, the structural analysis breakdowns the system in 37 components and 127 functions were identified with the functional analysis. So it is impossible for people to identify all the scenarios using only FMEA results presented in a huge table. Moreover, two interdependency levels must be taken into account: components interdependency level and networks interdependency level. The combination of components and/or functions failures generates too many scenarios. For these reasons, a computer tool is needed to automate design of these scenarios and take sufficiently advantage of the FMEA.

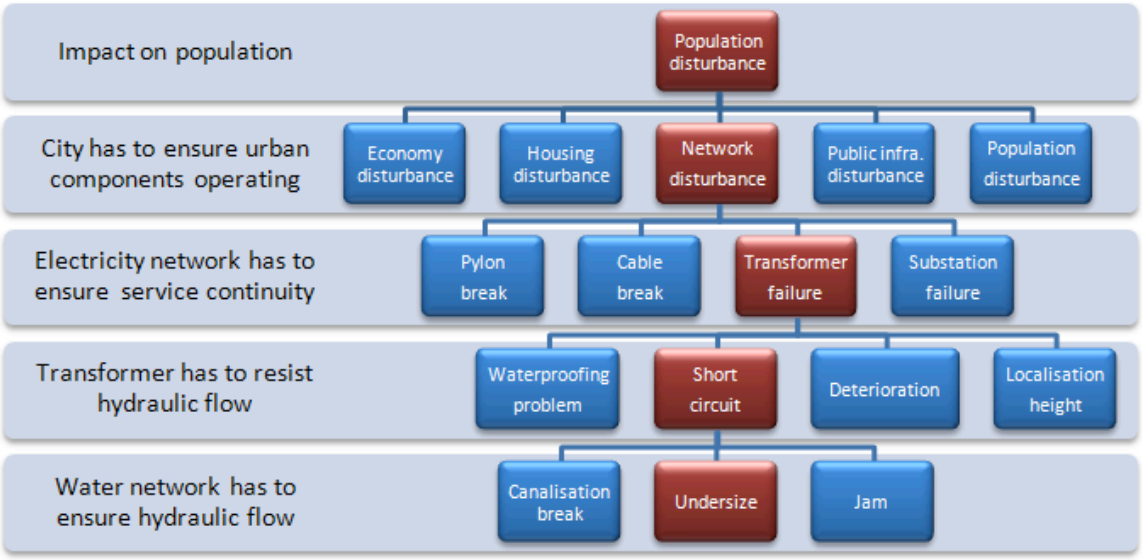


Figure 11 Failure scenario example – this type of scenarios can be identified without an automation process but it is impossible to produce all scenarios (Lhomme et al., 2011b)

The software responds to three main objectives. The first objective is to allow visualization and update of the FMEA. The second objective is to design failure scenarios. The third objective is to analyze the results and to allow an overall understanding of interdependent networks failure modes thanks to diagram representation of the results. In order to produce failure scenarios, FMEA has been implemented into a database.

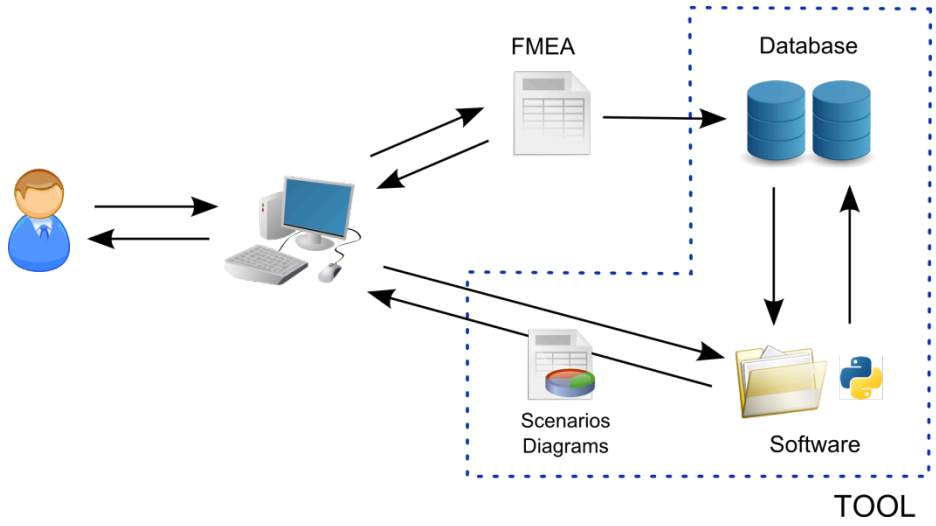


Figure 12 Computer tool architecture for modelling networks interdependencies (Lhomme et al., 2011b)

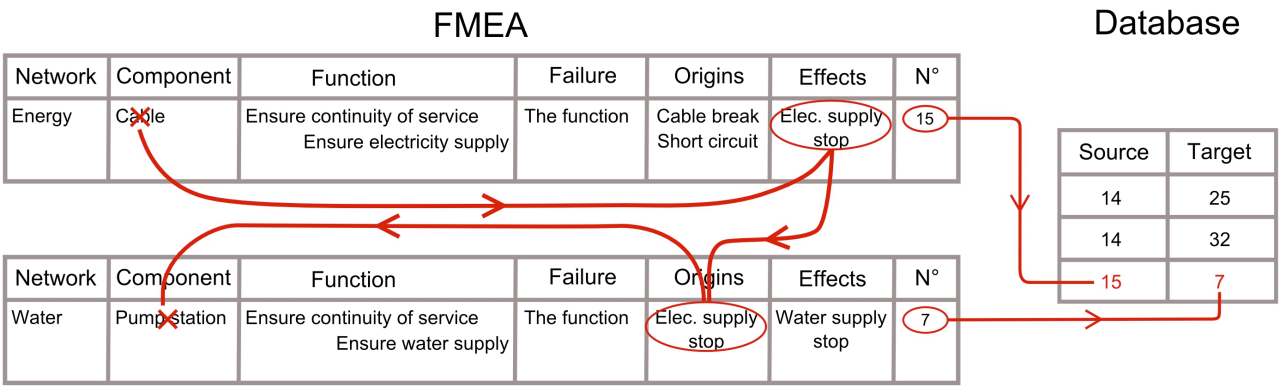


Figure 13 Automation process for interdependencies modelling using database (Lhomme et al., 2011b)

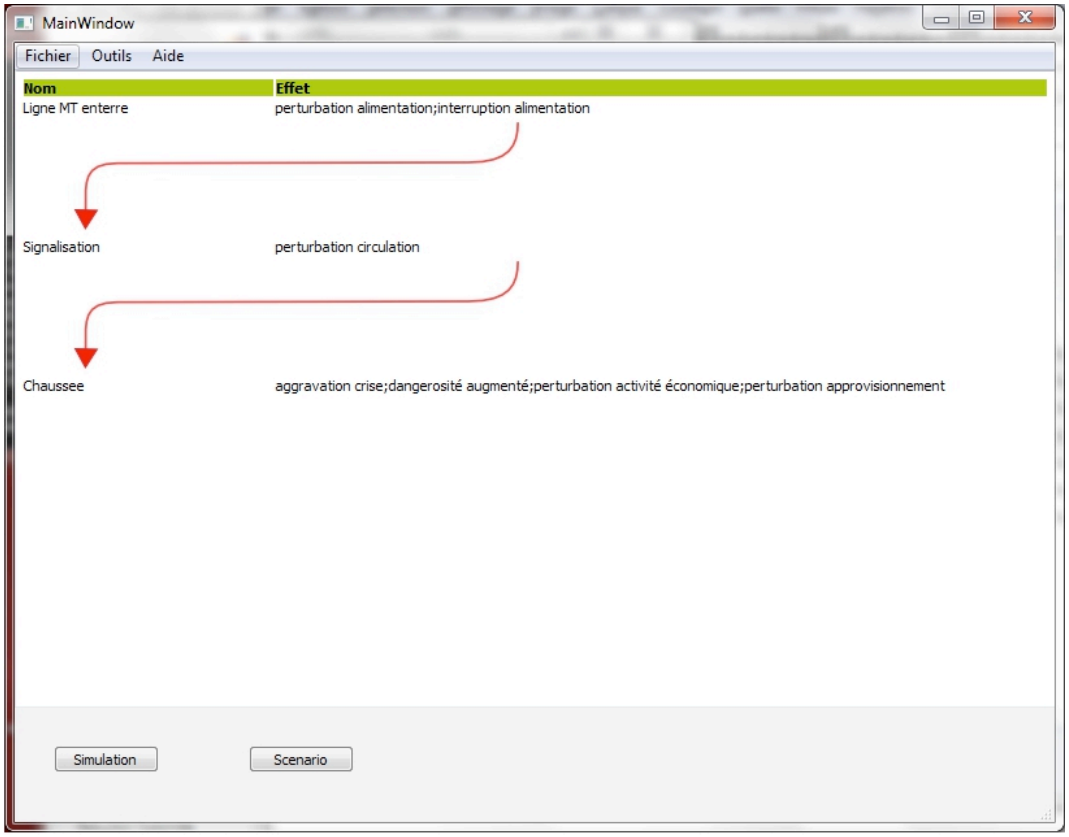


Figure 14 Modelling networks interdependencies thanks to a specific computer tool (French version) (Lhomme et al., 2011b)

3.4.3 From networks interdependencies modelling to networks risk analysis

The use of safety methods makes it possible to design an approach for studying urban networks disturbances caused by specific hazards, while also accounting for interdependencies between networks. Starting from classical internal network studies, crossing the exposure and vulnerability of the networks, it is possible to determine damages on the networks. Thanks to the network analysis, disruptions are determined for each network. Then interdependencies modelling methodology has been used in order to determine disruption scenarios between different networks. Thus, these disruptions require studying their impact on each network (feedback). Others internal networks studies are still required, up to the end of finding new disruptions.

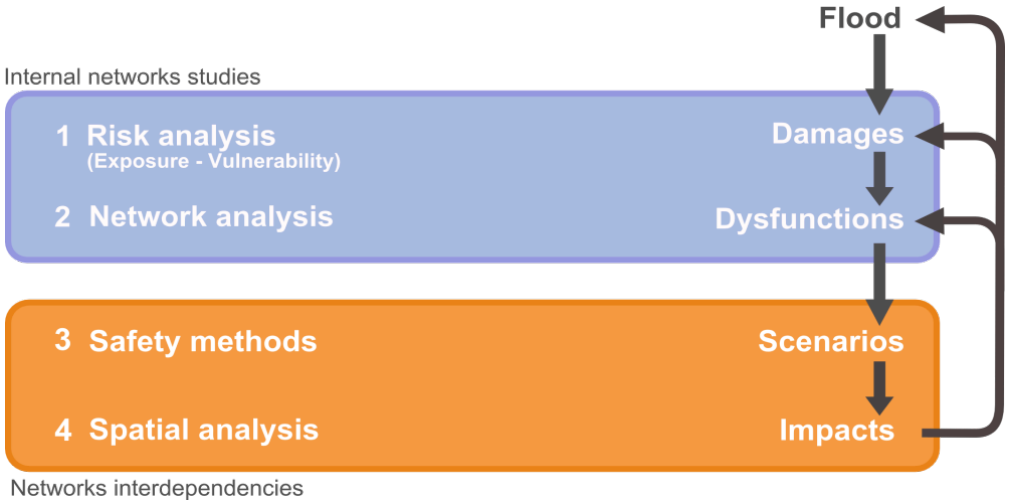


Figure 15 Approach for studying networks disruptions caused by flood and taking into account of interdependencies between networks (Lhomme et al., 2011a)

Data on technical networks are difficult to obtain, especially at a city level. Therefore, the case study presented here is fictional. This case study involves three networks (Figure 16). In the present case, the networks are characterized by an overall weak mesh density although having some densely meshed parts. This basic example puts forward the need to consider interdependencies (in orange dashed lines) between networks (Figure 16). For instance, the electrical network does not suffer direct damage (in red) and direct dysfunction (in pink) from flood hazard but it is damaged by the sanitation network (Figure 16). On a second step, as time increases, the initial failures further generate new dysfunctions (in orange) on sanitation and drinking water networks (by pump stations dysfunctions).

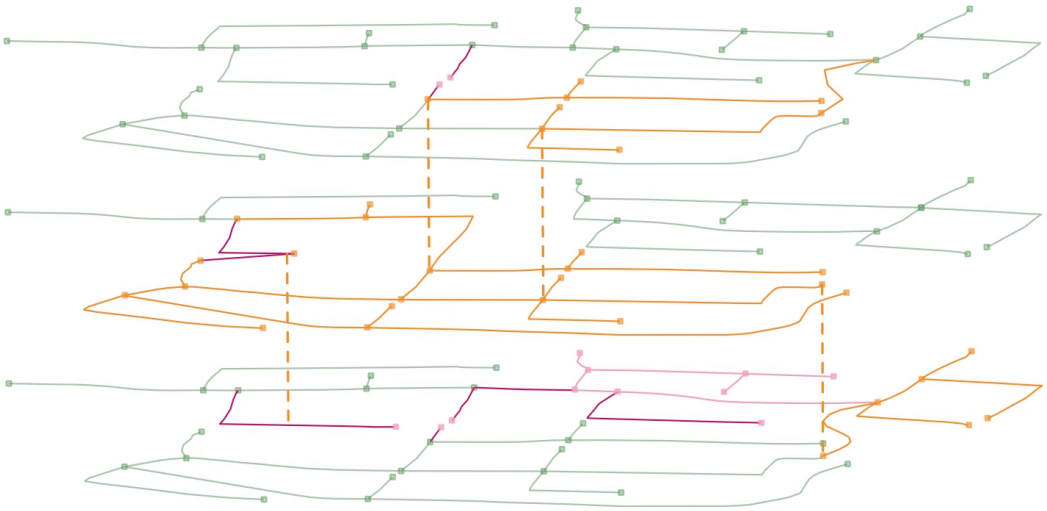


Figure 16 Three fictional networks. Up: drinking water network; Middle: electricity network; Down: sanitation network (Lhomme et al., 2011a)

3.4.4 Topologic properties of networks: redundancy indicators

In order to implement networks risk analysis approach, networks analyses are required. In this way, there are different levels of analysis (Figure 17).

Concepts from modern *graph theory* are fundamental to enable measuring of these observable differences in network topology and flow types. A graph is a very simple structure consisting of a set of vertices and a family of lines (possibly oriented), called edges (undirected) or arcs (directed), each of them linking some pair of vertices. A graph structure can be extended by assigning a weight to each edge of the graph. Weighted graphs are used to represent structures in which connections have some numerical values. For example if a graph represents a road network, the weights could represent the distance or the flow of each road. Thus the study of the graph is not only topologic, but also geometric (distance) and functional (flow). In the present case, the focus is on geometric and topologic properties. Indeed, there is a correlation between the use (the functioning) and the structure of the network. Moreover, studying the underlying network structure of a system has proven to be a useful tool, as many features of complex systems arise from their underlying network structure, rather than specifics of the objects, the interactions and the flows.

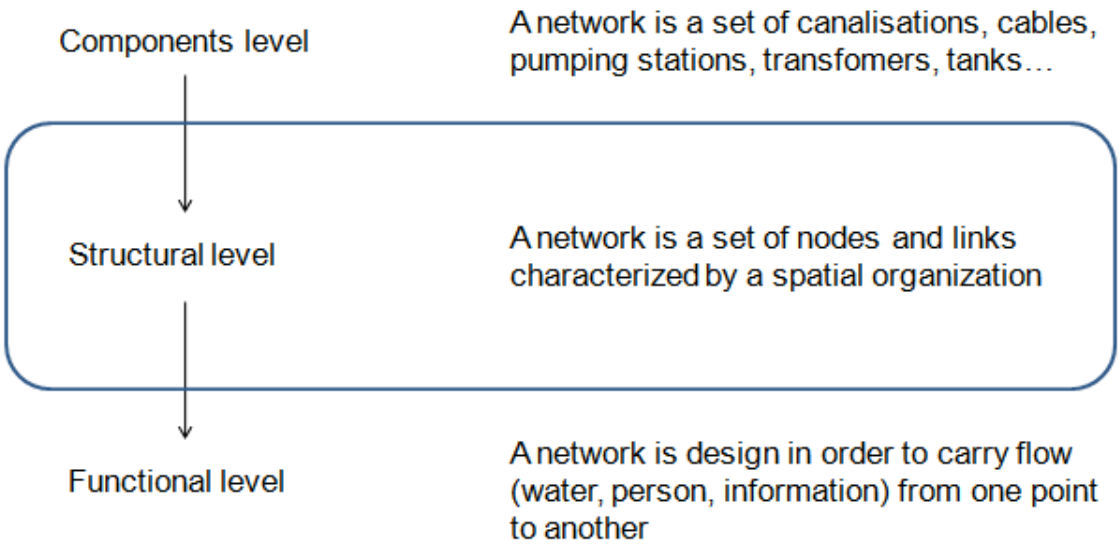


Figure 17 Different levels of networks analysis

A network is characterized by a specific capacity to absorb different types of disturbances. Most of the frequent disruptions are locally absorbed by the networks and the end users remain unaware of their occurrence. This fact results from the ability of the networks to redistribute the flow at the location of the disruption. This is a typical resilience capacity that allows networks to operate in a degraded mode. The geometric properties of the network limit the adaptive capacity of the network. Indeed, network configuration determines the number of alternative path to disruption of one or several components, in other word the redundancy of the networks.

High network redundancy, requires high opportunities (alternate paths to the shortest path) to get from one point to another point of the graph (Dueñas-Osorio, 2005). Some indicators already exist to quantify redundancy of a network, for instance the redundancy ratio. This is a good global indicator to characterize the redundancy of a network, but it presents some abnormality at a local scale. Clustering coefficient is a measure of the degree to which nodes in a graph tend to cluster

together. This indicator is close to the redundancy characterization. Evidence suggests that in most real-world networks, and in particular social networks, nodes tend to create tightly knit groups characterized by a relatively high density of ties (Holland and Leinhardt, 1971; Watts and Strogatz, 1998). Therefore this indicator does not work to characterize a relatively weak density of ties like a tree and a square grid.

The redundancy in the present case corresponds to the number of "independent" relationships to go from one point to the neighbors of the neighbors of this point. The suggestion is to count all the independent paths linking one point and the set of neighbors of its neighbors, like for example the redundancy ratio. The difference between this new indicator and the redundancy ratio is that this new indicator is the mean of this count and not the ratio between this count and the total number of independent paths if the graph was complete.

This indicator is not sufficient to characterize the redundancy of a network. Indeed, each point is considered as an origin or a destination point, but in many cases these points are “connection points”. This means that transitivity is one of the key issues. In mathematics, a binary relation *R* over a set *X* is transitive if whenever an element *a* is related to an element *b*, and *b* is in turn related to an element *c*, then *a* is also related to *c*. In the current case, the relation is not an edge but a path which does not includes the element b. Thus, redundancy corresponds also to a second indicator matching the number of relations (independent paths) between the neighbors of the neighbors of a point when this point is disturbed.

The usefulness of the networks structural analysis based on the two indicators developed is demonstrated by the case analysis of two cities. They are two little cities close to Orleans in the department of Loiret in France. These two cities have been selected because they present very different characteristics in terms of redundancy. The indicators are calculated and a classification in four different classes is carried out for each indicator. As a result, two different maps can be obtained. The last step consists in aggregating information into a single map. For this purpose, for each node, the less redundant class is chosen to characterize the redundancy. The two maps below show the difference of the calculated redundancy between the two cities in a very simple way (Figure 18). It is important to understand that the agglomeration is composed by thousands of points and that this is strictly impossible to detect this structural difference without indicators developed in the frame of the present research.

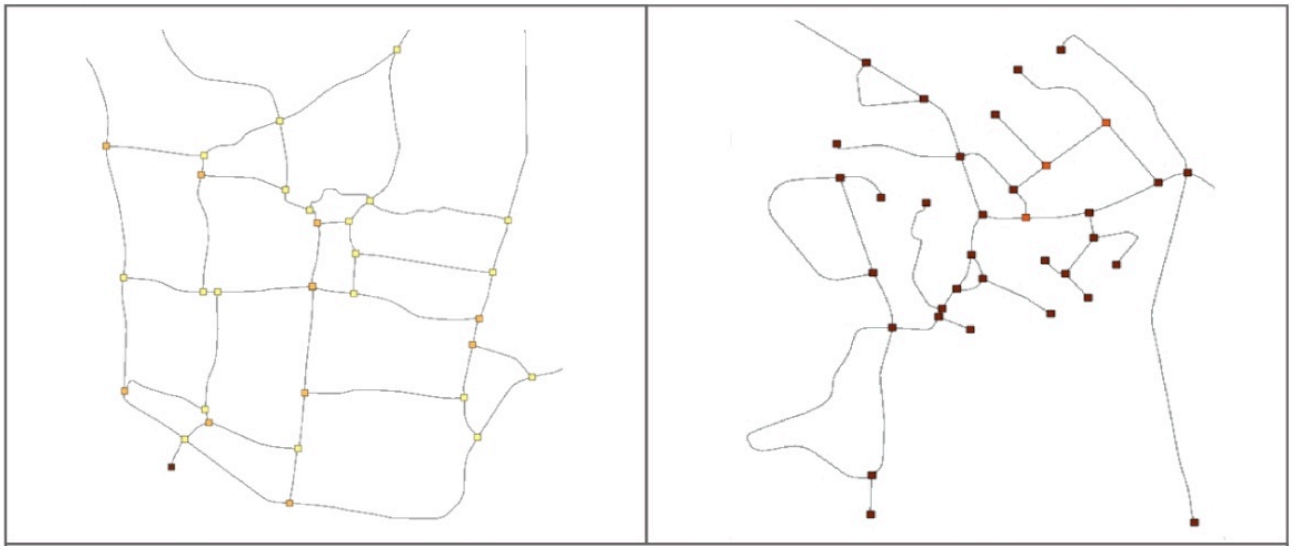


Figure 18 Networks redundancy - Application on the agglomeration of Orleans (left the city of Bou and right the city of Chanteau) (Lhomme et al. 2010)

3.4.5 Web GIS tool

Different information about networks is needed in the research process. This type of information is referred to as spatial information, and when visualized, relationships, patterns, and trends can be discovered that may not otherwise be apparent. A Geographic Information System (GIS) is a mapping software that provides spatial information by linking locations with information about that location. It provides the functions and tools needed to efficiently capture, store, manipulate, analyze, and display the information about places and things.

It is well known that GIS can be used to recover the spatial component of risk and it is clear that risk assessments have an important spatial component. For instance, to better respond to post disaster activities, geographic information system (GIS) technology provides a logical tool for integrating the necessary information and contributing to preparedness, rescue, relief, recovery and reconstruction effort (Gunes and Kovel 2000, Lembo et al. 2008). GIS is seen as a necessary tool in the area of emergency response (Carrara and Guzzetti 1996, Ware 2001).

That is why this type of tool has been chosen to implement these methods.

Web mapping is the process of designing, implementing, generating and delivering maps on the World Wide Web. Web GIS is similar to web mapping but with an emphasis on analysis, processing of project specific geodata and exploratory aspects. Web GIS offers the possibility to have a common platform for users. Moreover, this solution does not require downloading any software, which means that it has a very convenient architecture (see Figure 19).

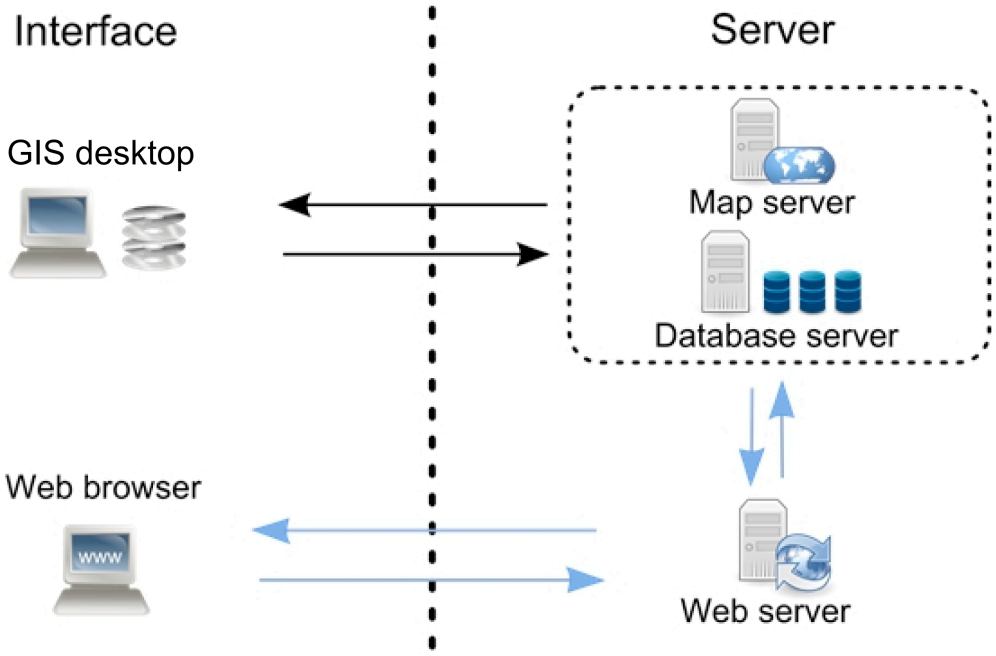


Figure 19 Web GIS architecture (Lhomme et al., 2010)

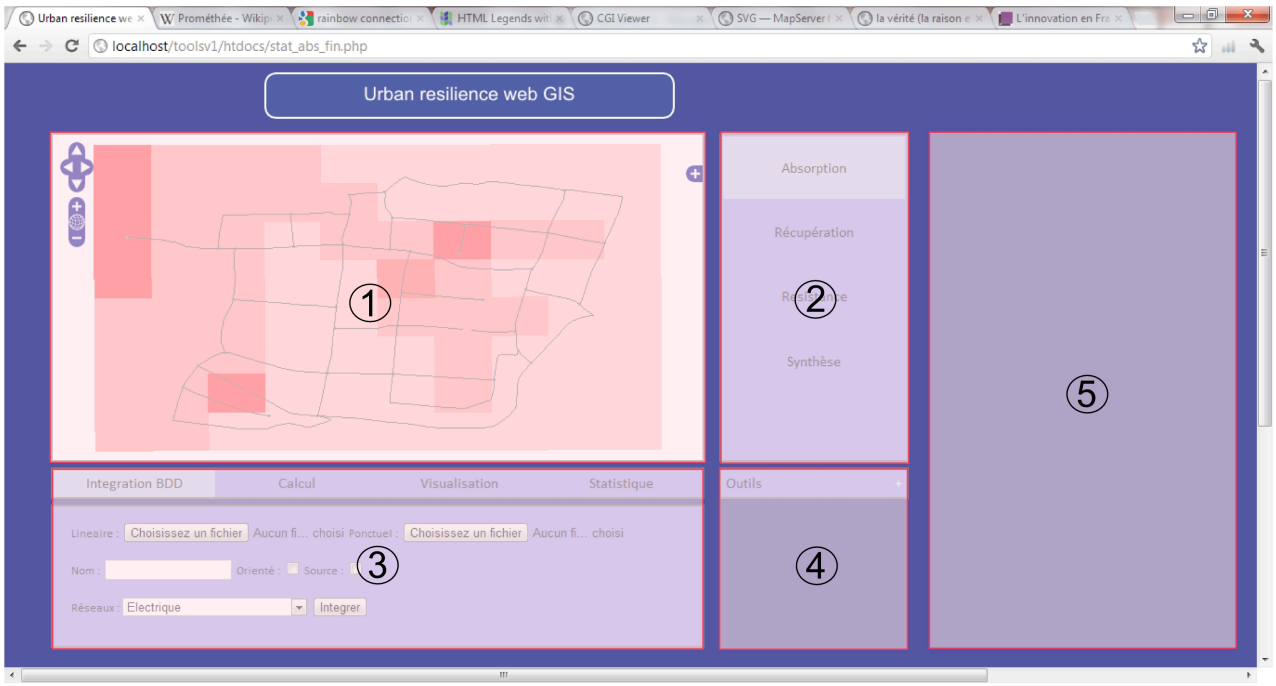


Figure 20 View of the GIS tool (French version) (Lhomme et al., 2011a)

The web GIS is composed by different modules (Figure 20):

1) The map with the main component for navigation and switch layers

2) The menu with the different levels of analysis : redundancy analysis, recovery analysis, disturbance analysis and synthesis of the result

3) The options with the different steps for calculation: from data import to visualization
4) Different tools in order to: print maps, interact with maps, interact with the display area.
5) Display area: area to display information about objects or to display statistic about maps

Types of data (input/output)

The Web GIS requires different types of data which are detailed in Table 7 below.

Table 7 Data needed to implement the Web GIS

	Input	Output
Sewer network	Canalizations Nodes (treatment plants; pumps…)	Map of redundancy (shp/wms) Map of dysfunction (shp/wms)
Road network	Roads Intersections	Map of redundancy (shp/wms) Map of dysfunction (shp/wms)
Drinking water network	Canalizations Nodes (pump stations; pumps…)	Map of redundancy (shp/wms) Map of dysfunction (shp/wms)
Electrical network	Electrical cables Nodes (transformers…)	Map of redundancy (shp/wms) Map of dysfunction (shp/wms)
Flood area	Map of area	-

The Web GIS is developed in order to be able to support different GIS formats (Table 8). In addition to this wide range of adaptability, the web GIS is able to read MIF/MID files.

Table 8 Formats supported by the Web GIS

Software	Format
ESRI	Shp, shx, dbf.
Geoconcept	TXT

MapInfo	TAB, DAT, ID, MAP

The main issue for the reading of the input data files is that they shall be written into the following formatted structure (see Table 9 and Table 10 below).

Table 9 File structure for the data on linear components of the network

Linear component of network				
Identifier (Integer)	Type (Text)	Start node (Integer)	End node (Integer)	Sensibility (Integer)

Table 10 File structure for the data on node components of the network

Node component of network		
Identifier (Integer)	Type (Text)	Sensibility (Integer)

3.4.6 Evaluation and conclusions

In France, two main studies on network vulnerability concluded that the electricity network is the most aggressive network because all the networks depend on electricity supply. As a result, the network vulnerability studies often recommend focusing actions on the electric network. The conclusions brought by the present developed tool are different.

First, in accordance with what is traditionally accepted, the study concludes that the electrical network is the most aggressive of networks (Figure 21). However, it could be shown that the other network components can be as aggressive as the electric components. For instance, electrical and telecommunication pylons are the most aggressive components. This is due to their configurations. These components are indeed located at the interface between their own network and the transportation network.

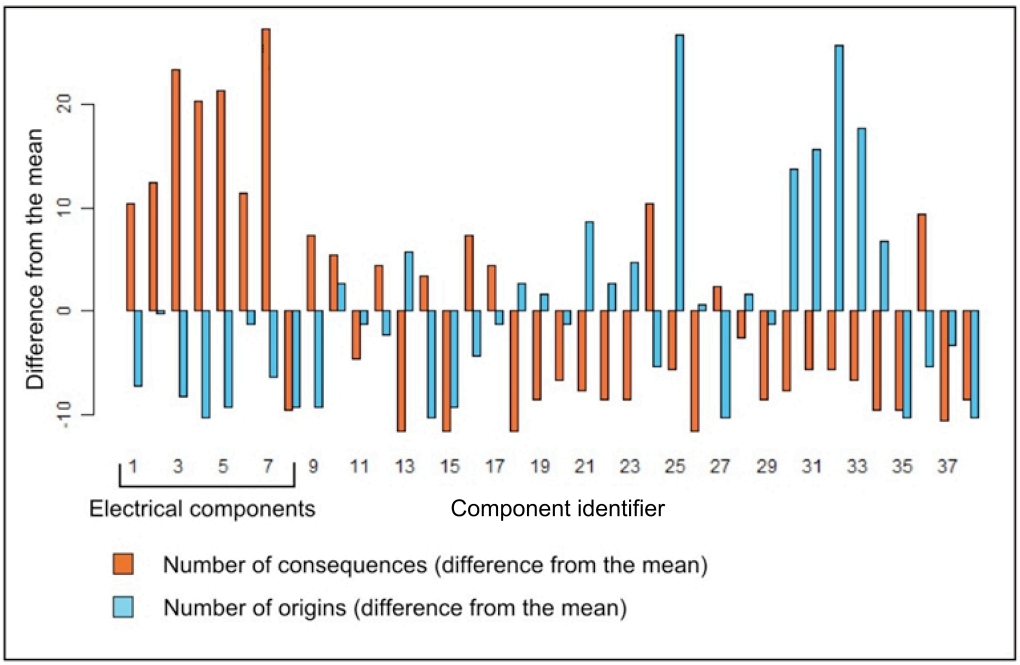


Figure 21 Component failure effects (orange) or causes (blue) diagram (Lhomme et al., 2011b)

The diagram does not only allow studying the most aggressive component, it also allows showing the most sensitive to the disturbance of others components. The most sensitive components can be impacted by a lot of components. These very sensitive components are involved in more scenarios than the most aggressive components. That is why it does not seem pertinent focusing only on aggressive components (for instance on electrical network components).

Some components are very problematic. Indeed, numerous scenarios involve these specific components. These components are not at the origin or the final effects of these scenarios, but are the components which spread the disturbance effect of a given component (Figure 22). Thus, these components disturb other components which are initially not directly impacted by an origin component. The impact of the disturbance of these specific components is more important than the two others indicators (number of causes and effects). Therefore, it seems more important focusing on these components in order to limit the impacts of flooding (pump stations, roads…).

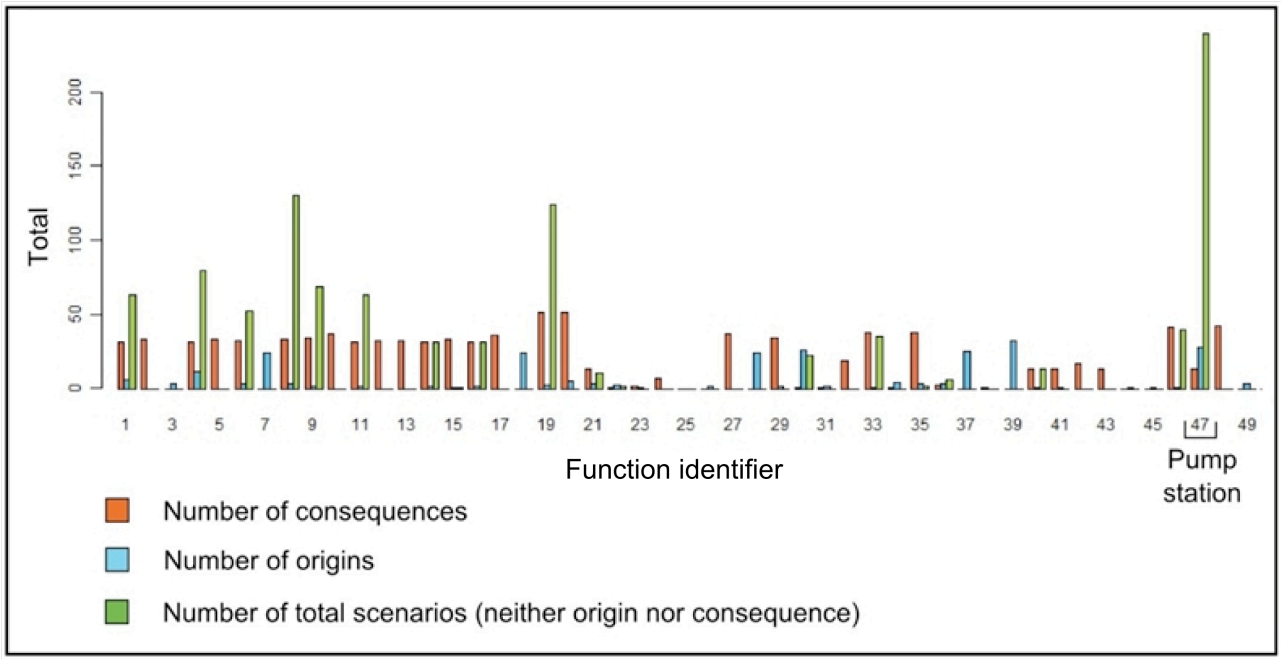


Figure 22 Numbers of consequences, origins and total scenarios (Lhomme et al., 2011b)

4 Barriers to developing and implementing methods and tools

4.1 Discussion on the use of the framework

This project aimed to develop guidance and support for flood vulnerability analysis of critical infrastructure (see chapter 1). In the project a general framework of four steps was defined and for two steps of this framework tools were developed.

This framework has not been applied yet, but the tools have been tried in hypothetical and real case study areas. Step 2, the explorative vulnerability analysis, was applied in Trondheim and step 4, the network independency analysis, was tried on Orleans. The successes and barriers are discussed in the next sections. In Dordrecht the CI vulnerability was studied using the general approach discussed in chapter 2.

4.2 Barriers met in CI research and application of the framework

When considering the study of the CIs in the pilot cities, namely Dordrecht (Netherlands), Trondheim (Norway) and Orléans (France), several challenges or so-called barriers have been encountered. The acknowledgment of these difficulties is a key element of the present work, for two reasons:

- First, these barriers can explain the limited scope of the case studies realized in the frame of this task, presented in the current report. They also illustrate some differences between the handling of flood vulnerability in these European cities.
- Second, the difficulty to collaborate efficiently with the actors which are the final target of the developed methodology must be taken into account as a concrete and determining factor for the implementation of the tool. It matches with the first step of the stepwise methodology. This step is obviously the easiest one in terms of science and detailed knowledge, but seems to be particularly challenging concretely, and is a burning issue for the good implementation of the whole process.

The specific challenges which were met in the three pilot cities are depicted below. They often show that the main resistance comes from the structural organization (internal and public/private) of the entities dealing with flood and vulnerability topics. Clarifying the roles of the stakeholders is a burning issue, as it was clear from the contacts with them, that there is both a real interest and a need for the tool.

4.3 City of Dordrecht (Netherlands)

In the city of Dordrecht, four main barriers exist:

- The critical infrastructures are managed by several different private institutions. They are not willing to provide detailed data, for reasons of security (fear for terrorism, or sabotage) or for competitive reasons (economic competition).
- There is no single organization responsible for CI vulnerability towards flooding.
- There is only little exchange in knowledge between flood risk management and CI. The private institutions do not have knowledge of flood hazards. The flood early warning organizations, safety regions and flood risk managers have no knowledge of CI.
- No flood has occurred in the Netherlands recently, only some water annoyance in a small area in the southwest. In addition, no useful historic data on CI failure exists.

4.4 City of Trondheim (Norway)

In the city of Trondheim, the main barriers came from the insufficient communication between the different stakeholders. When entering in contact with those persons, the first challenge is to find and meet the relevant interlocutor. Because of the structure of the public organization, the department for water utility does not have responsibility for overall risk management in the municipality. It is often that in practice an independent expert or expert group is appointed to implement the risk assessment at a general level. This assessment is done at very broad scope of

dangers (all kinds of risks threatening the city, not only water) with relatively gross analysis or assessment, which often result in high uncertainties.

The question of risk is in fact split between different corps (firemen, buildings, the water section of the municipality, and sectors such as road and railway, etc). This fragmentation has both benefit (for the quality of specific property or system) and disadvantage as no one in the city has yet a comprehensive overview of the risks. In addition, although receiving some strong feedback on the interest for the developed methodology, the stage on which and details for implementation are difficult to be defined: discussions for an agreement between the various actors takes time.

The stage of linking the infrastructures (interdependency in the risk evaluation) is thus an issue on which people are aware but no tool is yet available, which pleads on the methodology's behalf. This awareness is a very good starting point, but more dialogue is now needed between the stakeholders of the various infrastructures. The split of responsibilities between private and public owners makes it an even greater challenge.

In addition, there is a lack of communication on the tools available on the market and end users. There is a very relevant official website (klimatilpasning.no), but this website is not properly updated, thus incomplete, which makes it challenging to clearly identify the real gaps.

The exchanges with the municipality also emphasize the discrepancy between the structural organizations of a city at the size of Trondheim versus smaller cities, which have less available resources to cope with the risk, consequently more vulnerable than Trondheim when exposed to flood or other natural hazards.

4.5 City of Orléans (France)

In the city of Orléans, as in the city of Dordrecht, the CIs are managed by several private institutions, which are reluctant to provide data for both security (terrorism, sabotage) and competitive reasons.

The city of Orleans is involved with the local state authority for the crisis management of network infrastructures. However, the city managers do not have access to accurate geographic data and can only access the final results of these works.

Some studies about network vulnerabilities have already been carried out and a working group has been created. This clearly shows that the city managers are aware of the criticality and the vulnerability of the networks. Nevertheless, the city managers are not convinced that further knowledge is needed. This reaction could be explained by the fact that the issue seems to transcend their attributions.

5 Conclusion and further perspectives

The current report presents the work which has been done in the frame of Task 2.1 of the FloodProBE project, which focuses on the vulnerability assessment of critical infrastructure in urban areas with respect to floods.

Vulnerability assessment is an important tool to support authorities and property owners to identify potential risk scenarios before or after hazardous events and for risk preparedness, protection and reduction.

The present report suggests a stepwise approach, from simple coarse assessment to advanced modelling. This approach is oriented towards the stakeholders in charge for critical infrastructures and flood vulnerability in urban areas, whether they are public entities, private consultants or researchers. The focus is on Critical Infrastructure (CI). Prior to the presentation of the guidance, a special chapter is dedicated to building a clear understanding of what "critical infrastructure" stands for, and its scope, especially when related to floods. Many discussions are still on going for defining this term, according to both political and cultural issues. A consensus is obtained in the frame of this project for the following definition: critical infrastructure (CI) stands for the infrastructure which is essential for the functioning of society, and whose failure would seriously affect many people. The developed approach is to build a guide for the vulnerability assessment of CI. Approaching critical infrastructures with a vulnerability assessment is not a common practice yet. Unlike other types of assessments, a new vulnerability assessment has been developed that includes the possible secondary and indirect effects through a well-organised pattern of analysis in three steps: network analysis, analysis of the resistance and resilience of the network elements, and analysis of the effects of element failure on the network. In addition to this accounting for secondary effects, the strength of the methodology lies in the formatting of the interdependency between the infrastructures. The complexity of the interactions, as well as various methods to model the interdependencies, has been described in detail. The whole structure of analysis is perfectly adapted to flood risk.

Once the main concepts behind the guidance are defined, the comprehensive framework for vulnerability assessment of the CIs is finally presented. The stepwise steps match respectively with the demand of analysis in different levels, i.e. it goes from step 1, a simple analysis, to step 4, the most sophisticated assessment. In case that all the steps are performed, the final result is a thorough insight into the current CI, and its vulnerability towards flooding of the area under assessment:

- Basic analysis, gathering the stakeholders, first collection of information
- Risk assessment performed on various infrastructures
- Urban flood simulation and risk mapping
- Advanced analysis, FMEA (Failure Mode and Effect Analysis)

Within the frame of FloodProBE, only steps 2 and 4 have been tackled, as these are the steps for which the gap in existing tools is the most important, and thus leaves most space for innovation. The first tool, which allows fulfilling step 2 (Risk assessment performed on various infrastructures), consists in a coarse analysis which results in the generation of risk matrices. These matrices are easy handy tools which support the discussion and the decision process for the stakeholders. This first tool only requires basic knowledge of the area under investigation and can be performed by

users from different backgrounds. The second tool is a more sophisticated one, located on top of the suggested stepwise methodology. This is a modelling tool based on Failure Modes and Effects Analysis (FMEA). It enables to study the interdependency between networks subsequently to a disaster. The tool shows how a simple disruption can generate breakdowns on other networks through cascade effects. The output is a map of the assessed area, which identifies the most critical sectors. The tool is developed based on GIS analysis. Both tools developed in the project are presented in two ways: a brief overview of their methodologies, followed by a case study.

In addition to these scientific developments, one important finding of Task 2.1, concerns the various limitations and barriers which are met in the dialogue with the final target of the guidance: the stakeholders. Because of the complexity of the structural organisation within the public body, and because of the well spread duality between public and private stakeholders (raising security and economic issues), the application of the guidance is often slowed down. This special challenge reflects in fact the crucial step 1 of the methodology: gathering the relevant people and starting the assessment.

The strongest aspect of the developed methodology is that it provides guidance for CI vulnerability analysis, which was lacking up to now. It gives insight to define in which way the CI networks are vulnerable to flooding and what specific elements or links can cause this vulnerability. It also provides help in analysing the interdependencies of CI networks and thus in spreading the failure of one CI-network to failure of others. Furthermore, the guidance has been made as general as possible in the sense that it is not developed specifically for a certain country or area, and can thus be applied in various countries. Finally, the great advantage of this methodology is its flexibility, which offers different levels of detail.

Further research for the improvement of the present work could go deeper into the study of the duration of CI failure, the corresponding damage, and societal disruption. In addition, as mentioned, the framework and tools are still on the research step and need to be applied more intensively to become more strongly proven methods.

6 References

AGO-AUSTRALIAN GREENHOUSE OFFIC (2006). Climate change impacts & risk management – A guide for business and government. Department of Environment and Heritage, Australian Government.

AVEN T (2008), Risk Analyses - Assessing Uncertainties Beyond Expected Values and Probabilities. Whiley, ISBN 978-0-470-52736-9.

BOIN A, MCCONNEL A, (2007), Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. Journal of Contingencies and Crisis Management, 15(1), 50-59. doi:10.1111/j.1468-5973.2007.00504.x

BRUIJNE M D, EETEN M V, (2007), Systems that Should Have Failed : Critical Infrastructure Protection in an Institutionally Fragmented Environment. Journal of Contingencies and Crisis Management, 15(1).

BÆVRE, I. (2001). Delprosjekt Trondheim, Flomsonekart rapport nr. 6/2001.

CARRARA A, GUZZETTI F, (1996), GEOGRAPHICAL INFORMATION SYSTEMS IN ASSESSING NATURAL HAZARDS, KLUWER.

CASEY S (2005), Establishing Standards for Social Infrastructure. In: UQ Boilerhouse Community Engagement Centre, University of Queensland Ipswich Campus.

CHEN A., YANG H., HONG K. L., WILSON H. T., (2002), Capacity reliability of a road network: an assessment methodology and numerical results, Transportation research, pp. 225-252.

De BRUIJN, K.M. (2012). Analysis of the vulnerability of flooding of Critical infrastructure. Method applied to the Island of Dordrecht. Deltares, Delft, The Netherlands.

DELAURENTIS D, (2007), Role of humans in complexity of a system-of-systems. In: Duffy VG, editor. Digital Human Modelling. Berlin: Springer-Verlag, pp. 363–71.

DSB (1994). A guide to risk and vulnerability assessment in the municipality. Norwegian Directorate for Civil Protection and Emergency Planning.

DUENAS-OSORIO L, (2005). Interdependent response of networked systems to natural hazards and Intentional disruptions. Dissertation, Georgia Institute of Technology. Atlanta: Georgia TechLibrary, UMI 3198529.

EGAS W, LUYENDIJK E, BOOLTINK M, VISSER W, VAN KRUINING M, DE BRUIN E, TROMP E, ASSELMAN N (2010), Handreiking overstromingsrobuust Inrichten; samen maken we Utrecht mooier. Provincie Utrecht, Utrecht, The Netherlands 73 p. (In Dutch)

ELCON (Electricity Consumers Resource Council), (2004), The economic impacts of the August2003 blackout.

EXCIMAP (2007) Handbook on good practices for flood mapping in Europe, Prepared by EXCIMAP (a European exchange circle on flood mapping), Endorsed by Water Directors, 29-30 November 2007.

EU (2007b). Directives on the assessment and management of flood risks. The European Parliament and of the council of 23 October 2007.

FEKETE A (2011), Common Criteria for the Assessment of Critical Infrastructures. Int. J. Disaster Risk Science 2 (1): 15-24

FULMER JE (2009), What in the world is infrastructure? In: Investment Strategy, pp. 30-32.

GORDON K & DION M (2008), Protection of 'critical infrastructure' and the role of investment policies relating to national security. OECD, Investment Division, Directorate for Financial and Enterprise Affairs, Organisation for Economic Co-operation and Development

GUNES A E, KOVEL J P, (2000), USING GIS IN EMERGENCY MANAGEMENT OPERATIONS, J. URBAN PLANN. DEV., 126(3), PP 126-149.

HEC (2010). Hydraulic software tools developed by Hydrological Engineering Centre for River System Analysis, US Army Corps of Engineers.

HOLLAND P, LEINHARD S, (1971), Structural sociometry, Perspectives on Social Network Research, edited by P. Holland and S. Leinhardt, Academic Press, New York.

JAMSHIDI M, (1983), Large-Scale Systems: Modeling and Control. New York:Elsevier.

KAPPOS AJ, STYLIANIDIS KC, PITILAKIS K (1998), Development of Seismic Risk Scenarios Based on a Hybrid Method of Vulnerability Assessment, Natural Hazards 17: 177–192, 1998.

KOTOV V, (1997), Systems-of-systems as communicating structures, Hewlett Packard Computer Systems Laboratory Paper.

LEMBO A, BONNEAU A, O'ROURKE D T, (2008), INTEGRATIVE TECHNOLOGIES IN SUPPORT OF GIS-BASED POSTDISASTER RESPONSE, NATURAL HAZARDS REVIEW, ASCE, PP 61-69.

LHOMME S., NIE L., BALMAND E., HEILEMANN K., DE BRUIJN K., SERRE D.(2012), A Stepwise Approach For Flood Risk And Vulnerability Assessment For Urban Flood Critical Infrastructures, FloodRisk, Rotterdam, The Netherlands, 8 p.

LHOMME S., SERRE D., DIAB Y., LAGANIER R., (2010), A methodology for urban flood resilience assessment, Europeen Geosciences Union. General Assembly 2010, Session NH9.13 "Natural Hazard Resilient Cities", EGU2010-14633, 2-7 mai 2010, Vienne, Autriche.

LHOMME S., TOUBIN M., SERRE D., DIAB Y., LAGANIER R., (2011a), From technical resilience toward urban services resilience, Proceedings of the fourth Resilience Engineering Symposium, June 8-10 2011, Sophia Antipolis, France, Presses des Mines, collection sciences économiques, ed. Hollnagel E., Rigaud E., Besnard D., pp. 172- 177. http://www.mines-paristech.fr/presses/consultation.php?livreplus=171

LHOMME S., SERRE D., DIAB Y., LAGANIER R., (2011b), A Methodology to Produce Interdependent Networks Disturbance Scenarios, Vulnerability, Uncertainty, and Risk: Analysis, Modeling, and Management Proceedings of the ICVRAM 2011 and ISUMA 2011 Conferences, pp. 724-731. (doi:10.1061/41170(400)88), http://dx.doi.org/10.1061/41170(400)88.

MAKSIMOVIC, C., PRODANOVIC D., BOONYA-AROONNNET, S., LEITAO, J.P., DJORDJEVIC, S. AND ALLITT R. (2009). Overland flow and pathway analysis for modeling of urban pluvial flooding. Jo. Of Hydraulic Research, 47 (4):512-523.

McBAIN W, WILKE D, RETTER M (2010), Flood resilience and resistance for critical infrastructure. CIRIA C688-London, London, UK.

MCNALLY R K, LEE S-W, YAVAGAL D, XIANG W-N, (2007), Learning the critical infrastructure interdependencies through an ontology-based information system. Environment and Planning B: Planning and Design, 34(6), 1103-1124

MOTEFF J & PARFOMAK P (2004), Critical Infrastructure and Key Assets: Definition and Identification. In: CRS Report for Congress.

MURRAY A T, MATISZIW T C, GRUBESIC T, (2008). A methodological overview of network vulnerability analysis, Growth and Change, Vol. 39 No.4, pp. 573-592.

NICHOLSON A., DU Z. P., (1997), Degradable transportation systems: an integrated equilibrium model, Transportation Research, pp. 209-224.

NIE, L. (2004). Flooding Analysis of Urban Drainage Systems (Ph.D. Thesis). Norwegian University of Science and Technology. ISBN 82-471-6240-7. ISSN 1503-8181.

NIE L, HEILEMANN K, HAFSKJOLD LS, SÆGROV S, JOHANNESSEN BG (2009), Adapting community to flood risk and vulnerability caused by climate change. In: E. Pasch, N. Evelpidou, C. Zevenbergen, R. Ashley, S. Garvin (eds.): International Conference of European and Global Communities combine forces on Flood Resilient Cities, Paris, France, 26-27th November 2009.

NIE L, LI P., HEILEMANN K, SELSETH I. (2010) Risk and vulnerability assessment for urban flooding in Trondheim. SINTEF report.

NIE, L., HEILEMANN, K., JOHANNESSEN B.G.(2011). Flood risk assessment for urban critical infrastructures- from simple risk assessment to advanced models. Proceedings of the 5th International Conference of Flood Management (ICFM5), 27-29th September, Tokyo, Japan.

NS-EN752 (4) (1998), Drain and Sewer Systems Outside Buildings, part 4: Hydraulic Design and Environmental Considerations, European Committee for standardization (CEN), Brussels, Belgium.

NVE (2008). Planlegging og utbygging i fareområder langs vassdrag. Retningslinjer, nr.1 2008. pp.18.

OUEDRAOGO A, GROSO A, MEYER T (2011), Risk analysis in research environment – Part I: Modeling Lab Criticity Index using Improved Risk Priority Number– Safety Science 49 (2011) 778-784.

OUEDRAOGO A, GROSO A, MEYER T (2011), Risk analysis in research environment – Part II: Weighting Lab Criticity Index using the Analytic Hierarchy Process – Safety Science 49 (2011) 785-793

PEDERSON P, DUDENHOEFFER D, HARTLEY S, PERMANN M, (2006), Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research.

RINALDI S M, PEERENBOOM J P, KELLY T K, (2001), Identifying, understanding, and analyz- ing critical infrastructure interdependencies. IEEE Control Systems Magazine 2001;21(6), pp.11–25.

RINALDI S M, (2004), Modeling and simulating critical infrastructures and their interdependencies. 37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the, 00(C), 8 pp.

SERRE D., LHOMME S., HEILEMANN K., HAFSKJOLD S., TAGG A., WALLIMAN N., DIAB Y. (2011), Assessing vulnerability to floods of the built environment - integrating urban networks and buildings. Proceedings of the International Conference on Vulnerability and Risk Analysis and Management, American Society of Civil Engineers, University of Maryland, Hyattsville, MD, USA, pp. 746-753. In Vulnerability, Uncertainty and Risk, Ayyub B., ASCE, ISBN 978-0-7844-1170-4.

SERRE D., PEYRAS L., TOURMENT R., DIAB Y., (2008), LEVEE PERFORMANCE ASSESSMENT: DEVELOPMENT OF A GIS TOOL TO SUPPORT PLANNING MAINTENANCE ACTIONS, JOURNAL OF INFRASTRUCTURE SYSTEM, ASCE, VOL. 14, ISSUE 3, PP. 201-213.

SYNCERA, (2007) QUICK SCAN HALVE METER RAM, IN OPDRACHT VAN HET MINISTERIE VAN VERKEER EN WATERSTAAT, DG-WATER.

TOLONE W J, WILSON D, RAJA A, XIANG W, HAO H, PHELPS S, JOHNSON E W, (2003). Critical infrastructure integration modeling and simulation. Intelligence and Security Informatics, (August 2003), 214–225. Springer. Retrieved from http://www.springerlink.com/index/mn34d6uw84fcm6l4.pdf

UTNE B, HOKSTAD P, KJØLLE G, VAT, J, TØNDEL IA, BERTELSEN D, FRIDHEIM H, RØSTUM J (2008), Risk and Vulnerability Analysis of Critical Infrastructures - The DECRIS Approach, SAMRISK conference Sept. 1-2 , 2008 in Oslo, http://www.sintef.no/Projectweb/SAMRISK/DECRIS/Documents/.

VATN J. (2007). Description of tool for Identification and Estimation of Risk-related Critical Infrastructure (InfraRisk). Department of Production and Quality Engineering, Norwegian University of Science and Technology.

VOJINOVIC, Z. AND TUULIC D. (2009). On the use of 1D and coupled 1D-2D modeling approaches for assessment of flood damage in urban areas. Urban Water Journal. Vol.6, No.3, September 2009, 183-199.

WARE J I, (2001), GEOSPATIAL DATA FUSION: TRAINING GIS FOR DISASTER RELIEF OPERATIONS, 2001.

WATTS D J, STROGATZ S H, (1998), "Collective dynamics of 'small-world' networks." Nature **393** (6684), pp. 409–419.

ZWINGELSTEIN G., (1996). La maintenance basée sur la fiabilité, Collection Diagnostic et Maintenance, Hermès.