PREDICT

**PREparing** for the Domino effect in Crisis siTuations.

# PREPARING FOR THE DOMINO EFFECT IN CRISIS SITUATIONS

## D3.1 METHODOLOGY FOR THE IDENTIFICATION AND PROBABILITY ASSESSMENT OF CASCADING EFFECTS

Date: 01/12/2014
Document ID: PREDICT-20141201-D3.1 Methodology
Revision: Final

This project has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° FP7-SEC-2013-607697.

| Project co-funded by the European Commission within the Seventh Framework Programme (2007-2013) | | |
|---|---|---|
| Dissemination level | | |
| 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) | |

| Document change log | | | | |
|---|---|---|---|---|
| Revision | Edition date | Author | Modified sections / pages | Comments |
| DRAFT | 25-09-2014 | M.H.A. Klaver, K. van Buul, A.H. Nieuwenhuijs, H.A.M. Luijf | ALL | First draft; chapters I – IV |
| DRAFT | 30-10-2014 | CEA, ITTI, SYKE, VTT | Chapter II.4, Chapter III.2, Chapter VI | |
| DRAFT | 10-11-2014 | TNO | ALL | Final draft ; for review by VTT |
| Final | 24-11-2014 | TNO | ALL | |

# TABLE OF CONTENTS



# I. Introduction

## 1. The PREDICT project

PREDICT has the objective to provide a comprehensive solution for dealing with cascading effects in multi-sectorial crisis situations covering aspects of critical infrastructures (CI). The PREDICT solution will be composed of the following three pillars: methodologies, models, and software tools. Their integrated use will increase the awareness and understanding of cascading effects by crisis response organisations, enhance their preparedness and improve their response capability to respond in case of cascading failures.

PREDICT Work Package 3 (WP3) aims at developing a generic methodology for understanding the incident evolution and thus improving the capability to mitigate potential cascading effects.
Task 3.1 is the first task of WP3. It has the objective to develop a methodology to recognise the potential cascading effects in CI during a crisis and to assess their likelihood and extent.

## 2. Approach used

This deliverable D3.1 is the end result of task 3.1. This task builds on the results of WP2 [1], and examines the identified literature on CI, dependencies and cascading effects in more detail. The approach used to derive the end results is:

- a general analysis of lessons learned with CI incidents and cascading effects in relation to emergency response operations,
- a short description of the PREDICT case studies as a background for the development of the methodology;
- a review of the results of D2.1 [1] and its overview of existing methodologies for analysing cascading effects;
- the synthesis of existing methodologies towards the resultant PREDICT methodology.

## 3. Structure of this document

The organisation of this document is as follows:

- Chapter II provides a short introduction to CIs, their cascading effects, and their relationship with emergency response operations;
- Chapter III assesses existing methods for analysing CIs and their cascading effects. Based on this assessment, the main elements for the PREDICT methodology are derived;
- Chapter IV describes the PREDICT methodology and the steps for assessing cascading effects;
- Chapter V provides more detailed guidance on the use of the methodology;
- Chapter VII describes the way ahead towards the foresight and prediction tools, with focus on the threat specification (task 3.2), and the design of the foresight and prediction tools (WP5).

# II. Critical Infrastructures, cascading effects and emergency response

## 1. Introduction

Some infrastructures, such as electricity, transport, water management and the information and communication technologies (ICT) infrastructures, are so important for the functioning of modern societies that the disturbance of these infrastructures may have serious societal impact. Those infrastructures are generally referred to as Critical Infrastructures (CIs).
Due to the interconnectedness of CI, the risk of cascading effects exists, by which a disturbance in one CI may lead to serious disturbances in one or more other CI. This phenomenon is generally referred to as a cascading effect.
This chapter gives a short introduction to the cascading effect phenomenon and the impact that the cascading effects may have on emergency response operations.

## 2. Definitions

This document will use the following definitions (from www.cipedia.eu):

*Critical Infrastructure (CI)*
An asset, system or part thereof *{located in Member States}* which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a *{member}* state as a result of the failure to maintain those functions [2]

*Dependency*
A *dependency* is the relationship between two (CI) products or services in which one product or service is required for the generation of the other product or service [www.cipedia.eu].

*Cascading failure*
A cascading failure occurs when a disruption in one infrastructure causes the failure of a component in a second infrastructure, which subsequently causes a disruption in the second infrastructure [3]. In the rest of this document, it will also be referred to as cascading effect.

*Consequence*
In the context of CIP, consequence is defined as the outcome of an event affecting objectives [27]. The DHS lexicon [28] describes this as the harmful effects of an event, often expressed in number of deaths, injuries, and other human health impacts along with economic impacts both direct and indirect and other negative outcomes to society.

## 3. The risk of cascading effects and emergency operations

Many of the CIs are vulnerable to large scale threats such as severe storms, large scale floodings and earthquakes. Due to the interconnectedness of CIs, disturbances in one CI may lead to serious disruptions in other CIs; e.g. if electricity fails, many other CIs will be affected and may also suffer loss in their production and (downstream) supply.
During emergency response operations, it is important to take the risk of cascading failures of CI into account.

As an illustration of the importance of cascading effects for emergency response operations, we use some examples from [4]:

- In July 2001, train wagons containing chloride acid derailed in a downtown tunnel in Baltimore. Fire fighters decided to let the train burn. It was not known that a high-pressure water mains, a set of glass fibres and a power transmission cable were routed through the same tunnel. Due to the fire the water mains burst. As a result, over 70 million gallons of water flooded downtown streets and houses; the drinking water supply broke down, and the fire fighters lost their water supply. The glass fibres melted and caused a noticeable world-wide slowdown of the internet and local and international telephony outages. Over 1200 buildings lost power.
- In August 2002, the river Elbe in Germany flooded. Failures of the emergency response operations were analysed in [5]. In [4], it was analysed that not all CI specific lessons were fully understood. Some examples from [4]: emergency plans had not pre-planned that the dispatch of emergency support to the other side of the river depended on bridges that were closed to all traffic. Situational awareness of the disaster became unclear as the fixed telephony broke down because the flooding and emergency operations relied on public communication means and overloaded – often flooded – single-point-of-failure emergency communication centres. No help was given to safeguard a power generator of a hospital from flooding. This resulted in the need to evacuate 300 patients somewhat later. In the absence of plans for using public radio in emergency operations, the only way of warning people was to dispatch police cars to do that.
- Traffic congestion caused by flooding led to delay in ready-to-go resources during the response to the UK floods in 2007 [6]. There were also some near misses: had the Ulley Reservoir dam failed in 2007 and flooded in the nearby electricity substation and M1 motorway, this would have resulted in cascading failures of multiple CIs with serious consequences [7].
- The Cumbrian Floods in 2009 destroyed a bridge carrying 312 fibre optic circuits serving 40,000 people, including police and local businesses. Disruption to the transport sector due to the collapsed bridge was aggravated by the loss of communications [7].

These examples show that emergency response operations have to be aware of the CI in their area of responsibility. Emergency response operations should deal with the protection and fast recovery of the large set of CIs, to allow them to [4]:

- sustain and support the ‘static’ emergency resources, by supporting e.g. command centre(s) and operational centres of police, fire brigade, ambulance, and other emergency rescue services stations,
- sustain and support the emergency response operations deployed to the incident area in order to handle the emergency or disaster at hand, by, for example, delivering mobile communication services and water supply to fire fighters,
- support the not (yet) evacuated population in the incident area, with essential services such as, drinking water, and
- provide the continuation of providing the critical services to the area that is neighbouring the incident area, for instance a power generation station in the incident area that supports a neighbouring area.

## 4. The PREDICT case studies

Within PREDICT, three case studies will be used to analyse the impact of cascading effects in relation to emergency response operations. The three scenarios for the case studies are summarised below. Their full description can be found in Deliverable 7.1.

**Case 1: Flooding of the Alblasserwaard (Safety Region South-Holland South, the Netherlands)**

The town of Gorinchem, with about 35.000 inhabitants, is situated near the centre of the Netherlands, adjacent to the river Boven Merwede bordering the Alblasserwaard polder with its bottom level at an average of about two meters below sea level (Figure 1).


*Figure 1: Location of Gorinchem and the Alblasserwaard polder on an elevation map of the Netherlands*

In this case study, a breach develops in the dike near Gorinchem, which leads to failure of the weirs lying directly behind it. Rapidly, the water reaches heights of 2.5 meters and more in the city of Gorinchem. After an hour, the water flows into the Alblasserwaard, and after seven hours water heights rise up to 4 meters in the polder.

The water front moves to the north along both sides of the A27 motorway, to reach Lopik within 16 hours after the event, spreading gradually over the west side of the polder, flooding in the cities of Papendrecht, Alblasserwaard, Nieuw-Lekkerland, and Sliedrecht. A canal, running from Lopik to Gorinchem abates the spreading of the waterfront to the east for seven days, after which the eastern part of the polder also inundates. On the day eight, the A27 and A2 motorways, as well as the railways running in parallel to them are flooded.

**Case 2: Freight train derailment and fire (UIC)**

This case considers a derailment of a freight train on its route from Germany to Belgium. The accident is due to a sabotage of a track. It takes place in the Rheinartzkehl tunnel in Aachen, Germany. The train is loaded with chemicals and liquid gas. The coupling of the first derailed car breaks and the leading part of the train with twelve wagons derails and catches fire.

**Case 3: Maritime accident at 'Vuosaari' (Helsinki harbour)**

Vuosaari harbour is a seaport facility in Helsinki, Finland. The harbour, located in the suburb of Vuosaari in East Helsinki, handles goods traffic for the Helsinki region. Passenger services are handled in Helsinki city centre (Figure 2).


*Figure 2: Vuosaari harbour and the location where the vessel grounds*

The part of the Vuosaari fairway that is closest to the harbour is narrow, thus vessels are not allowed to meet in the last part of the fairway.
In this scenario, a container vessel 'XX' with 1000 containers arrives at Vuosaari harbour in Helsinki. The vessel contains, besides other goods, hazardous and noxious substances as cargo in several containers. The vessel 'XX' has to wait in the waiting area due to another vessel leaving the Vuosaari harbour. Due to a blackout, vessel 'XX' loses its power and the south-east wind grounds the ship on small islets at the position 60°11,0'N 025°11,9'E (Figure 2).
Due to the grounding, a crew member is injured, a fuel oil leak occurs (it is unclear how much oil is leaked into the sea but it drifts towards the Vuosaari fairway), two containers were lost and one was damaged. In the beginning it is unclear which containers dropped into the sea (unknown material with a possible risk to population, rescuers and environment).
The damaged container leaks phosphoric acid. The phosphoric acid reacts with aluminium, which results in a hydrogen gas cloud, possibly explosive, as well as irritating vapours. Some members of the crew have been affected by the hydrogen gas and need to be evacuated; they require immediate medical care. The wind shifts from south-east towards east, transporting the cloud towards densely populated areas in eastern Helsinki. Due to the traffic stopping and the gas cloud this scenario has a high economical and human impact.

# III. Existing methods for identifying and assessing cascading effects

## 1. Introduction

This chapter builds on the results of the deliverable D2.1 [1] which are itemised in Section III.2. Then this chapter describes some existing methods to analyse cascading effects. The methods were identified in the state of the art overview in D2.1.

The following methodologies are described:
- modelling all aspects of CI dependencies [10],
- empirical evidence on cascading effects [8],
- the Input-output Inoperability Method (IIM) [12].

In addition to these methodologies, two additional methodologies from earlier EU projects are studied:
- Floodprobe [14],
- CRISMA[13].

## 2. Observations and recommendations from PREDICT D2.1 [1]

The PREDICT methodology to be developed has the objective to support decision making in crisis situations by: identifying threats, identifying CI, specifying the plausible cascading effects and their likelihood. D2.1 states the following requirement for the analysis of cascading effects [1]
- ***MF3*** *(Critical infrastructures' dependency); this functionality (MF3) could be considered as an underlying one. It is a sort of a permanent input for all crisis management DSS. It can be extended to new CI members and can be periodically updated. Each EU CI will be described by its main functionalities. Then, the main functionality will be described by the main subsystems necessary for its realisation. The logical stream is CI → main functionalities → main subsystems. The dependence between two CI can be described as: strong, moderate or weak.*

In order to predict possible cascading effects, to control failures propagation, and to minimise undesirable consequences of perturbations of the systems, several complex factors have to be taken into account. D2.1 states that the following factors are important to consider [1]:
- dependencies among system components,
- possible consequences of cascading effects,
- risk of various hazardous phenomena occurrence,
- available means and resources,
- human behaviour,
- financial costs or time duration.

This deliverable (D3.1) focusses on the first two aspects: the dependencies between the CI and the cascading effects. D2.1 also stresses some aspects that are important to take into account for the modelling of the dependencies and the cascading effects:
- **the dynamic aspects** of CI dependencies: D2.1 states that the models should enable us to consider different operating phases, namely: decay (disruption of the function/service) and recovery (recuperation of the function/service) [1].

Introducing dynamic aspects when describing the cascading failures is necessary, although it is not an easy task. Many issues should be addressed before developing fully-dynamic descriptions for cascading failures and their propagation. One of the most problematic issues is the failure occurrence rate of the components within the threatened system. The failure rate of a component may vary as a function of the system in which the component is integrated. It varies as a function of the threat itself, as well.
The second problematic issue is the way to describe the dependency between different components of the same system and different components of different systems facing the same threat.
However, considering the current lack of adequate numerical data describing the likelihood of the components' failure occurrence, we recommend to start with a qualitative description, which includes:

- Threat occurrence likelihood & activation/duration time: these are very important inputs and will be used as references for the following concepts.
- Component resistance time: this concept describes how long a given component can withstand a given threat intensity before losing its functionality. The resistance time can then be short, medium or long with respect to the threat duration time.
- Component downtime: this is the time necessary to repair/replace a failed component within a given system in the presence of a given threat. Again it can be short, medium or long with respect to the reference time which is the "threat duration time".
- Component back-to-service time: this is the time necessary for the component to re-integrate in its parent system and the system to be back to effective service. Again, it can be short, medium or long with respect to the "threat duration time".

To develop a real quantitative dynamic description is a very complicated issue, which may not be fulfilled in the near future. Using a qualitative metric such as "short, medium and long" to describe the dynamic behaviour of a given failure would be a practical first step to introduce the dynamic aspect in describing cascading failures.

## 3. Modelling all aspects of CI dependencies [10]

In describing the status of CI, many models use a two-state approach: the CI is either available and fully-functional, or it is not available. As [10] outlines, CI states and dependencies are more complex. That paper focuses on one of the main shortcomings in the modelling of CI dependencies: The lack of support for modelling of essential real-world factors: quality factors of CI products and services (other than just on/off availability), process states, and environmental factors.
The model is based on a system analysis approach and views a CI as a system, supporting a process. It provides a classification of the elements and factors that must be considered to completely describe the behaviour of CI dependencies. There are 'quality' and 'response' elements that describe dependencies, along with the 'state of operation', and the 'environmental' factors that influence dependencies. This will be clarified hereafter:

- *Quality elements:* dependencies of CI products or services are characterised by more than just the on/off availability. CI products and services that are an input to a CI process also need to adhere to certain levels of quality: quantity/volume (of food, water or power), speed (of transport or information services), reliability (of information), temperature (of heating or cooling water), pressure (of gas or drinking water supply), frequency/voltage (of electrical power) and biological and chemical purity (of food, drinking water, surface water or chemicals). All these quality elements can be important when describing dependencies, as they might represent essential preconditions for the usability of the service/product by their customers.

- *Response elements:* the response function depends on the input of products and services and on time. Two types of input response are distinguished: functional behaviour how the CI output and dependency are related when either the dependency supply deteriorates, and the behaviour when the dependency supply recovers. There are four aspects of time response: 1) the time period between the moment of change in inputs and the moment when the change in output is noticeable as disturbed or unavailable, 2) the extent to which the output changes as a function of time, 3) the differential aspect of dependencies, and 4) the integrating aspect of dependencies.
- *State of operation factors:* there are four states of operation that influence a dependency: normal state, stressed state, crisis state and recovery state. The important issue is to recognise that the set of dependencies may (largely) shift between these states. It is, however, important that all dependencies in all states of operation are considered in the overall analysis, and for each specific mode of operation in the right temporal timeframe.
- *Environmental factors:* certain environmental factors that are outside the scope of a CI can influence dependencies. These factors can worsen or alleviate dependencies, change the response of the system to dependencies or even create new dependencies.

Having identified the elements of CI dependencies, it is possible to model the relationships between these elements. This model consists of a formula in the form of $\overline{O}_{j,1..m} = f_{s,e}(\overline{I}_{1..n}, t)$, which is typically a large set of functions.

**Relevance for the PREDICT methodology**

From this paper [10], the following elements can be identified:

- Modelling different aspects of CI products and services, process states and environmental factors are essential to describe real-world CI behaviour. These consist of:
  - Quality elements,
  - Response elements,
  - Modes of operation,
  - Environmental factors.
- A mathematical representation of describing the dependency relations is provided.
- One of the important factors to take into account for crisis response operations is the mode of operation (Figure 3). For instance, when an organisation enters a stressed mode of operations, e.g. due to the failure of a CI, a completely different set of CI dependencies can be recognised. Empirical evidence (e.g., from [4]) shows that CI operators and emergency response planning mostly understand and plan mitigations for disruptions of a CI one is depending upon for the *normal mode of operation*. However, it is much harder to understand and prepare for CI dependencies which occur in the non-normal modes of operations..

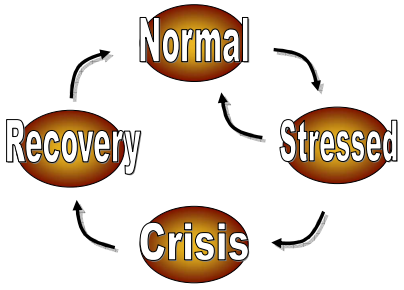



*Figure 3: Modes of CI operation*

Shifting dependencies with changes in mode of operation, and the need to plan for operation in other modes, can be illustrated by the example of a hospital losing power. In case of a power

failure, normal operation is immediately replaced by a stressed mode of operation in which power is delivered by a local diesel generator and hospital services can be continued with only minor deterioration. We see that the hospital is dependent on the power supply in normal operation, and is dependent on diesel supply in the stressed mode. To prevent getting into the crisis mode (no electricity available), the hospital should plan for supply of diesel fuel in a stressed situation, and plan for the fact that for example fuel pumping stations will not work if electricity has failed there also, that the power failure could result in traffic obstructions by closed railway crossings or open bridges, et cetera.

## 4. Empirical evidence on cascading failures across CI [8]

This paper describes an analysis of data from TNO's Critical Infrastructure Incident Database (CIID). This database is a daily-maintained database, collecting information about CI disruptions, common cause events, and cascading effects, gathered from public media. Only incidents that have some wider relevance are included, based on criteria such as whether it is a CI disruption and it does meet one of the impact threshold criteria (number of people affected, damages, environmental impact). For example, only power outages which affect at least 10.000 customers are included.
For each recorded incident in the database, the following data is recorded per affected CI service: the CI sector, the affected CI service, the initiating event (if any), its dependency of another affected CI service, whether the cause was a common cause event, the concerned organisation, start time and date, end/recovery time and date, country, geographic area within country, size of affected area, a textual description of cause, the threat category and subcategory, an indication of the consequences, the duration and progress of recovery, and reference(s) to (web) source(s).

This paper contains a thorough analysis of the data in the database: The paper raises several important issues:

- Cascades occur in fact fairly frequent. Cascading failures are at once more banal and more frequent than often envisioned. This stands in contrast to the theory that cascades are events of low probability and high consequence.
- The cascades are highly asymmetrical (originating in few sectors and affecting other sectors) and narrowly focused on particular sectors. While there are an almost unlimited number of dependencies and interdependencies among infrastructures possible – that is, there are many pathways along which failures could propagate across sector boundaries – it was found that this potential for cascades is not expressed in the empirical data on actual events. The overwhelming majority of cascades originate in the energy and telecommunication sectors.
- Few cascades take place outside of these pathways. Standing in stark contrast to the theory regarding an intricate web of dependencies, it was found that **inter**dependencies rarely appear to be strong enough to trigger a reported serious outage.

**Relevance for the PREDICT methodology**

- The analysis shows which of the CI-sectors are most involved in cascading effects (Figure 4). It shows both the sectors that are mostly involved as initiating sector and the sectors that mostly suffer from cascading effects. These statistics may be used as a basis for prioritisation of sectors to include in the method.
- For commonly occurring cascades, the Energy and Telecom sectors cause 85% of all cascades;
- The Energy, Telecom and Transport sectors are sectors frequently affected by cascading effects;

- Commonly occurring cascades seldom exceed two or three steps of depth[1].

| | | *Initiating sector* | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | *Energy* | *Financial services* | *Government* | *Health* | *Industry* | *Internet* | *Food and postal services* | *Telecommunications* | *Transport* | *Water* | *Sample size* |
| *Affected sector* | *Education* | 33% | | | | | | | | | 67% | 3 |
| | *Energy* | 89% | | | | 4% | | | 2% | 1% | 3% | 93 |
| | *Financial services* | 18% | 18% | | | | 9% | | 55% | | | 33 |
| | *Food* | 38% | | | | 36% | | 13% | | 13% | | 8 |
| | *Government* | 42% | | 2% | 2% | 2% | 9% | | 37% | 2% | 2% | 43 |
| | *Health* | 65% | | | 12% | | | | 18% | | 6% | 17 |
| | *Industry* | 80% | | | | 7% | | | | 7% | 7% | 15 |
| | *Internet* | 24% | | | | | 23% | | 53% | | | 79 |
| | *Postal services* | | | | | | | | | | | 0 |
| | *Telecom* | 49% | | | | 1% | 1% | | 46% | 4% | | 155 |
| | *Transport* | 79% | | 1% | | 2% | | 1% | 5% | 10% | 3% | 150 |
| | Water | 68% | | | | 20% | | | | | 12% | 25 |
| | Total | *59%* | 1% | 0% | 0% | *3%* | *4%* | 0% | *26%* | *4%* | *3%* | *621* |

*Figure 4: Percentages of cascades initiated in a sector (from [8])*

## 5. The Input–output Inoperability Model [12]

The Input-output Inoperability Model (IIM) is commonly used in economics to assess the strength of relationships between actors as a function of financial data. The criterion used to determine relational strength is most commonly derived from economic relations (financial transaction between two parties). As this criterion focuses on only one perspective, Setola et al. [12] proposes to change this parameter with technical and operational data applied to CI sectors. Every essential field is modelled as a consumer of the other field's products or services. Indeed operators know much better on which sectors they are dependent than knowing the sectors that depend on own products

[1] That is, insofar it is observable and reported by the press. The fact that a specific maintenance engineer is delayed and hampered by the lack of a working mobile telephone is a dependency which stays unnoticed at the system (of systems) disruption level.

([11], [16]). The quantitative values for this IIM analyses are elicited in expert interviews. Specialists described the influence of the outage of all other CI fields on the operability of their own field. Data uncertainty is incorporated by using fuzzy numbers. Five outage time scenarios are studied: less than 1 h; 1 to 6 h; 6 to 12 h; 12 to 24 h; and 24 to 48 h.
This method has been applied to an Italian Infrastructure case study. It allowed to confirm the evidence that the degree of dependence is related to/ is a function of the outage time. The same conclusion holds when one plots the influence gains of each sector as a function of time. As expected, the electricity and telecommunication sectors represent the more influencing parameters. Based on these qualitative parameters, this paper builds the influence matrix A for modelling direct inoperability transmission. In this model, the vector x(i) corresponds to the inoperability of the sector i. (x(i) = 0 means the sector works well). This paper assumes that **the restoration process is neglected**. The inoperability transmission could be modelled with this very simple matrix equation:

$$X(k+1)= A \cdot x(k) + c$$

in which the vector c corresponds to the inoperability vector, representing external failures/events. The mathematical conditions are not detailed here.

This methodology also proposes a few matrix operations to transform the first order dependency matrix A into a higher order dependency matrix. This allows us to calculate the cascade of the inoperability transmission through the system – without considering any recovery mechanisms.

**Relevance for the PREDICT methodology**

- Dependency is a function of outage time (change of state of operation);
- IIM provides a simple way to model linear dependencies and calculate first and higher order dependencies;
- For the PREDICT project, this paper highlights the fact that dependency factors between CI are not constant during the crisis but shift with the duration of the crisis;
- IIM enables ranking dependencies according to their strength;
- Moreover, expert interviews and use of fuzzy numbers could be employed when statistical data are not available or not precise or reliable enough to assess the links strength.

## 6. FloodProBE [14]

FloodProBE is an EU project that aims to provide cost-effective means for flood risk reduction in urban areas [14]. One of the elements in FloodProBE is the development of a method for risk assessment of CI for flooding based on an existing methodology and software tools for risk and vulnerability assessment. To this end, a computer-based analysis tool has been developed. In this tool, the user provides frequencies of occurrence of thirteen threat events. Vulnerability is assessed by checking or unchecking relevance of these threat events for six types of categories: people, environment, and infrastructure (water network, transportation, electricity network, telecommunications). No input is required for impact.
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 geographical region. The outputs are presented as several matrices that can be compared to each other that allows visualising the risk events for which action must/ should be taken.

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

- Identify hazardous events and undesired technical defects (also called barrier failures);
- Perform frequency and consequence analysis;
- Assess the potential risk;
- Evaluate the risk according to the selected risk acceptance criteria, and then planning for adaptation and mitigation measures.

**Relevance for the PREDICT methodology**

- Vulnerability is calculated with regards to people, environment, and infrastructure (water network, transportation, electricity network, telecommunications);
- The method is based on a simple algorithm;
- The risk categories might be re-used for PREDICT.

## 7. CRISMA [13]

CRISMA is an EU project that aims to develop a simulation-based decision support system, for modelling crisis management, improved action and preparedness [13]. The CRISMA System aims to facilitate simulation and modelling of realistic crisis scenarios, possible response actions, and the impacts of crisis depending on both the external factors driving the crisis development and the various actions of the crisis management team.
One of the elements of the CRISMA project is the development of a method for time-dependent vulnerabilities of elements at risk.

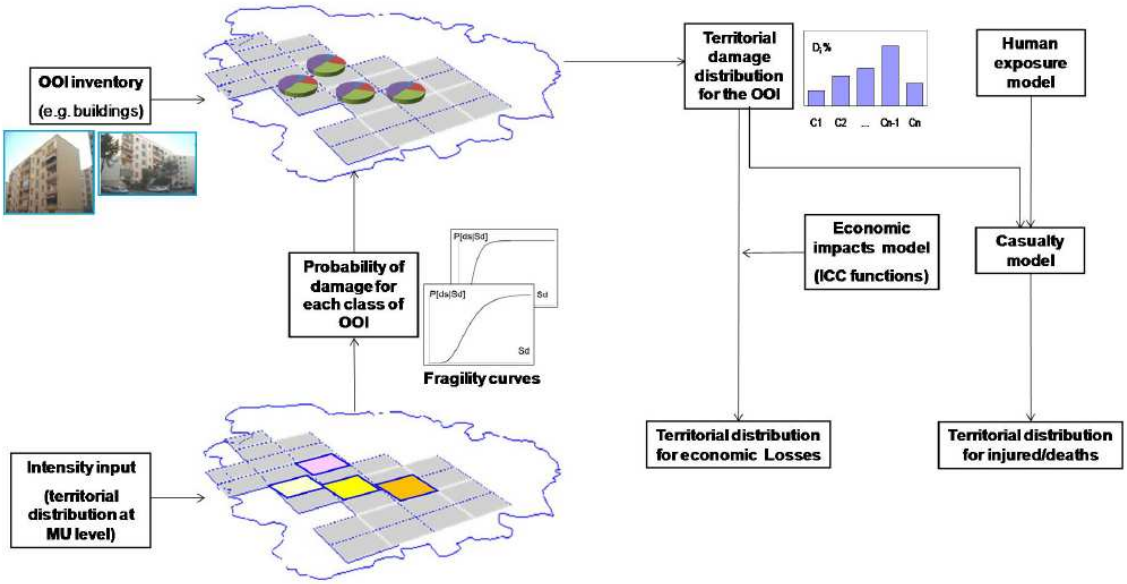



*Figure 5: The relationship of models and data needed for the assessment of an impact scenario [13]*

Figure 5 illustrates the approach used, to assess the impact.

The main elements include:

- the object of interest (OOI) inventory;

- the intensity input;
- the probability of damage for each class of OOI.

Although CRISMA is not focussed on CI specifically, part of the approach can be reused as part of the PREDICT methodology.

**Relevance for the PREDICT methodology**

- The CRISMA methodology might be useful to assess the first order impact on CI.
- The CRISMA methodology for time-dependent vulnerability does not specifically take into account the concept of cascading effects.
- In order to be useful for PREDICT, the CRISMA methodology should be adapted to CI.
    - The OOI inventory can be used to include CI nodes;
    - The intensity input could reflect the threat modelling (PREDICT task 3.2);
    - The probability of damage could be part of the assessment of the first order impact of CI disturbances;

## 8. Conclusions on the PREDICT methodology

The PREDICT methodology has the objective to support decision making in crisis situations by identifying CI, the possible cascading paths and their probability, and the temporal and spatial effects in the specific crisis situation.
Based on the methodologies described above, the following conclusions can be made:

- In order to identify cascading effects, the CI in the affected region should be described by its main functionality, its main elements, and dependencies with other CI;
- The risk of cascading effects depends on the **vulnerability of the CI nodes** to the threat involved, and on the **dependencies** between the CIs;
- The vulnerability of the CI nodes must be described. Note that this vulnerability depends on:
    - characteristics of the threat;
    - characteristics of the node.
- The dependencies between the CIs are important for assessing the cascading effects. These dependencies may depend on the following parameters
    - characteristics of the link between the CI nodes (e.g., vulnerability to external threat, disruption and recovery characteristics, mean-time-to-repair under the condition, other modalities which may take up some of the disrupted service);
    - the mode of operation (normal, stressed, crisis, recovery);
    - external conditions (weather, time of the year, time of the day, …).

# IV. The PREDICT methodology for identifying and assessing cascading effects and their probability

Chapter III discussed some existing methodologies for identifying CI and analysing cascading effects in CI. In this chapter the main elements of these methodologies are synthesised into the proposed seven steps of the PREDICT methodology for assessing cascading effects.

The methodology described in this chapter consists of the following steps:
1. Identify the threats to be considered;
2. Identify the CI in the region;
3. Identify the key CI elements;
4. Characterise the vulnerability of the key CI elements to the threat;
5. Assess the first order impact of the threat on the CI elements;
6. Describe the dependencies between the CI elements in the region;
    - o describe the required input and output of all key CI elements;
    - o distinguish between the different modes of operation;
    - o include the temporal and spatial factors;
7. Assess the CI cascading effects.

Please note that the steps described in this chapter focus on the steps that relate to the assessment of cascading effects. The overall PREDICT methodology will consist of more steps and modules and for instance include threat modelling, environment modelling, and other forecast and prediction tools (chapter VI).
In order to illustrate the main steps of the PREDICT methodology for assessing cascading effects, a scenario of a large scale flooding is used as an example. The description of this example is based on reports of lessons learned from earlier incidents, including the Pitt review [6] and the von Kirchbach report [5].

## 1. Step 1: Identify the threats to be considered

The assessment of the risk of cascading effects starts with the assessment of the threat(s) to be analysed, e.g., an earthquake or a large scale flooding. The modelling of such threats will be part of task 3.2. Section 2 of Chapter VI will discuss the threat modelling in more detail.
The output of this step will include:
- an assessment of the region that is threatened;
- an overview of the time factors, when the threat will occur;
- an overview of the affected area;
- an assessment of the severity of the threat.

**Illustration of this step**
A region in the Netherlands is threatened by large scale flooding. The description of the threat may cover aspects such as:
- *Geographical data:* which areas are at risk to be flooded, or are flooded and what is the severity? For this, inundation maps play an important role;

- *Time factors*, e.g. the warning time, the time that elapses until the peak depth of the flooding of a low area is reached, the expected water crest movement, and the duration of the inundation;
- *Data on the severity of the flooding*. These include:
  - depth,
  - water flow rate,
  - level of biological or chemical contamination.

An illustration is presented in Figure 6

.

This type of threat modelling is part of task 3.2.

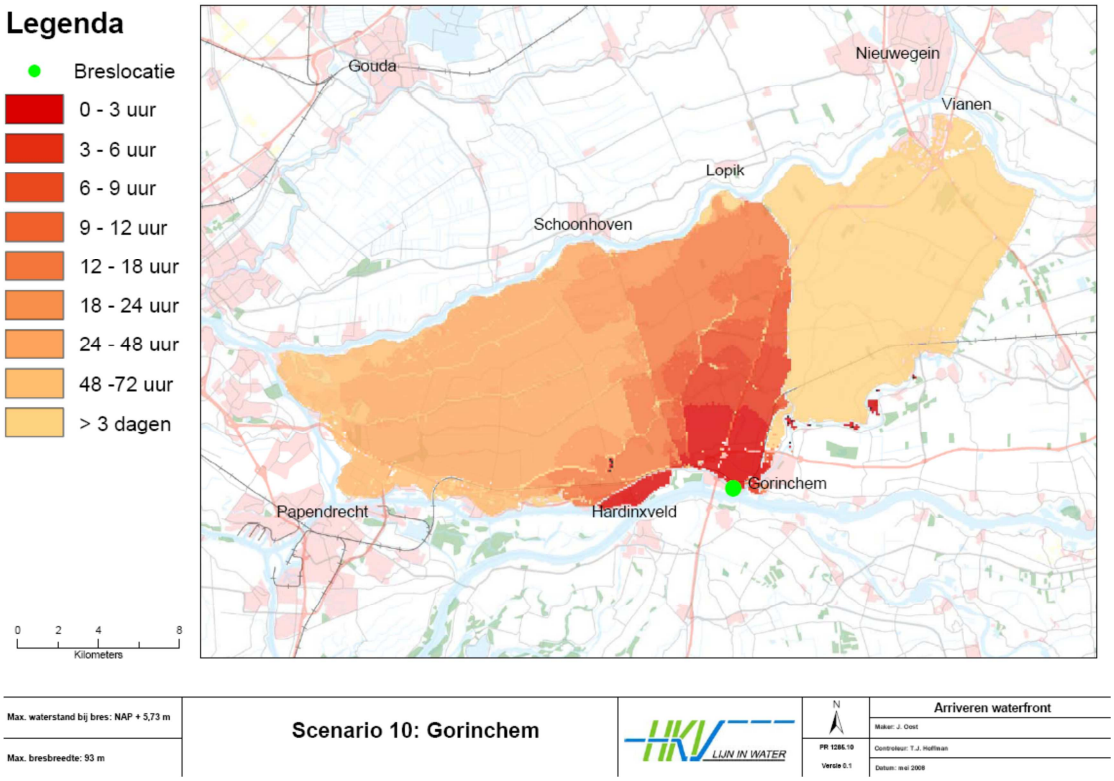



*Figure 6 : Timeline for movement of waterfront*

## 2. Step 2: Identify the CI in the region

Once the region that is threatened is known, the second step is to identify the most important CI within that region. In identifying the relevant CI and CI nodes, the following perspectives can be used:

- the CI that are essential to the life-support of the population within the affected region, e.g. electricity, transport, drinking water, communication, food, health, financial services;
- the CI that can pose a risk to the population or emergency response within or outside the affected area when compromised, e.g. chemical plants or storage facilities;
- the CI that directly support the emergency response operations, e.g. energy, communication and transport for emergency services;
- the CI which has a footprint in the region, not directly of use to the region, but essential to the population outside the region such as the nation, cross-border region or adjacent region(s).

The set of CI that are essential may **shift** during the different phases of the threat. Before the flooding reaches a specific region, transport will be an important CI in order to evacuate part of the population. When the flood has reached the area, distribution of food and drinking water will become important.

**Illustration of this step**
Based on lessons learned of earlier incidents, checklists and analysis of the threat, the relevant CI can be identified. Some of the CIs that may be vulnerable to flooding and are relevant for emergency operations include:

- infrastructures in support of the emergency operations, including police and ambulance stations; fire stations and (local) command centres; command and control systems in support of emergency operations.
- essential transport infrastructure, including roads as well as railways and shipping in specific cases. This may be an important factor for emergency response operations since these infrastructures may also be needed for mass evacuation routes;
- the energy infrastructure, including nodes of the electricity and gas infrastructures and distribution system, as well as fuel for transport, emergency generators, heating and cooking;
- drinking water infrastructure (non-evacuated, evacuated and emergency operations personnel);
- the ICT infrastructure, including fixed and mobile communication carrying voice, video and data;
- water management infrastructure;
- food services (non-evacuated, evacuated and emergency operations personnel);
- financial infrastructure, e.g., Automated Teller Machines (ATM);
- healthcare infrastructure, including hospitals, medicine supply chain and transport for dead and wounded;
- facilities with hazardous material, e.g. chemical plants.

## 3. Step 3: Identify the key CI elements

For each of the relevant CIs that are identified in step 2, the key CI elements are described. This step includes the identification of the most relevant CI elements (objects, services), within the region and near the region. The criteria for identification of the most critical elements are similar to the criteria used in step 2:

- the CI elements essential for the CI to function properly;
- the CI elements that are in direct support to sustaining life of the population within the affected region;
- the CI elements that can pose a risk to the population within or outside the affected area when compromised;
- the CI elements that are in direct support to the emergency response operations in the region;
- the CI elements that are essential to the population outside the region.

**Illustration of this step**
This includes for instance the identification of the substations for the electricity networks, the mobile phone masts, relay stations and switches for mobile and emergency communication, key food distribution centres, and roads for transport of goods and people (Figure 7).

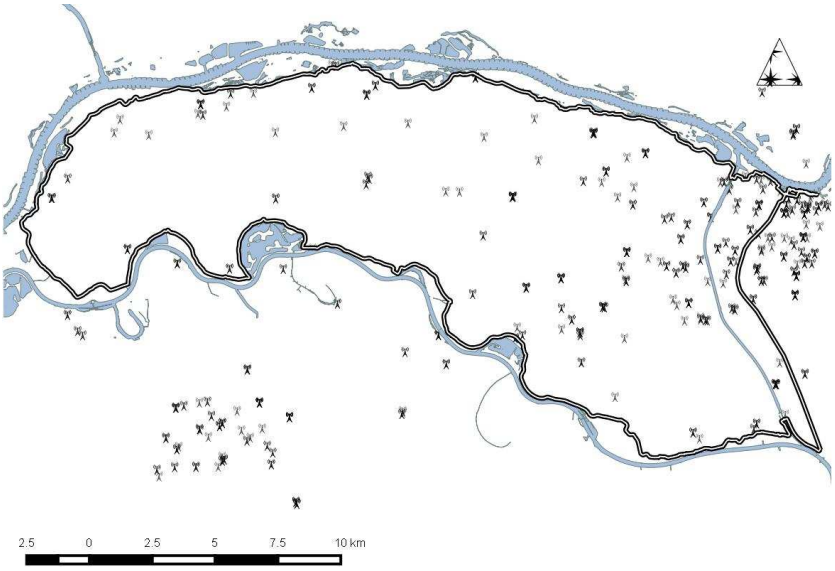



*Figure 7: An overview of the mobile phone masts in a region as an example of the identification of CI nodes within the region*

## 4. Step 4: Characterise the vulnerability of the key CI elements for the threat

For each of the key CI elements identified in Step 3, and the threat(s) identified in Step 1, the vulnerability of the key CI elements can be analysed. This includes e.g., an assessment whether the CI element is vulnerable for a storm or for flooding. In general, the vulnerability depends on the type of asset, the type of threat, and the severity and duration of the threat.
One way to model this vulnerability is shown by the EU project CRISMA, which uses the concept of a Damage Probability Matrix (DPM). The DPM represents for a given element class, the conditional probability of obtaining a damage level k, due to an event of intensity I [13] (Figure 8).

**Table 2. Generic scheme of damage probability Matrix for Elements of Class T.**

| Intensity | Damage Level | | | | | |
|---|---|---|---|---|---|---|
| | 0 | 1 | ... | $D_k$ | .... | $D_{kmax}$ |
| ... | % | % | % | % | % | % |
| ... | % | % | % | % | % | % |
| I | % | % | % | $P[D_k\|I,T]$ | % | % |
| ... | % | % | % | % | % | % |
| $I_{max}$ | % | % | % | % | % | % |

*Figure 8: The use of DPM in the EU project CRISMA [13]*

**Illustration of this step**
In case of a large scale flooding, for each type of key CI element the vulnerability must be assessed. In general, this vulnerability will depend on e.g., the water depths and the water flow rate.
As an example, we include the assessment of the vulnerability of the Dutch electricity sector in the recent Deltaprogramma [15]. In general, the power transmission system is less vulnerable than the elements of the power distribution system. At a water depth of more than 2.5 meter, the power transmission system may fail. At regions with a depth less than 0.5 meter, the disruption of the power transmission system in the inundated region is less likely.

A more detailed example of a vulnerability matrix is a Damage Probability Matrix that models the vulnerability of a specific type of building for a seismic event [13].

## 5. Step 5: Assess the first order impact of the threat to the CI elements

Based on the vulnerability of the node, and the severity of the threat, an assessment can be made on the first order impact for each CI element. This assessment of first order effects will indicate which critical services will be disturbed by the threat and what the impact will be. For instance, this could include the assessment of the amount of people that are in danger or the effect of the CI disruption expressed in households or customers who will suffer the loss of electricity when a specific substation stops operating.
In order to perform this step, two sub-steps can be discerned:

- Determining the vulnerability of the CI elements impacted by the threat. In this step, the CI elements that are likely to be compromised by the threat are determined. If tdata is available to do so, this can include an expected time-sequence of failure.
- Determining the types and extent of societal effects of impacted CI elements. In this step, the effects of failure of individual CI elements on society are determined. These effects include all negative impacts that are deemed relevant to the model, which can include deaths, wounded, financial, physical, ecological, mental and intangible damages, etc. Impacts to other infrastructures through dependencies are accounted for in a later step, and are therefore excluded from this step.

**Illustration of this step**
The 2007 floods in the United Kingdom showed the vulnerability of CI to flooding:

> In summer 2007 major flooding again caused widespread and sustained power interruptions across the Yorkshire operating area. Supplies to around 130,000 customers were interrupted and flooding occurred at 4 of Northern Powergrid's major substations with substantial damage occurring at 55 Yorkshire secondary substations. Around 110 HV[2] faults and 536 LV faults were recorded where we would normally expect around 14 HV and 80 LV faults over a similar period of time. The company's Gelderd Road control centre in Leeds had to be evacuated and the National Grid, Grid Supply Point (GSP) at Neepsend was flooded and ceased to provide an in-feed to Yorkshire's distribution network which resulted in rota disconnection being implemented. The final cost of recovery from this incident was approximately £6m with the highest cost to restore an EHV substation being approximately £150,000 for Rawmarsh Road.
>
> *IMP/001/012 – Code of Practice for Flood Mitigation at Operational Premises, Mar 2012*

> It was only by a whisker that 500,000 inhabitants of Gloucestershire and south Wales, and 750,000 people around Sheffield did not lose power due to flooding the electricity substation serving their homes. As the Pitt review noted, a power failure on that scale in either region would have almost certainly caused loss of life.
>
> As it was, the flooding of the Mythe water treatment works in Gloucestershire meant 350,000 people were without fresh water for up to two weeks, 40,000 had no power for 24 hours in Gloucestershire and 9,000 were on rota disconnection in South Yorkshire and Humberside. It was a wake-up call for the utilities industry.
> *The Guardian, Tuesday 16 September 2008.*

[2] HV = high voltage; MV= medium voltage; LV= low voltage

## 6. Step 6: Describe the dependencies between the CI elements in the region

The disruption to the CI nodes as assessed in Step 5, may lead to cascading effects due to dependencies.
These dependencies generally depend on the mode of operations, e.g. when electricity is disrupted and emergency power units are used, a new dependence develops on the supply of diesel.
The dependencies may be modelled by the functions proposed in [10], or in the IIM model [12].
Based on the analysis in Chapter III, the following factors are of importance to include:

- the mode of operation,
- the temporal effects (e.g., the time that a mobile mast will function based on battery power, disruption and recovery characteristics[3]).

**Illustration of this step**
As an example of the dependencies and the shift in dependencies due to time factors or modes of operation:

- When there is a power outage, the masts for mobile communication will stop functioning after x hours.
- When there is no electricity available, the hospital will first use an emergency power unit. After y hours, diesel is needed to keep on functioning.
- When after a power disruption, the power for pressurising drinking water is supplied again, the pressurising process may take p time before the whole area sees an initial flow of water from the tap and q time before a normal pressure level is achieved.

## 7. Step 7: Assess the CI cascading effects

Based on the dependencies between the CI, established in step 6, and the CI elements directly impacted by the threat(s), established in step 5, the CI cascading effects can be determined (Figure 9). Including quality and quantity requirements in dependency descriptions will yield more realistic results. However, to simplify the model or provide a worst-case analysis, a simple on/off description of dependencies might suffice.

This analysis provides the basis for the estimated probability and extent of cascading effects.

**Illustration of this step**
During the UK floodings in 2007, a substation was shut down with a loss of electricity to 400.000 people. The loss of electricity caused water discharging pumps to stop working, leading to increased flooding.

[3] E.g., a power blackout takes less than seconds; recovery is a stepwise balancing process which may take hours or even days.

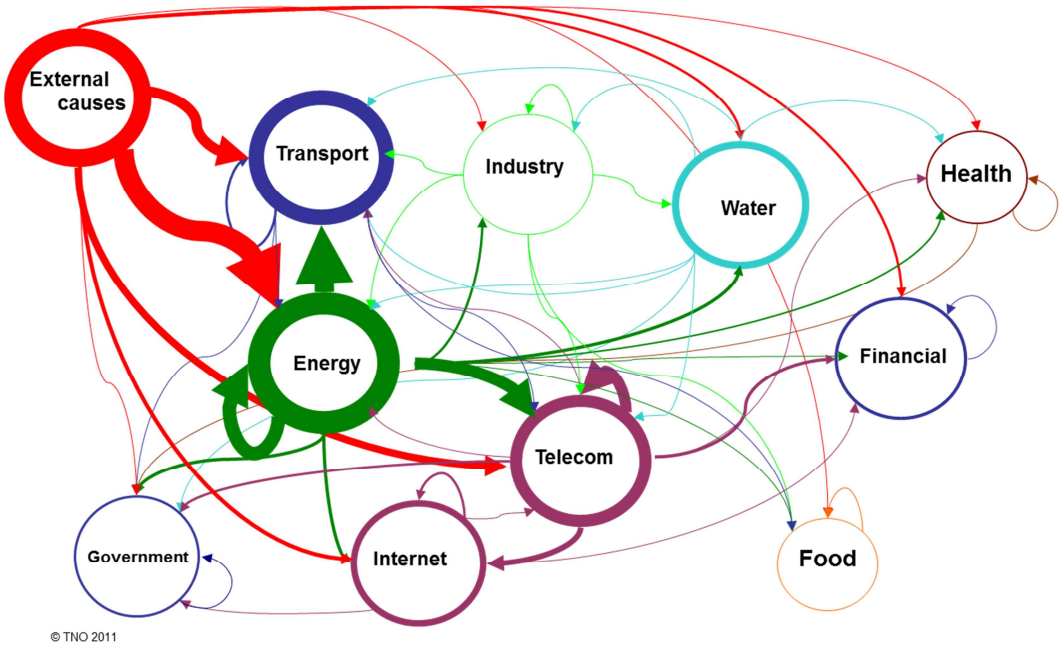



*Figure 9: An example of CI dependencies based on an analysis of the CIID in [8]*

## 8. Summary of the main steps of the PREDICT methodology

The methodology described in this chapter consists of the following steps:

1. Identify the threats to be considered;
2. Identify the CI in the region;
3. Identify the key CI elements;
4. Characterise the vulnerability of the key CI elements to the threat;
5. Assess the first order impact of the threat on the CI elements;
6. Describe the dependencies between the CI elements in the region;
    - o describe the required input and output of all key CI elements;
    - o distinguish between the different modes of operation;
    - o include the temporal and spatial factors;
7. Assess the CI cascading effects.

Each of these steps may be performed either in great detail, or by a more qualitative approach. In order for the methodology to be useful, please note that the desired and attainable level of detail is determined in an iterative process in which:

- the use and desired output of the model is described;
- the need for and availability of input/information is determined to reach this level of detail;
- the feasibility of such a model is evaluated and the requirements for use and level of detail are adjusted if needed.

Experience shows that it may be hard to obtain detailed quantitative data for each of the steps of the methodology. Therefore it would be wise to develop both a qualitative and a quantitative approach or a mixed mode approach, to provide for those situations where reliable quantitative data is scarce. This will allow the end user to choose between the two approaches, based on his preferences or on the data that is available.

# V. Practical guidance for using the methodology

## 1. Introduction

In this chapter, we shall outline some general and practical background to support the steps described in the previous chapter. As most information for executing the methodology will be case-dependent, we shall limit ourselves to describing some initial data that can be used as a starting point for collecting more case-specific data.

## 2. Guidance on the level of detail from WP2

From a scientific perspective, the recommended level of detail would be: “as detailed as possible”. However, in the current context the recommendation about the required level of the details would be: “as micro as achievable” or (exclusively) “as macro as acceptable”. The current state-of-knowledge is characterised by:

- *Threat identification & specification:* threats are not all at the same advanced level of understanding, definition and specification. Some are specified by their intrinsic properties (waves height, wind speed, quantity of ejected magma, quantity of energy released). Some others are specified by their impacts (eco-systems degradation, number of buildings destroyed, number of injuries and fatalities, etc.). Some are specified using quantitative metrics while others use qualitative metrics.
- *CI responses*: CI failures induced by a given threat are not systematically identified or specified. And even worse, there are almost no databases containing the CI downtime as a function of the degradation type and the degradation level of CI.
- *CI dependencies:* although experts can qualitatively assess limited sets of dependencies between a few CI, systematic database generation about CI dependencies per threat are inexistent.
- *Dynamic data:* the existing CI failures data (failure modes, mechanisms, occurrence likelihood, downtime, etc.) do neither allow the development nor the use of real dynamic resilience models.
- *Metrics:* the state of development of metrics to measure threats (magnitude, intensity, likelihood) is not sufficient enough for them to be systematically used in CI resilience modelling, simulation and analysis.

## 3. Guidance based on the use cases in WP7

From the end user perspective a different approach can be derived. Here the recommended level of detail can be described as: “as detailed as necessary to make the right crisis management decision”. From this perspective, it is not always necessary to use detailed models and information. Each of the steps may be executed either in great detail, or by a more qualitative approach. In executing the methods and models, the reliability and level of detail achieved in previous steps should always be considered when deciding on the level of detail for a subsequent step. The right level of detail for a specific scenario can only be determined on a case by case basis, using an iterative process to determine the desired and attainable level of detail.

Experience also shows that the attainable level of detail may be limited because it might be hard to obtain detailed quantitative data for each of the steps of the methodology.

## 4. Threat taxonomy

The threats that can potentially be considered are manifold. In D2.1, taxonomy is presented listing threats that can harm CI [17]. This taxonomy can be used to select the threats taken into account for the analysis. An abbreviated and simplified version of this taxonomy is included below in Table 1.

*Table 1: Simplified threat taxonomy*

| | | |
|---|---|---|
| **Natural** | **Geological** | **Earthquake, landslide, volcanic activity, subsidence, erosion** |
| | Air | High wind speed, absence of wind, high air temperature, low air temperature, high air humidity, low air humidity |
| | Precipitation | Snow, hail, rain, fog |
| | Water | High water levels, low water levels, high flow rates, low flow rates, high water temperature, low water temperature |
| | Space | Meteorite impact, comet shock wave / collision |
| | Radiation | Electro-magnetic storm, earth-magnetic change, natural nuclear radiation, sun radiation bursts, cosmic high-energy particles |
| | Fire | Heat, smoke, toxic gases |
| | Biological | Vegetation threats, bacterial threats, viral threats, animal threats, prion threats, fungal threats |
| **Man-made** | Ecological | Soil contamination, air contamination, water contamination, troposphere contamination |
| | Economical | Diminishing stature, sale barriers, instable banking/ economy, organisational problems, legal problems, disruption of conditional goods or services (dependency) |
| | Societal | Civil disorder/ riots insurrections, political crises, strike / labour unrest, mass migration |
| | Personal | Lapse of attention, incompetence / training, missing or wrong Information / communication, organisational structure, criminal intent, epidemic illness |
| | Technical/technological | Force, fire, chemical, electro-magnetic, hardware, ICT |
| | Dependencies | Energy , ICT, water, food, health, financial, public & legal order and safety, civil administration, transport, chemical and nuclear industry, space and research |

Note that the PREDICT cases may combine several threat types.

If the identification and probability assessment is done as part of a service analysing the potential ways along which an actual event may develop, the threats to be considered should at least contain the set of threats that shaped the event. Possible other threats have to be considered as well, as they could influence the chain of events. For instance, flooding due to excessive precipitation might have caused an incident, but high winds for example might exacerbate the situation, even if they are not at the root of the incident.

Note that in addition to specifying the threat types, one should also determine the *intensity* of the threat. In PREDICT deliverable D2.2, example categories for the intensity of several threat types can be found.

## 5. CI sectors

There are many taxonomies of CI sectors. One such taxonomy offering a fairly extensive list, is presented in Table 2 [18].

*Table 2: EU green paper taxonomy of CI [18]*

| Sector | | Product or service |
|---|---|---|
| I | Energy | 1 Oil and gas production, refining, treatment and storage, including pipelines |
| | | 2 Electricity generation |
| | | 3 Transmission of electricity, gas and oil |
| | | 4 Distribution of electricity, gas and oil |
| II | Information, Communication Technologies (ICT) | 5 Information systems and networks protection |
| | | 6 Instrumentation automation and control systems (SCADA etc.) |
| | | 7 Internet |
| | | 8 Provision of fixed telecommunications |
| | | 9 Provision of mobile telecommunications |
| | | 10 Radio communication and navigation (e.g. Loran, GPS and Galileo) |
| | | 11 Satellite communication |
| | | 12 Broadcasting |
| III | Water | 13 Provision of drinking water |
| | | 14 Control of water quality |
| | | 15 Stemming and control of water quantity |
| IV | Food | 16 Provision of food and safeguarding food safety and security |
| V | Health | 17 Medical and hospital care |
| | | 18 Medicines, serums, vaccines and pharmaceuticals |
| | | 19 Bio-laboratories and bio-agents |
| VI | Financial | 20 Payment services/payment structures (private) |
| | | 21 Government financial assignment |
| VII | Public & Legal Order and Safety | 22 Maintaining public & legal order, safety and security |
| | | 23 Administration of justice and detention |
| VIII | Civil Administration | 24 Government functions |
| | | 25 Armed forces |
| | | 26 Civil administration services |
| | | 27 Emergency services |
| | | 28 Postal and courier services |
| IX | Transport | 29 Road transport |
| | | 30 Rail transport |
| | | 31 Air traffic |
| | | 32 Inland waterways transport |
| | | 33 Ocean and short-sea shipping |
| X | Chemical and nuclear industry | 34 Production and storage/processing of chemical and nuclear substances |
| | | 35 Pipelines of dangerous goods (chemical substances) |
| XI | Space and Research | 36 Space |
| | | 37 Research |

Studies [8], [11] show that CI sectors which account for the majority of cascading effects, include foremost the telecommunication, energy and transport sectors. To include these sectors in the analysis is therefore obvious, although specific demands on the probability assessment of cascading effects could result in higher priorities for other sectors to be included.

Again, whether to include CI sectors in the analysis or not is a decision that can be made freely, as long as one is aware of the consequences this will have on the reliability and precision of the analysis results. In general, restricting an analysis to only relevant sectors will considerably reduce the effort needed to do the analysis, but the results will not reflect contributions in the chain of events of CI sectors that were excluded because their influence was expected to be insignificant.

## 6. Impact types

A well-considered and fairly complete taxonomy of impact types to consider in case of a CI failure, is used in the Dutch NRA method [20], which is used to assess the wide gamut of (national) risk including CI failure in the Netherlands.
In this method, the impact is assessed for five main impact types characterised by ten sub-types:

| Impact type | Impact sub type | Definition[4] |
|---|---|---|
| **1. Territorial security** | 1.1 Encroachment on national territory | The actual or functional loss, or out of action and/or access or the loss of control over parts of the nation, including territorial waters and airspace. |
| | 1.2 Infringement of the international position of the nation | The damage to the reputation or the influence or appearance of the nation abroad. |
| **2. Physical security** | 2.1 Deaths | Fatal injuries, immediate fatality or early fatality within a period of 20 years |
| | 2.2 Severely wounded and chronical ill | Cases of injury in the categories T1 and T2, and people with long-term or permanent health problems such as breathing difficulties, serious burns or skin disorders, damage to hearing, suffering post-traumatic stress syndrome (PTSS). Victims in the categories T1 or T2 need immediate medical assistance and should be treated immediately (T1) or must be kept under continuous observation and be treated within 6 hours (T2).<br>Chronically ill people who experience limitations over a long period (> 1 year): needing medical care, being wholly or partially excluded from participating in their work, experiencing difficulties in their social functioning due to their illness |
| | 2.3 Physical suffering | Exposure to extreme weather conditions, as well as a lack of food, drinking water, energy, housing, basic sanitary provisions or other primary necessities of life |
| **3. Economic security** | 3.1a Costs | An amount of money in terms of repair costs for damage suffered, extra costs and lost income |
| | 3.1b Impairment to the vitality of the economy | Impairment to the vitality of the economy. |

[4] Re-formulated to include areas outside the Netherlands

| Impact type | Impact sub type | Definition[4] |
|---|---|---|
| **4. Ecological security** | 4.1 Long-term impact on the environment and on nature (flora and fauna) | Long-term or permanent impairment to the quality of the environment, including contamination of the air, water or ground, and long-term or permanent disturbance of the original ecological function, such as the loss of diversity of types of flora and fauna, loss of special ecosystems, being overrun by foreign species. |
| **5. Social and political stability** | 5.1 Disruption of everyday life | The infringement of the liberty to move about freely and to gather in public places and spaces, whereby participation in the normal social existence is hindered. |
| | 5.2 Violation of the democratic system | The impairment in the functioning of the institutions of the democratic system and/or the infringement of rights and liberties and other core values bound to the democratic system as set out in the Constitution. |
| | 5.3 Psycho-social impact and social unrest | The reaction of citizens who are characterised by negative emotions and feelings (such as fear, anger, dissatisfaction, sadness, disappointment, panic, disgust, and resignation/apathy). This concerns the population as a whole, therefore besides those people directly affected also citizens who experience the incident or process via the media or other means. The expressions of these emotions and feelings may or may not be perceptible (i.e. audible, visible, readable). |

In the guideline [20], each of the mentioned impact category are complemented by clear and concrete guidelines on how to score them on a five point scale while considering the uncertainties in the assessment.

## 7. Dependencies

As a quick start guide for determining the CI sectors which should be included in the assessment, below are several tables which indicate the percentage distribution of cascading events that took place in Europe in the last decade. They are drawn from the TNO outages database [8] and updated to include outages up to October 2014.

These tables can be used both to assess which CI cause most of the cascade effects (columns) and which CI sectors suffer from them (rows) (Figure 10). Figure 11 presents a similar matrix for the Member States of the European Union; Figure 12 depicts this graphically including the disruption initiates by non-dependency threats. Figure 13 shows the matrix for The Netherlands.

| AFFECTED SECTOR \ INITIATING SECTOR | Energy | Financial services | Food | Government | Health | Industry | Internet | Telecom | Transport | Water | Sample size |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Education & Research | 57% | | | | | | | | | 43% | **7** |
| Energy | 93% | | | | | 3% | | | 2% | 2% | **121** |
| Financial services | 18% | 36% | | | | 3% | 9% | 33% | | | **33** |
| Food | 30% | | 20% | | | 10% | | | 10% | 30% | **10** |
| Government | 32% | 4% | | 4% | 2% | 2% | 9% | 38% | 2% | 6% | **47** |
| Health | 45% | | | | 10% | 21% | | 14% | | 10% | **29** |
| Industry | 69% | | | | 3% | 11% | 3% | 3% | 9% | 3% | **35** |
| Internet | 14% | | | | | | 19% | 67% | | 1% | **177** |
| Telecom | 44% | | | | | | 2% | 53% | 2% | | **234** |
| Transport | 70% | | | | | 4% | 1% | 8% | 14% | 4% | **186** |
| Water | 87% | | | | | 2% | | | | 11% | **45** |
| **Total** | **51%** | **2%** | **0%** | **0%** | **1%** | **3%** | **5%** | **31%** | **4%** | **3%** | **924** |

*Figure 10: Percentages of cascade effects initiated in a CI sector in Europe and received by an affected CI (01/01/2004 – 07/11/2014)*

| AFFECTED SECTOR \ INITIATING SECTOR | Energy | Financial services | Food | Government | Health | Industry | Internet | Telecom | Transport | Water | Sample size |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Education & Research | 50% | | | | | | | | | 50% | **6** |
| Energy | 93% | | | | | 4% | | | 2% | 1% | **100** |
| Financial services | 19% | 38% | | | | 3% | 9% | 31% | | | **32** |
| Food | 33% | | 22% | | | 11% | | | 11% | 22% | **9** |
| Government | 33% | 4% | | 4% | 2% | 2% | 9% | 37% | 2% | 7% | **46** |
| Health | 43% | | | | 11% | 21% | | 14% | | 11% | **28** |
| Industry | 66% | | | | 3% | 13% | 3% | 3% | 9% | 3% | **32** |
| Internet | 14% | | | | | | 16% | 69% | | 1% | **169** |
| Telecom | 43% | | | | | | 1% | 53% | 2% | | **222** |
| Transport | 69% | | | | | 5% | 1% | 7% | 15% | 4% | **177** |
| Water | 85% | | | | | 3% | | | | 13% | **40** |
| **Total** | **50%** | **2%** | **0%** | **0%** | **1%** | **3%** | **5%** | **33%** | **4%** | **3%** | **861** |

*Figure 11: Percentages of cascade effects initiated in a CI sector in the European Union and received by an affected CI (01/01/2004 – 07/11/2014)*

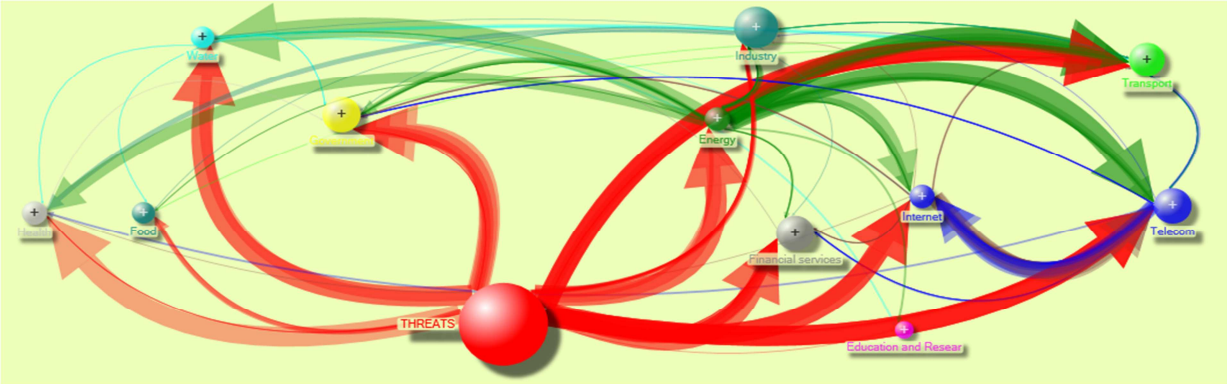



*Figure 12: Cascade effects initiated by CI sectors in the European Union (01/01/2004 – 07/11/2014) – figure produced with NodeXL by courtesy of TNO*

| | | INITIATING SECTOR | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Energy | Financial services | Food | Government | Health | Industry | Internet | Telecom | Transport | Water | Sample size |
| AFFECTED SECTOR | Education & Research | | | | | | | | | | 100% | **1** |
| | Energy | 96% | | | | | | | | | 4% | **23** |
| | Financial services | 25% | 25% | | | | | 13% | 38% | | | **16** |
| | Food | 40% | | 20% | | | 20% | | | | 20% | **5** |
| | Government | 33% | 6% | | 6% | 3% | | 9% | 39% | 3% | | **33** |
| | Health | 33% | | | | 11% | 33% | | 17% | | 6% | **18** |
| | Industry | 78% | | | | 11% | | 11% | | | | **9** |
| | Internet | 9% | | | | | | 26% | 65% | | | **91** |
| | Telecom | 41% | | | | | | 2% | 57% | | | **97** |
| | Transport | 62% | | | | | 8% | 2% | 14% | 14% | 2% | **66** |
| | Water | 91% | | | | | | | | | 9% | **11** |
| | **Total** | **41%** | **2%** | **0%** | **1%** | **1%** | **3%** | **9%** | **39%** | **3%** | **2%** | **370** |

*Figure 13: Percentages of cascade effects initiated in a CI sector in The Netherlands and received by an affected CI (01/01/2004 – 07/11/2014)*

# VI. Applicability within the foresight and prediction tools

## 1. Introduction

The methodology described in this document will be used and build upon in the other tasks and work packages of the PREDICT project.
The methodology builds on results established in WP2. It will be an essential part of the incident evolution framework (WP3) and will be implemented in the foresight and prediction tools (WP5). This chapter described the main relationships with the other tasks in WP2, WP3 and the interaction with WP5.

## 2. Coupling with threat quantification

In this section, the connections between Tasks 3.1 and 3.2 are described by pointing out the link of the Task 3.2 working plan to the PREDICT methodology. The use of the conceptual methodology to determine the cascade probability function for a crisis situation is introduced and illustrated by a simple example.

**Guidance for the quantification based on WP2**
Considering the current state-of-knowledge as described in D2.1 and in D2.2, and regarding (1) the level of detail required to assess the different probabilities describing the threat occurrence likelihood, (2) the CI loss of service, (3) the duration of the downtime and (4) the probability of given cascading failures through the CI, some suggested approaches from these studies would include:

- Threat likelihood: in the absence of reliable data on the threat occurrence, the occurrence likelihood over a predetermined interval of time (a day, a week, a month, a year, …) could be expressed in the terms: low, medium or strong likelihood. Each of the levels should be clearly and univocally defined in terms of probability. The use of the same scale of occurrence likelihood for all the identified threats, even if the predefined interval of time differs from one threat to other, could be beneficial.
- Threat specification: considering that a target of all crisis management actions is to protect a given set of CI, one could consider using '*service loss*' as a metric to describe the combined effect of threat level and vulnerability. It could be expressed on a three-point scale, each level describing a clearly defined range of loss of function.
- Downtime: once the intensity of the impact is specified and subsequently the "level of service loss" is determined, experts can assess the characteristic downtime of a given CI, at a given "level of service loss" resultant from a well-specified threat. The downtime $\tau$ can be expressed on a three-point scale, with each level describing a clearly defined range of absolute or relative (to another time factor) duration.
- Failures propagation: one CI failure (loss of provision of product or service) may result in the failure of some other CIs. A dependency matrix might be convenient way to model this. The dependency between two identified CIs could be described as: weak, medium or strong, each level describing a clearly defined range of probability of propagation of failure.

**Coupling of threat quantification with the PREDICT seven-step methodology**
In Task 3.2: Threat quantification, the physical and systemic models of threats related to an incident will be chosen and specified. The emphasis of the work is on the efficient utilisation of the results of models describing the development of hazards. The different predictions that are generated with the

prediction tools will be put on the same time line in order to create a common picture of the situation and its development.

The working plan for Task 3.2 includes the following phases:

Phase 1: Definition of the threats in the scenarios

The threats in a specific scenario will be defined and illustrated taking into account the development of the situation.

Phase 2: Selection and specification of modelling approaches to quantify the threats

The selection and specification of modelling approaches will be based on the WP2 review of existing crisis management tools and the CRISMA project study of time-dependent physical vulnerability. It is expected that several modelling approaches will be defined for case-by-case use, due to the widely varying features of different scenarios.

Phase 3: Development of a common picture of the situation

A common picture of the situation will be developed by putting the different predictions on the same time line. In this process, separate event chains with parallel or serial linkages are illustrating the cascading effects.

Phase 4: Probability estimation

The probabilities of cascading effects resulting from the original incident will be determined, and the cascade probability functions based on the threat quantification will be formulated.

The determination of probabilities of threats as functions of time enhances the situational awareness of various actors and helps in the decision making on the allocation of resources. The operations of organizations will be modelled in Task 3.3 to support the prevention and mitigation of threats.

The threat quantification in Task 3.2 is closely related to steps 1, 4, 6 and 7 of the PREDICT methodology described in Chapter IV. The relation between the phases of Task 3.2 working plan and the steps of the PREDICT methodology described in this deliverable can be summarised as follows:

| Task 3.2 phase | Methodology step | Description of coupling |
|---|---|---|
| Phase 1 | 1: Identify the threats to be considered | Phase 1 is directly coupled to Step 1 with similar contents. |
| Phase 2 | 4: Characterise the vulnerability of the key CI elements for the threat | The characterisation of the vulnerability forms the basis for the selection of the modelling approach. |
| Phase 3 | 6: Describe the dependencies between the CI in the region | The coupling is bidirectional:<br>• The description of the dependencies between the CIs is the basis for the definition of the separate event chains and their linking.<br>• On the other hand, the dependencies between the CIs are clarified by the common time line of the related predictions. |
| Phase 4 | 7: Assess the CI cascading effects | The CI cascading effects of the situation as a whole are described by the cascade probability function. |

**Coupling of threat quantification with the probability assessment**

In this section we are trying to explain at a general level what threat quantification means in connection with the likelihood of cascading effects. The approach will be further developed in T3.2.

Threat quantification may have different meanings. It may mean (1) the probability of a threat (risk of an event) or it may mean (2) the amount of consequences of a threat e.g. how many people are threatened in what time schedule or a spread of an oil spill over time. It may also mean (3) the progression of the domino effect over time. Here we are talking about (3) with an addition, that the progression may also be probabilistic.

When the threatened CI and the chains of possible cascading effects between them have been identified, we can start to look at the likelihood of the cascading effects in question. The likelihood is determined by the dependence of CI on output of others to sustain their functions. To be able to make a prediction about how the situation develops, we need to model those interdependencies. These models are deeply case dependent, which means that the development work in the PREDICT project has to start with looking at the case studies. After creating a system that works for those cases we can try to make generalisations.

Threat quantification, as described in the definitions, describes the (probabilistic) progression of the domino effect over time. This can be described in mathematical terms as follows:

The probability $P_{xyi}$ of a certain cascading effect i between critical infrastructures $CI_X$ and $CI_Y$ is dependent on the states X and Y of $CI_X$ and $CI_Y$. We can write $P_{XYi}=F_i(X,Y)$ i.e. the probability of the cascading effect i is a function of the states X and Y of the respective CIs in question. The states of the CIs may be dependent on time (t), constant parameters (a,b,..), stochastic variables (ξ, ζ,…), time dependent variables (u(t), v(t),…), time dependent stochastic variables (ψ(t), ω(t),…) etc.. So for example we may have:

$$P_{xyi} = F_i\{X[t, a, \dots \xi, \dots, u(t), \dots \psi(t), \dots], Y[t, b, \dots, \zeta, \dots, v(t), \dots \omega(t), \dots]\} \quad (1)$$

As we can see, depending on the parameters of function (1) the probability of the cascading effect may be time-dependent or a constant. In a crisis situation, there may be several CIs threatened and between CIs there may be several different and parallel cascading effects, which is schematically described in Figure 14. In principle we could define the dependencies, find models for them and solve the probabilities as is described in the example 1a below.

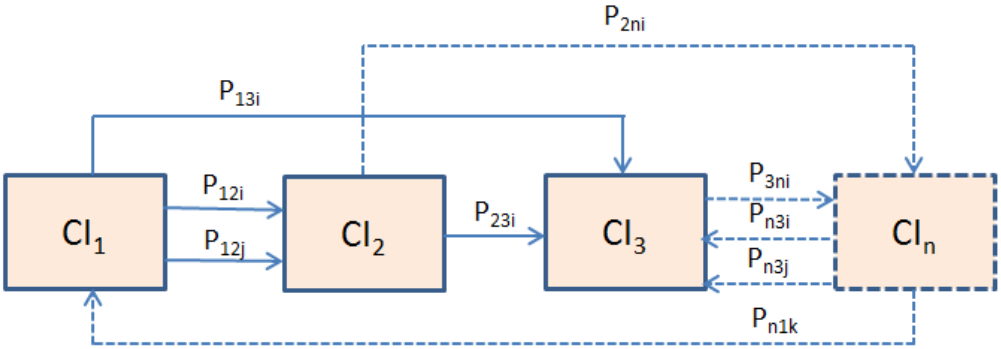



*Figure 14: A schematic picture of a system with chains of cascading effects*

*Example 1a:* *In order to find out how much time there is available for the fire brigade to operate before serious consequences are unavoidable for the nuclear power plant (NPP), Monte Carlo fire simulation was used [9] to determine the time-dependent probability of a component of the safety system of the NPP to fail during a fire in a cable room. The indicator of the state of the system was the temperature of the insulating material around the metal wires. A cable failure was assumed to happen at a critical temperature 180℃ or 215℃* (Figure 15).

Model: Monte Carlo/ CFD fire (FDS)

State variable X: temperature of the insulating material around the metal wires (Critical X: 180℃/215℃)

X is a time dependent stochastic variable, which is dependent of the following parameters:

| Parameter | Type |
|---|---|
| time | variable |
| material parameters | constant |
| place of ignition | stochastic |

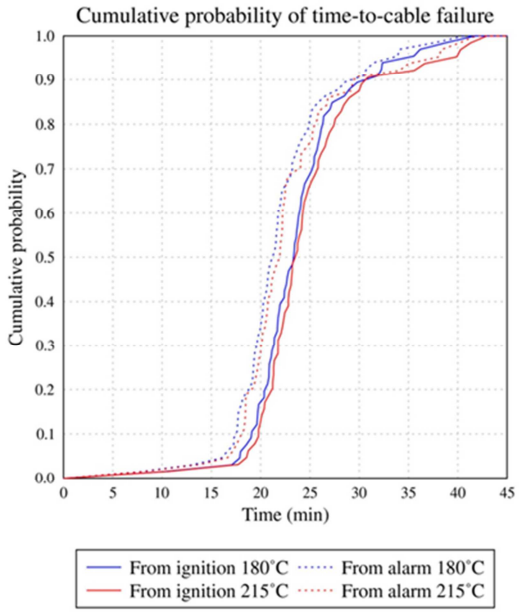



*Figure 15: Time-dependent probability of a cable failure in a fire of a cable room of a NPP [9]*

In practical terms we cannot carry out such heavy simulations for each dependency of the system; we have to make simplifications. In task 3.2 we will investigate how this could be done. Intense simulations can be used if there are sufficient resources and time. For the purposes of preparing for crisis situations and learning more about them this intensive kind of approach can be used. For the purposes of decision making in the actual situation or training of personnel we have to develop simplified approaches. One way to cope with this problem would be the following procedure, which has been inspired by the deliverable D432 of the CRISMA project [13].
Define the states of the CI

- Define how the states are described:
  - Indexes (discrete)
  - Curves (continuous)
  - Probability matrices (constant or time dependent probabilities)
- Define the critical states that can lead to specific cascading effects
- Define models for the states; the models can be based on the following methods:
  - Empirical models based on past experiences and statistical analysis
  - Analytical models
  - Expert assessments
  - A combination of the previous methods

To get to the point where we can also look at the capability of mitigation of the potential cascading effects we should look at the dynamic progress of the situation and the organisation's response to it. In task 3.3 we shall develop models for the organisation's response and communication. In the following example (1b) we are showing how this was done for the situation of example 1a.

*Example 1b:* *In order to find out if the fire brigade has a possibility to prevent the cable failure before serious consequences, a SOTM model [9] was combined with the fire simulation that was described in the example 1a. A stochastic fire simulation was used to determine when the fire will cause failing of a component (a probability distribution); SOTM model was used to determine when the fire brigade will be able to suppress the fire (a probability distribution). As a combination of 1 and 2 the probability was determined for the failure of a component of the safety system in the situation.*

## 3. Integration of the methodology in the foresight and prediction tools

The following paragraphs describe some initial ideas on the development of the PREDICT foresight and prediction tools. At this stage of the project that includes propositions of:

- approaches to computational modelling for simulations,
- implementation of the methodology for the assessment of the cascading effects, and
- ideas on how to include geographical elements.

**Approaches to computational modelling**
It is important to be aware that at this stage of the project user requirements are not yet fully specified. The following approaches however are considered to be possibly the most useful for the development of the PREDICT foresight and prediction tools.

In order to properly apply the methodology identified in this document, all of the approaches will be analysed and pre-validation will be conducted at the early stage of the System Architecture Design work package. Thus it will only then be possible to choose the most appropriate approach to

computational modelling for simulations in order to fully meet requirements for modelling of the cascading effects.

Modelling cascading effects demands considering multiple factors including insight into causes and effects, modelling complex overall interactions between CI, modelling reductions in CI capacity due to damage of physical system or shortages of essential inputs, as well as taking into account products of likelihood and consequence. One of the world's crisis management leading research and development organisation - NISAC (National Infrastructure Simulation and Analysis Centre) - in *Multiple Modelling Approaches and Insights for Critical Infrastructure Protection [22]* publication stated unambiguously that there could be no single model to answer all questions regarding interdependencies of CI and so on. Thus all the work done within the NISAC is based on the network theory forms, consisting of **network flow models**, **system dynamics models** and **agent based models**. The NISAC approach will be taken into consideration while developing the PREDICT tools.

Findings of the SoTA (see [1]), literature review and crisis management modelling experience indicated that one of the most popular approaches to modelling cascading effects is the one called **Agent Based Modelling (ABM) [23]**. ABM is the computational modelling of systems as a collection of autonomous interacting entities (called "agents"). The key characteristic of the approach is that each agent is perceived as an individual entity which maintains a state, and sensors input. Each agent possesses also rules of behaviour that act upon the inputs and either modify the state or produce an output. Moreover, the ABM principle can also be used to construct real-world systems. Examples include shop bots, automated internet auctions, smart-grid electronic devices, and data storage systems. The resulting real-world systems can, in turn, be simulated by ABMs that mimic their basic architecture and consistent agent types.

Another noteworthy approach is called **Actors Based Modelling [23]**. Actors are computational agents which map each incoming communication to a 3-tuple consisting of (i) a finite set of communications sent to other actors; (ii) a new behaviour (which will govern the response to the next communication processed); (iii) a finite set of new actors created [25]. Moreover, actors can make a local decision, create more actors, send more messages, and determine how to respond to the next message received. The Actors model can be used as a framework for modelling, understanding, and reasoning about a wide range of concurrent systems. For example: electronic mail, web service, etc.

However as there is no yet complete user requirements specification **Event-driven programming [26]** has to be taken into account as well. Event-driven programming can be defined as an application architecture technique in which the application has a main loop divided down to two sections: (i) event selection (or event detection), and (ii) event handling. In embedded systems the same may be achieved using interrupts instead of a constantly running main loop. In that case the former portion of the architecture resides completely in the hardware. Event-driven programming is widely used in graphical user interfaces as it has been adopted as a model for interaction by most commercial widget toolkits.

However the propositions mentioned above are yet to be verified once the full specification of the user requirements is developed and delivered.

**Implementation of the geographical elements**
In order to start the discussion regarding implementation of the expected geographical elements it has to be decided whether the proposed system will be a web application (client-server architecture)

or a desktop application. If the geographical elements are to be static (e.g., points location, static map visualisation) web based solution would probably be good enough. However if the user requirements demand dynamic visualisation (e.g., real-time simulation of the progression of a flood) desktop based solution would be a better choice. The architecture of both solutions is similarly constructed, however, the representation of a single element would differ significantly.

Currently considered as the most effective and popular approach to web-based software engineering is called N-tier application architecture. N-tier application architecture provides a model by which developers can create flexible and reusable applications. By segregating an application into tiers, developers acquire the option of modifying or adding a specific layer, instead of reworking the entire application. A three-tier architecture is typically composed of a presentation tier, a domain logic tier, and a data storage tier. The three-tier architecture is also commonly used while creating desktop based software, however the individual characteristics differ.

Data storage tier in the web-based software is currently the most frequently based on GIS systems. Experience acquired while developing crisis management tools proved GIS systems to be effective. Thus it would be probably recommended to use PostgreSQL with the PostGIS extension relational database.

The presentation tier is the topmost level of the application. The presentation tier displays information related to such services as browsing merchandise, purchasing and shopping cart contents. It communicates with other tiers by which it puts out the results to the browser/client tier and all the other tiers in the network. If the PREDICT prediction and foresight tools are to be created using the client-server technology, the presentation tier would most probably be based on Leaflet (java script library) and OpenLayers solutions.

The domain logic tier is pulled out from the presentation tier and, as its own layer, it controls an application's functionality by performing detailed processing. In that case Map servers are indispensable. Probably solutions such as MapServer or GeoServer should be taken into account. The same solutions should be considered in the desktop applications.

There are a number of data storage tier solutions, which has to be taken into account while designing system architecture of the desktop based tool. It would be probably recommended to save the information in the Extensible Markup Language format (.xml), so that a result ESRI Shapefile (.shp) or Keyhole Markup Language (.kml) have to be considered.

The presentation tier in the desktop software is the one, which gives an almost unlimited field of creativity. However, the acquired experience in the crisis management modelling proved NASA WorldWind solution to be exceptional. As it has been already used and implemented in several crisis management domain projects, we would recommend to implement it in the PREDICT foresight and prediction tools (see pictures below).

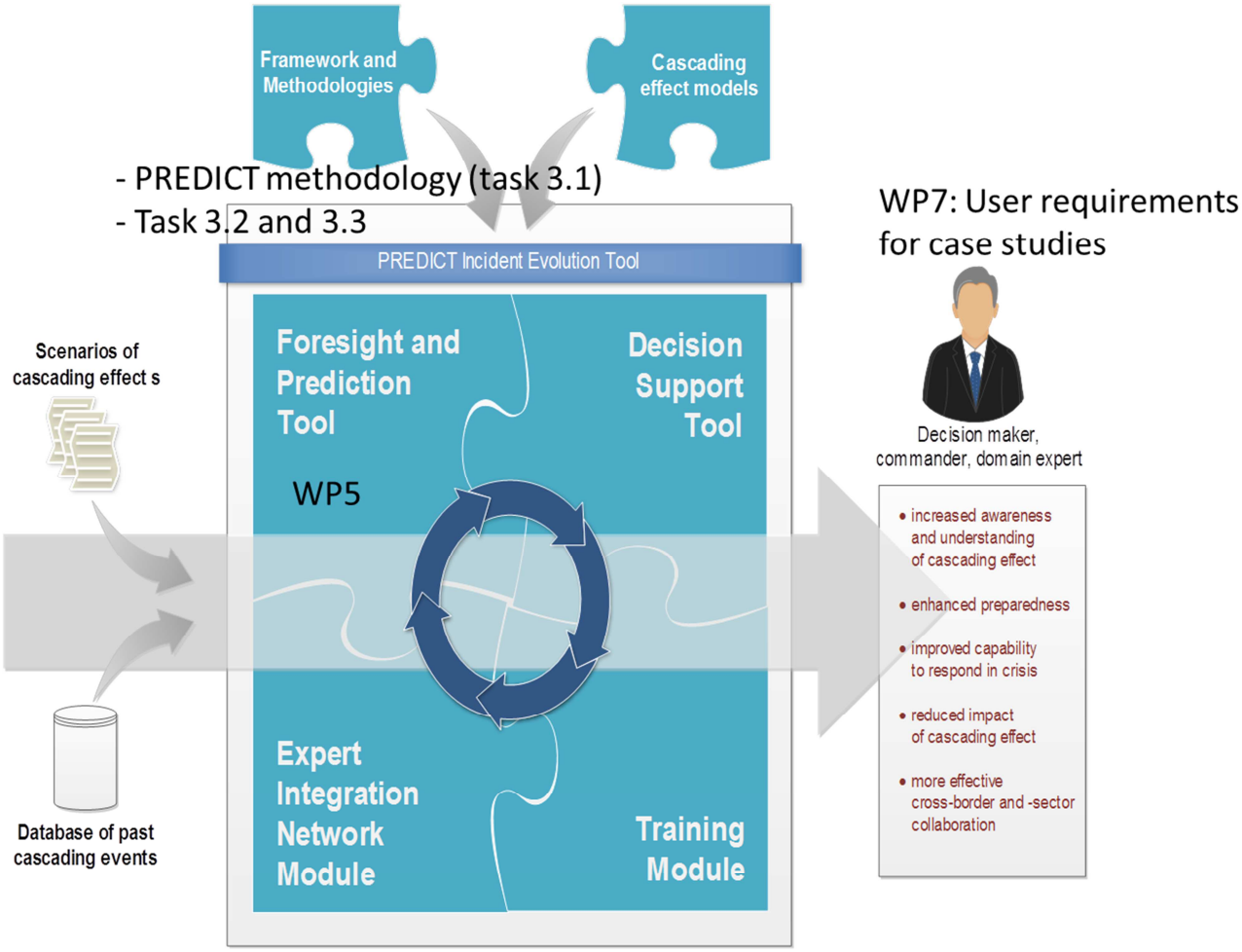
It is important however to remember that the above mentioned propositions are yet to be verified once the full specification of the user requirements is developed and delivered.

**Implementation of the methodology for the assessment of the cascading effects**
In order to properly implement the methodology for the assessment of the cascading effects, a detailed user requirements specification has to be provided. At this stage of the project only be initial ideas and a basic vision of the implementation can be presented.

- **Geographical representation**: the user could be provided with a map limited to the area, which is in the scope of the user's responsibility. It could be e.g. a city district, a metropolitan area or the whole region.
- **Critical data usage**: a database could consist of threat models, which contain the CI with its typology associated strictly with the nature of the threat. The moment when the threat is defined, the CI is being localised on the map.
- **CI key elements:** the description of the CI could contain a description of its key elements. Those key elements could be correlated with the threat, which would be analysed in order to properly react and prepare. E.g. in case of a flood the power station is in danger and its working capacity could be disrupted. Going down, that means power generator could be flooded. In case of a hurricane the power station would also be in danger. However the key element identified in such a situation would be the power lines, not a generator. That could be enlisted or presented visually on the map – it is to be specified by the end-users at the further stage of the project.
- **CI key vulnerabilities:** the database could contain key vulnerabilities, which would be identified in correlation to a seriousness of the threat. E.g., in case of a flood and an endangered power station - if the flood exceeds 3 metres, the generator would be flooded. If not, probably there would not be any disruptions in the working capacity. Such vulnerabilities could be listed, presented visually on the map or presented by a probability matrix. It is probably important to include information about impact within the time frame. It could be presented by radius at the map or as issues above – in the probability matrix or enlisted.
- **CI working capacity disruptions metrics:** for each CI there could be a working capacity disruption metrics defined. It has to be decided, whether the system should provide the users with the possibility of manual adjustments of such metrics or not.

## 4. Summary and next steps

As the descriptions in this chapter show, the PREDICT methodology proposed in Chapter IV, will be used and extended in the Tasks 3.2 and 3.3 and in WP5.




We used the analysis of lessons learned of crisis response operations and cascading effects, and the database of past cascading events, to identify the essential elements for identification and probability assessment of cascading effects and develop the main steps of the PREDICT methodology to assess cascading effects.

The Tasks 3.2 and 3.3 will build on this methodology and refine it towards further quantification of both the threats (Task 3.2) and the (use of the method in enhancing the) organisation's response (Task 3.3). As stated in the descriptions of these tasks in this chapter, these types of models are highly case dependent. When the user requirements of the case studies (D7.1) are available, a more detailed analysis can be made of the types of models that are suited to the case studies. After creating a system that works for those case studies, we can study the possibilities to make generalisations and work towards a more generic model.

A purely quantitative approach may not always be necessary or even possible for all of the steps of the PREDICT methodology. Experience shows that it may be hard to obtain detailed quantitative data for each of the steps. Therefore it would be wise to develop both a qualitative and a quantitative approach or a mixed mode approach. This will allow the end user to choose between the two approaches, based on his preferences or on the data that is available.
Also, in some cases expert interviews and use of fuzzy numbers could be employed when statistical data are not available.
The PREDICT methodology was used in WP5 to identify some of the main modules for the foresight and prediction tools.

- Geographical representation (derived from descriptions in all steps)
- Information requirement for description of CI behaviour (all steps)
- CI key elements (step 3)
- CI key vulnerabilities (step 4)
- CI working capacity disruptions metrics. (Step 7 and others)

Again, the user requirements for the case studies being identified in WP7 may serve as a starting point in choosing the right level of detail for each of those modules.

## VII. References

[1] PREDICT D2.1 (2014), State of the Art of the R&D activities in cascade effect & resilience and global modelling.

[2] European Council (2008). Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Brussels, Belgium. On-line: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008L0114:EN:NOT

[3] Rinaldi, S., J. Peerenboom, and T. Kelly (2001). Identifying, understanding and analysing critical infrastructure interdependencies. IEEE Control Systems Magazine, pp. 11–25.

[4] Luiijf, E., Klaver, M. (2009). ”Insufficient Situational Awareness about Critical Infrastructures by Emergency Management”, paper 10 in: Proceedings Symposium on “C3I for crisis, emergency and consequence management”, Bucharest -12 May 2009, NATO RTA: Paris, France. RTO-MP-IST-086. On-line: http://ftp.rta.nato.int/public//PubFullText/RTO/MP/RTO-MP-IST-086///MP-IST-086-10.doc

[5] Von Kirchbach, H-P. et al (2003). Bericht der Unabhängigen Kommission der Sächsischen Staatsregierung Flutkatastrophe 2002, https://publikationen.sachsen.de/bdb/artikel/10825, accessed 10/11/2014.

[6] Pitt, M. (2008), The Pitt Review: Learning Lessons from the 2007 Floods, Cabinet Office, United Kingdom, June 2008. On-line: http://www.environment-agency.gov.uk/research/library/publications/33889.aspx

[7] Houses of Parliament, Parliamentary office of science & technology, Resilience of UK Infrastructure (2010). POSTNOTE Number 362, Houses of Parliament, United Kingdom, October 2010. On-line: http://www.parliament.uk/documents/post/postpn362-resilience-of-UK-infrastructure.pdf

[8] Eeten, M. van, Nieuwenhuijs, A. H., Luiijf, H. A. M., Klaver, M. M. A., & Cruz, E. (2011). The state and the threat of cascading failure across critical infrastructures: the implications of empirical evidence from media incidents reports. Public Administration, 2, 89, pp. 381-400.

[9] Hostikka, S., Kling, T., Paajanen, A. (2012). Simulation of fire behaviour and human operations using a new stochastic operation time model. 11th International Probabilistic Safety Assessment and Management conference PSAM 11, Helsinki, Finland, June 25-29, 2012. 10 p.

[10] Nieuwenhuijs, A. H., Luiijf, H. A. M., Klaver M. H. A. (2008). Modeling Critical Infrastructure Dependencies, in: IFIP Critical Infrastructure Protection, eds. E. Goetz and S. Shenoi.

[11] Swedish Civil Contingencies Agency (MSB) (2009). If one goes down – do all go down?, Swedish Emergency Management Agency, Stockholm, Sweden.

[12] Roberto Setola, Stefano De Porcellinis, Marino Sforna (2009). Critical infrastructure dependency assessment using the input–output inoperability model, in: International Journal of Critical Infrastructure Protection 2, eds ELSEVIER. pp. 170-178.

[13] CRISMA, version 2 of Dynamic vulnerability functions, Systemic vulnerability, and Social vulnerability, http://www.crismaproject.eu/deliverables/CRISMA_D432_public.pdf, accessed 5/9/2014.

[14] Floodprobe (2013) D2.1, Identification and analysis of most vulnerable infrastructure in respect to floods.

[15] Het Deltaprogramma, (2014) "Deltaprogramma 2015; werk aan de delta, De beslissingen om Nederland veilig en leefbaar te houden", (in Dutch), The Hague, The Netherlands.

[16] Luiijf, E., Burger, H., Klaver, M. (2003). "Critical Infrastructure Protection in The Netherlands: A Quick-scan", In U.E. Gattiker (Ed.), *EICAR 2002 Conference Best Paper Proceedings* (ISBN: 87-987271-2-5) 19 pages. Copenhagen: EICAR.

[17] Luiijf, H.A.M., Nieuwenhuijs, A.H. (2008), Extensible Threat Taxonomy for Critical Infrastructures, International Journal on Critical Infrastructures, Vol. 4, No. 4, pp.409-417.

[18] European Commission (2005). Green Paper on a European Programme for Critical Infrastructure Protection, COM(2005) 567 Final, Brussels, Belgium, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576&from=EN , accessed 23-10-2014.

[19] European Commission (2004). *Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism*, COM/2004/0702, Brussels, Belgium, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52004DC0702&from=EN, accessed 23-10-2014

[20] Ministry of Security and Justice, The Netherlands, *Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of the Netherlands*, http://www.preventionweb.net/files/26422_guidancemethodologynationalsafetyan.pdf, Accessed 19-11-2014

[21] PREDICT 2.2 (2014). D2.2 Security Metrics for threats, for systems' resilience MS&A activities, PREDICT Consortium, France.

[22] Theresa Brown (2006), Multiple Modeling Approaches and Insights for Critical Infrastructure Protection, National Infrastructure Simulation and Analysis Center, United States 2006. On-line: http://www.sandia.gov/nisac/wp/wp-content/uploads/downloads/2012/03/Multiple-Modeling-Approaches-and-Insights-for-Critical-Infrastructure-Protection-2006-2827-C.pdf

[23] Paul L. Borrill, Leigh Tesfatsion (2010), Agent-Based Modeling: The Right Mathematics for the Social Sciences?, Department of Economics Ames, Iowa, July 2010. On-line: http://www2.econ.iastate.edu/tesfatsi/ABMRightMath.PBLTWP.pdf

[24] Actor model. On-line: http://en.wikipedia.org/wiki/Actor_model

[25] Gul A. Agha (1985), *Actors, A Model of Concurrent Computation In-distributed Systems*, United States of America, Arlington, Virginia 2006. On-line: http://www.cypherpunks.to/erights/history/actors/AITR-844.pdf

[26] Event-driven Programming. On-line: http://en.wikipedia.org/wiki/Event-driven_architecture

[27] ISO/IEC 27000:2014 and ISO 31000:2009

[28] DHS Risk Lexicon 2010 Edition, September 2010

**PREDICT project Partners**