European
Commission

JRC SCIENTIFIC AND POLICY REPORTS

Risk Assessment Methodology for Critical Infrastructure Protection

Georgios Giannopoulos
Bogdan Dorneanu
Olaf Jonkeren

2013

Report EUR 25745 EN

Joint
Research
Centre

European Commission
Joint Research Centre
Institute for Protection and Security of the Citizen

Contact information
Georgios Giannopoulos
Address: Joint Research Centre, Via Enrico Fermi 2749, TP 210, 21027 Ispra (VA), Italy
E-mail: georgios.giannopoulos@jrc.ec.europa.eu
Tel.: +39 0332 78 6211
Fax: +39 0332 78 5469

http://stanet.jrc.it/
http://www.jrc.ec.europa.eu/

Legal Notice
Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of this publication.

JRC78292

EUR 25745 EN

ISBN 978-92-79-28181-5

ISSN 1831-9424
doi:10.2788/78850

Luxembourg: Publications Office of the European Union, 2013

Printed in Italy

Contents

List of Figures

List of Tables

Nomenclature

δx	Economic losses
a_{ij}^{*s}	Inoperability in sector i due to total inoperability in sector j in region s
A^*	Interdependency matrix
a_{ij}^*	Inoperability in sector i due to total inoperability in sector j at national level
a_{ij}	Ratio of the input from sector i to sector j
B^*	Overall inoperability transmission
c^*	Demand-side perturbation vector
c_i	Final demand of the i^{th} sector
f_i	The failure rate of the node i
i, j	Indices
K	Sector resilience matrix
k	The number of links that enter node i
L_{ij}	Links between nodes i and j
lq_i^s	Proportion of demand for sector i in region s satisfied internally
$p_i(t)$	Production inoperability

q	Inoperability vector
r_i	The recovery rate of the node i
t_f	Failure time of node i
th_i	The threshold rate of a node i
X_i	The state of the dependent node i
x_i	Total production output of sector i
$X_i(t)$	Inventory level
x_i^N	Total production output of all sectors in nation N
x_i^N	Total production output of sector i in nation N
x_i^s	Total production output of all sectors in region s
x_i^s	Total production output of sector i in region s
$X_{i,k}$	The state of the nodes that are linked to node i through link k
$\hat{x}$	Production potential of sector i
CI	Critical Infrastructure
CIPS	Prevention, Preparedness and Consequence Management of Terrorism and other Security-related risks
DIIM	Dynamic Inoperability Input-Output Model
EPCIP	European Programme for Critical Infrastructure Protection
GIS	Geographical Information System
IIM	Inoperability Input-Output Model

IO	Input-Output
JRC	Joint Research Centre
KRSC	Key Resource Supply Chain
MS	Member States
OSP	Operator Security Plans
SE	Systems Engineering
SoS	Systems of Systems
WIOD	World Input-Output Database

Chapter 1

Risk assessment methodology for critical infrastructure protection

1.1 Introduction

The EC Directive 114/08/EC ([1]) defines the concept of European critical infrastructure as an “asset, system or part thereof [...], which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption of which would have a significant impact [...] as a result of the failure to maintain those functions”. Critical infrastructures have slowly begun to be the most significant technical systems influencing the social and economic life in all countries. Through the years, the vertically integrated systems, with only a few points of communication, turned into complex horizontally integrated systems, with many points of interaction in many of their dimensions ([2]). Moreover, the critical infrastructures can be destroyed or disrupted by natural disasters, technical failures or deliberate acts of terrorism. Concerns about the security of these systems resulted into a series of programmes for their protection, such as the EPCIP. The high level objectives of such programmes is to increase the protection and lately the resilience of critical infrastructures against all hazards. In the endeavour of this high level objective, several specific objectives have to be achieved such as identifying systems' vulnerabilities, interdependencies and evaluating impact. Development of specific case studies in order to validate methodologies and tools in practice, measures to reduce vulnerabilities and increase resilience, establish best practices are some of the elements that are usually part of these programs.

1.2 The EPCIP and risk assessment

As mentioned before, the EPCIP aims at improving the protection of critical infrastructures in Europe against all hazards. It has six pillars (see Figure 1.1), one of these is the EPCIP Directive "on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection". The specific programme "CIPS" is the financial instrument of EPCIP through which research projects and JRC activities have been financed. JRC has carried out several research projects but it has also supported the implementation (e.g. [3]) and the review process of the EPCIP Directive.

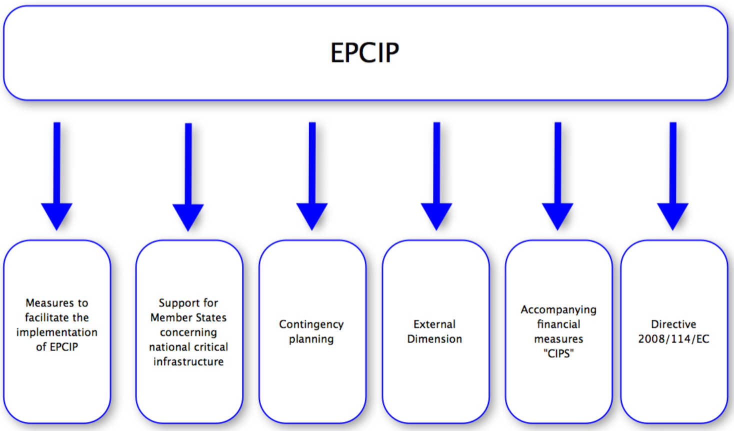

EPCIP
Measures to facilitate the implementation of EPCIP
Support for Member States concerning national critical infrastructure
Contingency planning
External Dimension
Accompanying financial measures "CIPS"
Directive 2008/114/EC

Figure 1.1: *The EPCIP structure*

Within the Directive text, risk assessment can be identified as an important element.

It is mentioned several times for different purposes: As an obligation of MS to report on risks, threats and vulnerabilities in the particular sectors as well as an obligation for risk assessment within the framework of OSP (Operator Security Plans, a model of such operator plan can be found here). Clearly elements of risk assessment methodologies can be identified in OSPs.

Risk assessment methodologies applied by the operators are clearly sectorial or even focused to particular assets. Methodologies such as fault tree analyses [4] are a clear example of this approach. In addition, methodologies applied by operators are not particularly influenced by the Directive. The majority of operators had already certain methodologies in place in order to support their daily business. However, it is not clear whether these methodologies can serve the purpose of the Directive that is the increase of protection of critical infrastructures in order to reduce the impact to the economy and society.

JRC has supported both the first phase of the application and implementation of the Directive as well as the review phase. During this phase, the debate on risk assessment for CI has been reanimated. JRC responded to this need in several ways among which drafting a technical report for reviewing existing methodologies, identify the gaps and propose new approaches. More information can be found in([5]).

1.3 Systems of Systems and risk assessment

As mentioned before, the state of the art in risk assessment for CI is mostly sectorial and asset based. We just mention here the work of Sole et al. [6] for physical network modelling as well as the work of Trucco ([7]) in economics. For more information on risk assessment methodologies refer to the work of [2], [8] and [9].

The work on risk assessment for interconnected infrastructures or in other words

SoS (Systems of Systems) is rather limited. To this end Carcano et al. and Eusgeld et al. ([10], [11]), have focused on the System of Systems character of the interconnected critical infrastructures ([12]). Researchers have pursued two main directions for the investigation of the critical infrastructures behaviour ([2]):

a) The study, analysis and understanding of the infrastructures current makeup. Based on the understanding of the current status, insight into the operation of an infrastructure is gained through various methods for the vulnerability, risk and/or threat assessment. The drawback of this approach is that offers a clear picture only for the events that took place in the past. Although many of the possible roots for failure are detected, not all consequences are visibly perceived and understood.

b) Understanding the dynamic behaviour of the infrastructure systems. In this approach, all possible paths and any cause for instability are explored. The drawbacks of this method are the increased number of paths that have to be considered, as well as the fact that many of the failures are of low probability-high impact nature.

The above mentioned qualitative approach provides only an indication of the system's behaviour but lacks the capacity to obtain tangible output. In order to perform this, two approaches are identified ([2]):

a) Simulation of the critical infrastructure system behaviour using mathematical models. The great advantage of this approach is the increased accuracy and preciseness of the models. However, as the complexity of the system grows, a suitable mathematical representation of the systems becomes a difficult task to be achieved.

b) Analysis of the aggregated behaviour of smaller interacting models. The behaviour of a set of infrastructure is studied through a multi-agent system, where each of the agents represents an infrastructure or an infrastructure system or asset. The collective behaviour of all these agents within an integrated environment allows the analysis of the infrastructure system response to disruptive events.

These approaches provide the main elements that are necessary in order to build risk assessment methodologies for interdependent critical infrastructures. Considering also the main conclusions of the review on risk assessment methodologies [5] it has been possible to gather all the necessary elements in order to proceed towards a comprehensive methodology keeping in mind that we need to render these methodologies more adequate to policy makers, operators and relevant public authorities. This can be achieved on the basis of reducing complexity and implement a higher level of abstraction. The details of the proposed methodology and implementation can be found in the following paragraphs.

1.4 A proposal for a risk assessment concept for networked critical infrastructures

The methodology proposed here focuses on the impact and cascading effects of a disruptive event without performing detailed analysis on each infrastructure asset. This affords a certain level of abstraction that is still reasonable for obtaining a valid representation of the infrastructure and the dynamics of the event being considered. Previous work performed in JRC ([13]), adopted a similar systemic approach for CI disruption and identified three layers of analysis: the micro level (links and nodes), the meso level (network) and the macro level (territory). All these layers are covered with the proposed methodology.

In Figure 1.2 we provide a schematic representation of this risk assessment methodology.

The proposed methodology starts from asset analysis (e.g. a power station), in-

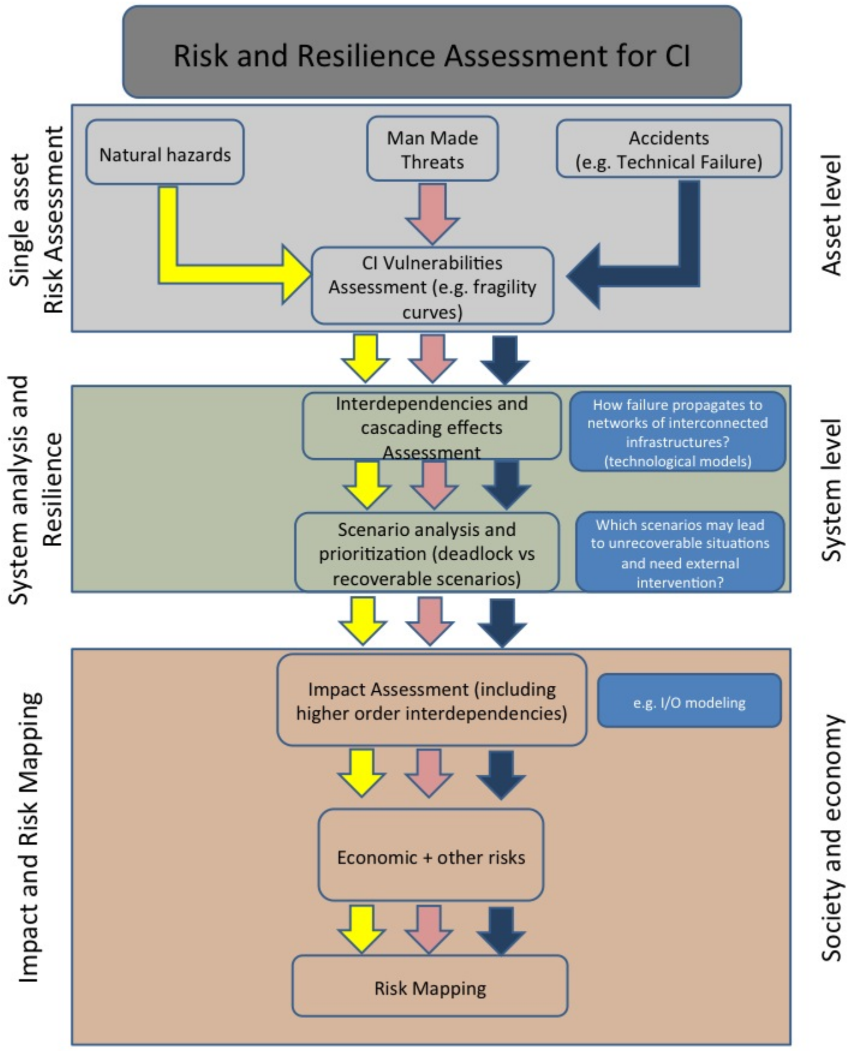

Risk and Resilience Assessment for CI
Single asset Risk Assessment
Natural hazards
Man Made Threats
Accidents (e.g. Technical Failure)
CI Vulnerabilities Assessment (e.g. fragility curves)
Asset level
System analysis and Resilience
Interdependencies and cascading effects Assessment
How failure propagates to networks of interconnected infrastructures? (technological models)
Scenario analysis and prioritization (deadlock vs recoverable scenarios)
Which scenarios may lead to unrecoverable situations and need external intervention?
System level
Impact and Risk Mapping
Impact Assessment (including higher order interdependencies)
e.g. I/O modeling
Economic + other risks
Risk Mapping
Society and economy

Figure 1.2: *Schematic representation of the risk assessment methodology*

vestigates the failure propagation to a critical infrastructure network (e.g. the grid), the cascading effects on networks of interdependent infrastructures and finally estimates the total economic impact due to this disruption. In the following chapters the elements and the models that have been developed for the implementation of this approach are explained in detail.

Concerning the implementation of this methodology we consider that is composed by two principal components, the modelling at technological level and the modelling at economical level. According to the authors knowledge is the first time that there is an effort to assess critical infrastructures using a combination of technological and economical models. Following this terminology, it would be adequate to consider critical infrastructures as complex techno-economical systems. In addition, we consider that the modelling approach that we have adopted here simplifies the amount of data that is necessary for performing the analysis. This will be further explained in the chapter that describes the technological modelling.

A critical element of the present approach is the link between resilience assessment and risk assessment. According to the established terminology, risk assessment is a function of events likelihood, vulnerability and impact. When it comes to resilience it is necessary to have tools in place that may assess the behaviour of complex systems in terms of propagation of failure and recovery. Clearly this goes a step further with respect to typical risk assessment. If we consider risk assessment as indispensable for building risk barriers into assets of critical infrastructures that can be applied also to large scale systems by introducing the element of interdependencies, the resilience paradigm is necessary in order to evaluate the dynamic behaviour and stability of a system.

The methodology that we present here will be further improved and federated with the work on resilience that is taking place in parallel. Elements of this work can be found in [14] and [15]. According to the authors view, resilience is a wider concept that covers much more than a simple risk assessment approach. It incorporates all the measures that have to be applied to critical infrastructures in order to reassure that can withstand a shock, bounce back and recover in case of a disruptive event. The concept of resilience is applicable to assets of critical infrastructures, networks of critical infrastructures and at an even higher level, Systems of Systems. However, the real added value of the resilience paradigm is clearly shown when it comes to networks of critical infrastructures. At this level the kind and diversity of threats, the cascading effects and the complexity of putting risk barriers to complex networks require a different approach. An approach that is based mostly on the continuation of service and less on the risk reduction side.

Chapter 2

Hierarchical technological modelling for risk assessment of networked critical infrastructures

2.1 Introduction

In this chapter we present the technological modelling of risk assessment for networked critical infrastructures that is focused on the element of interdependencies. Numerous methodologies exist in order to assess critical infrastructures at asset level. But when it comes to networks of critical infrastructures a major gap exists. In this chapter we will demonstrate the modelling approach that has been implemented in order to assess the propagation of failure in a critical infrastructure and further on to interdependent critical infrastructures. Thus at this point we consider intra-sectoral and cross-sectoral interdependencies. An important parameter is that the proposed methodology considers a high level of abstraction in terms of infrastructure representation. Clearly representing networked infrastructures at the maximum level of detail is out of the scope due to enormous complexity, data requirements and also appropriateness of the output for a policy maker.

2.2 A systems engineering approach for modelling interdependent critical infrastructures

The methodology presented here aims to assess the impact on critical infrastructures at system level. A key assumption is that the disruption of service takes place for a specific (or several) critical infrastructure asset (assets), it may cascade within the limits of a critical infrastructure and then cascade to dependent and interdependent critical infrastructures. The final goal is to analyse interdependencies and the economic consequences of infrastructure failure.

For this purpose, the systems engineering model is plugged to an IIM (inoperability input-output model). The systems engineering component is applied to analyse performance degradation and then the recovery of the disrupted system. Next, economic losses are estimated with the IIM component that leverages information obtained from the SE component of the model. However, dynamic phenomena taking place in a complex system are often unpractical to model in a rigorous way. For instance, an electrical power system is a large, integrated, interconnected and complex, dynamic, technical infrastructure. Such system can be subjected to various physical phenomena ranging from very fast events such as transients due to lightening, to quite slow ones, such as for steam generators ([16]). Inevitably, this implies that such systems require some simplification. In order to achieve this, the modelling approach proposed in this report focuses on the interdependencies within sectors and across sectors, in other words on the interface between infrastructures and components of infrastructures.

Using this approach the critical infrastructure is abstractly modelled as a network of nodes interconnected by links ([17], [18]). These modelling components are further explained in the following sections. A general representation of the technological modelling approach is shown in Figure 2.1.

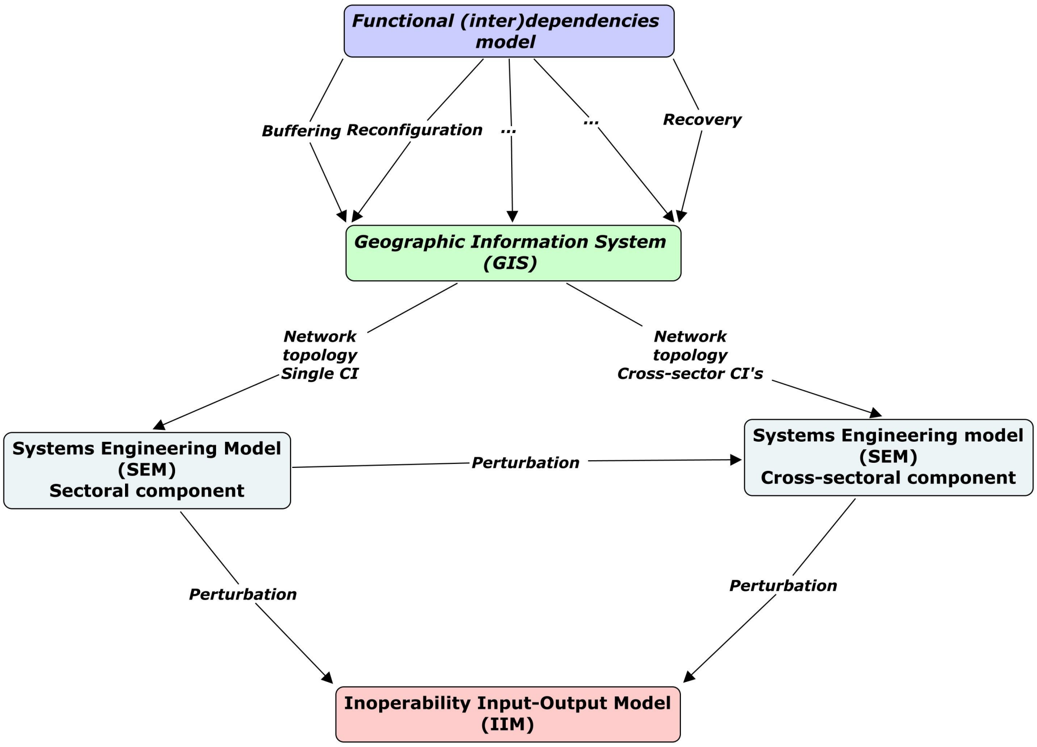

Functional (inter)dependencies model
Buffering
Reconfiguration
...
...
Recovery
Geographic Information System (GIS)
Network topology Single CI
Network topology Cross-sector CI's
Systems Engineering Model (SEM) Sectoral component
Perturbation
Systems Engineering model (SEM) Cross-sectoral component
Perturbation
Perturbation
Inoperability Input-Output Model (IIM)

Figure 2.1: *Representation of the methodology at technological level for assessing critical infrastructures disruption*

2.3 Aggregation of assets and critical infrastructures

The nodes are the model representation of the critical infrastructure's assets. The role of the nodes is to produce, store, and/or to transform a specific type of resource that characterises the critical infrastructure. The nodes, depicted with their suffixes in Figure 2.2, can be a sub-network in their own right, with nodes and links (L_{ij}), where i is the source node and j is the end node. Depending on the scope and goals of the modelling procedure, different levels of abstraction of the network elements can be afforded. The modeller is therefore free to decide the level of detail abstraction of the critical infrastructure modelled structure. A node can represent an asset of a particular critical infrastructure, but, it can also represent a single critical infrastructure in an interconnected system of critical infrastructures. Moreover, the user can consider the critical infrastructure system of an entire country, a region inside one country, or even a region that comprises critical infrastructures on the territory of several countries. Different levels of aggregation are thus allowed.

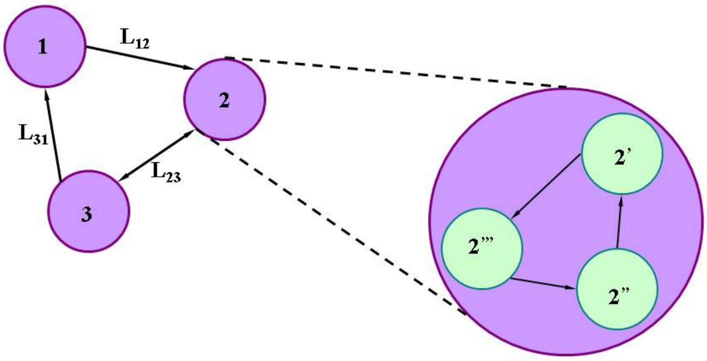


Figure 2.2: *Network representation of a critical infrastructure system*

2.3.1 Critical infrastructure systems and modelling of interdependencies

The transmission lines that connect the aforementioned nodes represent the links of the network and are a schematic representation of dependencies and interdependencies. As already mentioned modern interconnected critical infrastructures can be considered as SoS. A SoS is a combination of heterogeneous components that interact in various ways. According to Rinaldi et al. [19], there are several types of interdependencies:

- Physical

- Cyber
- Logical
- Geographic

Without much loss of generality we can safely assume that these interdependencies can be grouped into functional (Cyber, Logical) and to topological (Physical, Geographic). Functional dependencies can be defined as on-off dependencies (1 or 0). An example of functional dependency can be the link between a power plant and a control centre. The power plant needs information in order to be able to adjust accordingly its production. Topological dependencies on the other hand are much easier to understand and visualise.

a) Topological dependencies - Refer to the physical/geographical location of the component inside the system

b) Functional dependencies - based on the role of the component inside the system, and relates to information about the system such as measures for protection, control, buffering, resilience, etc.

The main difficulty encountered when it comes to functional dependencies is to obtain the necessary data. This can be obtained either through expert opinion or through available data (this is mostly the case for the topological dependencies). Functional dependencies will always require some kind of expert opinion, mainly due to their nature. The present work on the systems engineering part indeed focuses on the functional dependencies. However, topological dependencies are considered as well. Under certain circumstances and using specific modelling techniques we can safely implement the concept of functional dependencies to describe all kind of interdependencies. This would allow the establishment of a harmonised framework for assessing interdependencies in critical infrastructures and would be useful for policy makers. However, this is foreseen as a future development of the present concept.

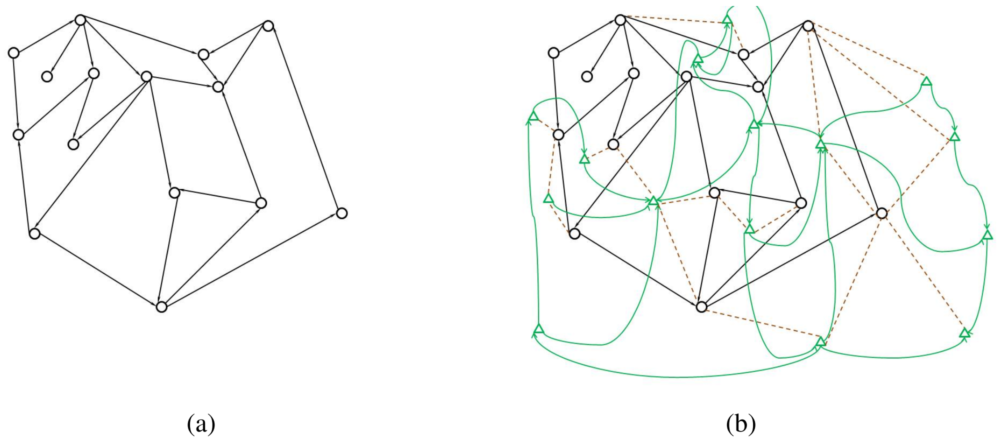
2.3.2 Technological model implementation

The systems engineering model is developed as a federation of sub-models integrated in a common platform, shown in Figure 2.1. Definitely a critical component of this infrastructure is the GIS (Geographical Information System) component and the integration with MATLAB and SIMULINK. The GIS offers a friendly user interface through which the user is able to provide the input data that are required in order to simulate the behaviour of the system, as well as for the visualisation of the simulation results. On the basis of this information, the system engineering model is automatically created using MATLAB/SIMULINK.

Considering the intra-sctoral and cross-sectoral nature of modern critical infrastructures, the systems engineering model is developed in order to reflect this approach as shown in Figure 2.1. The distinction between the sectoral and cross-sectoral interdependencies is mainly done due to the differences in the modelling approaches. At sectoral level, interdependencies can be of all different kinds and the choice of available models is huge. We mention for example the work of Bird et al. ([20]) on the conservation principle of the resources of a system, high level architecture approaches by Eusgeld et al. ([11]), agent-based models by Oliva et al. ([21]), system dynamics by Min et al. ([22]), etc. At cross-sectoral level interdependencies are mainly functional.

2.3.3 Extraction of the topology of systems of infrastructures

The first step in the process to simulate the behaviour of networked systems is to build the model on the basis of its topology. With the term topology we consider both functional as well as topological connectivity of the various infrastructure elements. The level of aggregation for every node depends on the user and the amount of data available. Based on the information on the network topology (Figure 2.3(a)) and functional dependencies (Figure 2.3(b)), information on the structural properties of a specific node with respect to other nodes (criticality, vulnerability, interdependency, interaction and coupling coefficients, etc.) are determined. This allows for a further simplification of the network, since the least affected nodes can be removed from the analysis. This work is part of another report [23] and is linked to resilience assessment of critical infrastructures.

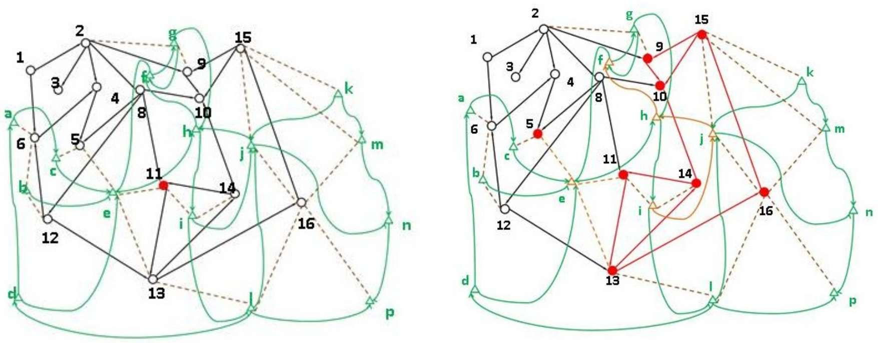

(a)

(b)

Figure 2.3: *Representation of a) network topology; b) functional dependencies in a critical infrastructure network*

What is shown in Figures 2.3 is that both functional and topological dependencies can be assigned in critical infrastructure networks. The topological dependencies are clearly depicted through the GIS system but the user has the ability to assign an additional layer of dependencies by creating links between the nodes of the network. Since this layer of dependencies is purely functional it is subject to certain rules. The implementation of such rules in the existing modelling approach will be the subject of future development. At this stage this is done purely by the user and is based on expert judgement.

In order to demonstrate the importance of having both topological and functional dependencies we have introduced a simple schema of a fictive network. A disturbance that follows a disruptive event is injected into the system (Figure 2.4(a)). This disruptive event may be for example an input from a tool such as RAPID-N [24], or any other tool that may provide this kind of input. For example injecting the perturbation in Node 11, the



(a)

(b)

Figure 2.4: *a) Disturbance injection and b) Network response*

topological model shows only the (possible) propagation to the nodes connected by the red links (topological dependencies). Taking into account the functional interdependencies, Node 5 may also be affected, although this information is not depicted in the physical topology. The consideration of both structural and functional interdependencies allows for a better representation of the model behaviour, as presented in Figure 2.4(b). An example of such infrastructure could be the electricity grid where the topological dependencies can be represented by the grid topology while the communication layer can be provided by the user in terms of functional dependencies.

The perturbation obtained at infrastructure level is the input for the assessment at cross-sectoral level. The same methodology as explained before can be used for the representation of the systems of critical infrastructures however a certain level of abstraction is required in order to obtain reasonable complexity. Similarly to what was already mentioned, the cross-sectoral model determines the perturbation that the critical infrastructure system suffers following a disturbance.

The implementation of the model is done using MATLAB/SIMULINK suite. This suite has been chosen due to its ability to model the behaviour of such systems, as well as its ability to connect to the PostGreSQL database used by the GIS platform in order to import the topology and translate it automatically to a Simulink model. A simple network of six nodes, shown in Figure 2.7(a) is presented here as a proof of concept.

2.4 Building the model in Simulink

Having selected the system and having available the required information on its topology and behaviour, the network topology is extracted through the PostGreSQL database, using either the Database Toolbox available in MATLAB, or MS Excel as intermediate. The Database Toolbox is an extensive collection of toolboxes for use with MATLAB that enables the import and export of data between MATLAB and relational databases ([25]). This toolbox is preferred since it allows for an automated extraction process. In order to proceed with the necessary operations in Matlab and Simulink it is necessary to translate the topology extracted from the GIS system into mathematical representation. This is obtained through the *adjacency matrix*. The adjacency matrix is automatically calculated on the basis of the GIS information. For the purposes of the present analysis and due to the fact that only functional dependencies are considered, the adjacency matrix values are either 1 or 0. Obviously 1 represents a connection between two nodes.

Simulink is an excellent tool for simulating the performance of systems in the time and frequency domain. It is based on building blocks that perform various mathematical calculations but usually it requires the design of the system on a case by case basis. This is not practical for the analysis of critical infrastructures. That is due to the dynamic nature of critical infrastructure systems, the evolution of network topologies and the need to assess situations that a failure of a component leads to the reconfiguration of the whole network. For this reason we develop an automated procedure that is based on building blocks. These building blocks represent the nodes of a system. Currently we assume a standard behaviour for a node. According to this assumption if the node N_j (or nodes) upon which node N_i depends fails (or fail) then the node N_i enters in failure mode following an exponential decay of its performance. The time constant of this exponential function defines the decay rate (failure time). Below a certain threshold value, it is considered that the node N_i has failed and it does not provide any services to the network components that depend on node i. As a consequence the nodes that depend on node N_i enter also in a failure mode and so forth.

The recovery of a node starts when the node (or nodes) upon which this node depends is recovered, or if we consider that an external intervention brings this node back to functional state. Again the recovery is simulated using an exponential function with the time constant being the recovery time. Both buffering and recovery time for each node are already introduced in the GIS layer for each node for the particular scenario to be analysed. This information is thus already available.

The behaviour of each node of the system is represented by a block in Simulink as shown in Figure 2.5(a). This is further elaborated to create the building block shown in Figure 2.5(b). It is clear from this figure that an AND functionality exists in each node, which means that the failure of one of the nodes upon which this node depends, triggers the failure mode of the node concerned. The depiction in Figure 2.5(a) is for the case of a node with only two inputs. This clearly depends on the GIS information and as a consequence from the information in the adjacency matrix. The input connectivity is modified accordingly in order to reflect the connectivity to more nodes. Finally a Matlab function is implemented (see Figure 2.5(c)) in order to perform the threshold check for the node state. This threshold is also inserted through the GIS system. The input parameters that are required for performing the Simulink simulation are the following:

- The failure rate of a node i, f$_i$
- The recovery rate of a node i, r$_i$
- The threshold rate of a node i, th_i

As future work, it is foreseen to offer the capability to define the behaviour of nodes through a drop-down menu of available functions within the GIS layer. The input requirements will be obviously modified accordingly.

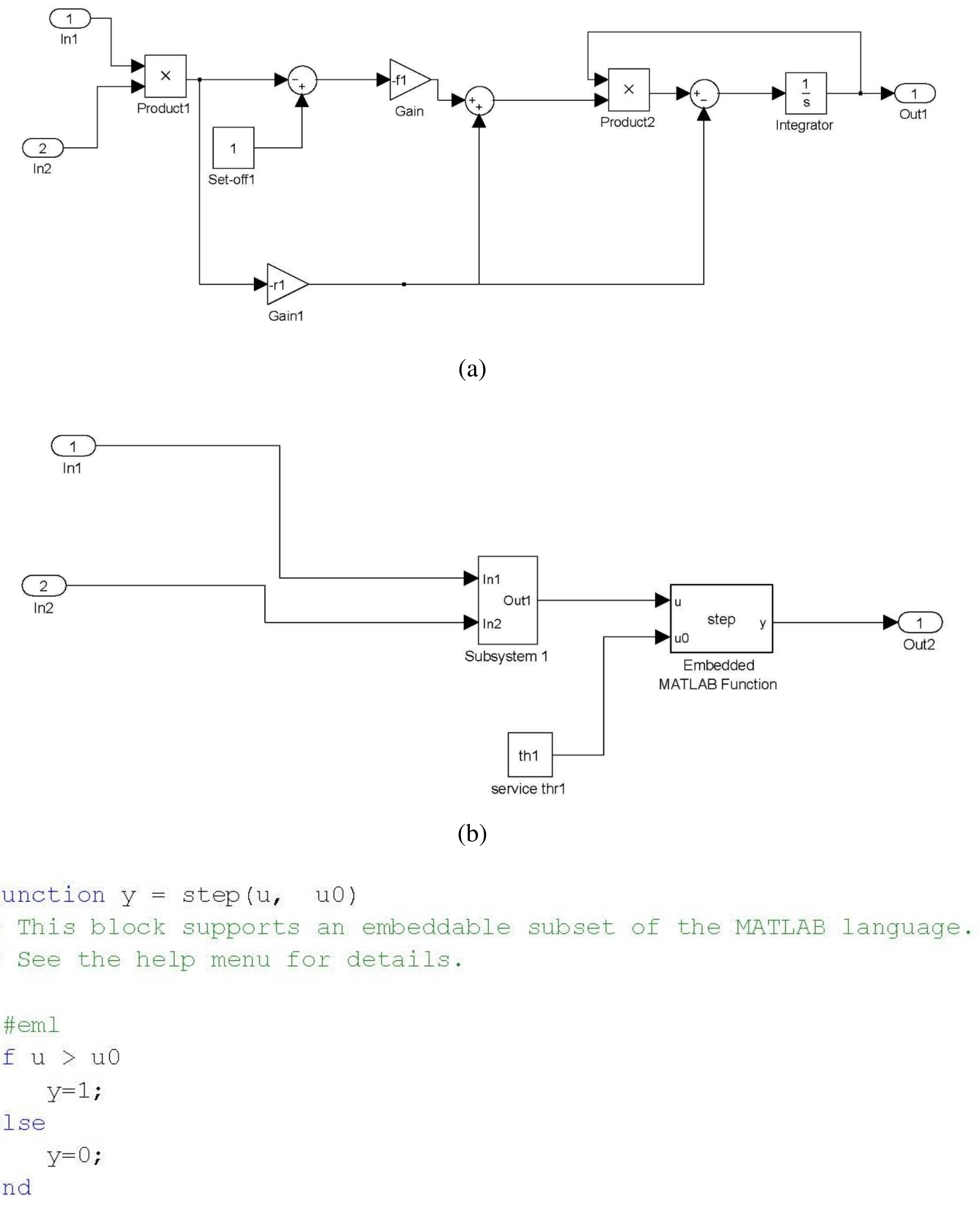
An additional category of nodes is also implemented, the so called directly affected nodes. In that case it is not necessary to simulate the performance of the node because its behaviour is defined by the perturbation vector. In Simulink terminology this is translated to a pulse generator that is linked to this node and it is used to inject a perturbation signal. The Simulink model of the directly affected node (or nodes) is shown in Figure 2.6. Again the connectivity of this Simulink block is defined by the adjacency matrix. For this reason in 2.6 the node depicted has two outputs since two different nodes are connected to this node (see below in Figure 2.8).

2.5 A proof of concept for a simplified System of Systems

In order to demonstrate the validity of the approach a simple case study with 6 nodes is simulated. For the purposes of this proof of concept we can safely assume that each of these nodes represents a different infrastructure assuming thus an abstraction of information at high level. The network topology as well as the necessary parameters for each node is exported from the GIS system.

A disruptive event is simulated by injecting a perturbation (in the form of a step function) to one of the system nodes. In the present example the perturbation is injected in node 2. Node 1 that is directionally connected to node 2 is not considered any more in the analysis since it is totally disconnected from the rest of the network. The failure time t_f defines the duration for which the node is considered to be in failure mode. In Simulink this perturbation is inserted through the Pulse Generator block as shown in Figure 2.6 but the perturbation value is inserted already through the GIS layer.

Once the model is finalized and the disturbance is injected into the directly affected



(a)

(b)

```
function y = step(u,  u0)
% This block supports an embeddable subset of the MATLAB language.
% See the help menu for details.

%#eml
if u > u0
    y=1;
else
    y=0;
end
```

(c)

Figure 2.5: *SIMULINK model of the dependent node a) Behaviour model of the node b) Connectivity model (subsystem1 is represented in Figure 2.5(a)) c) Matlab code for threshold check*

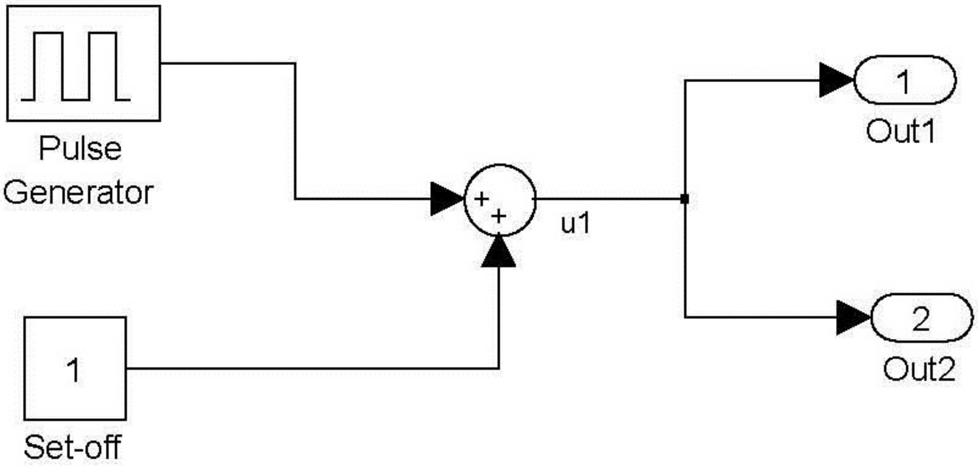
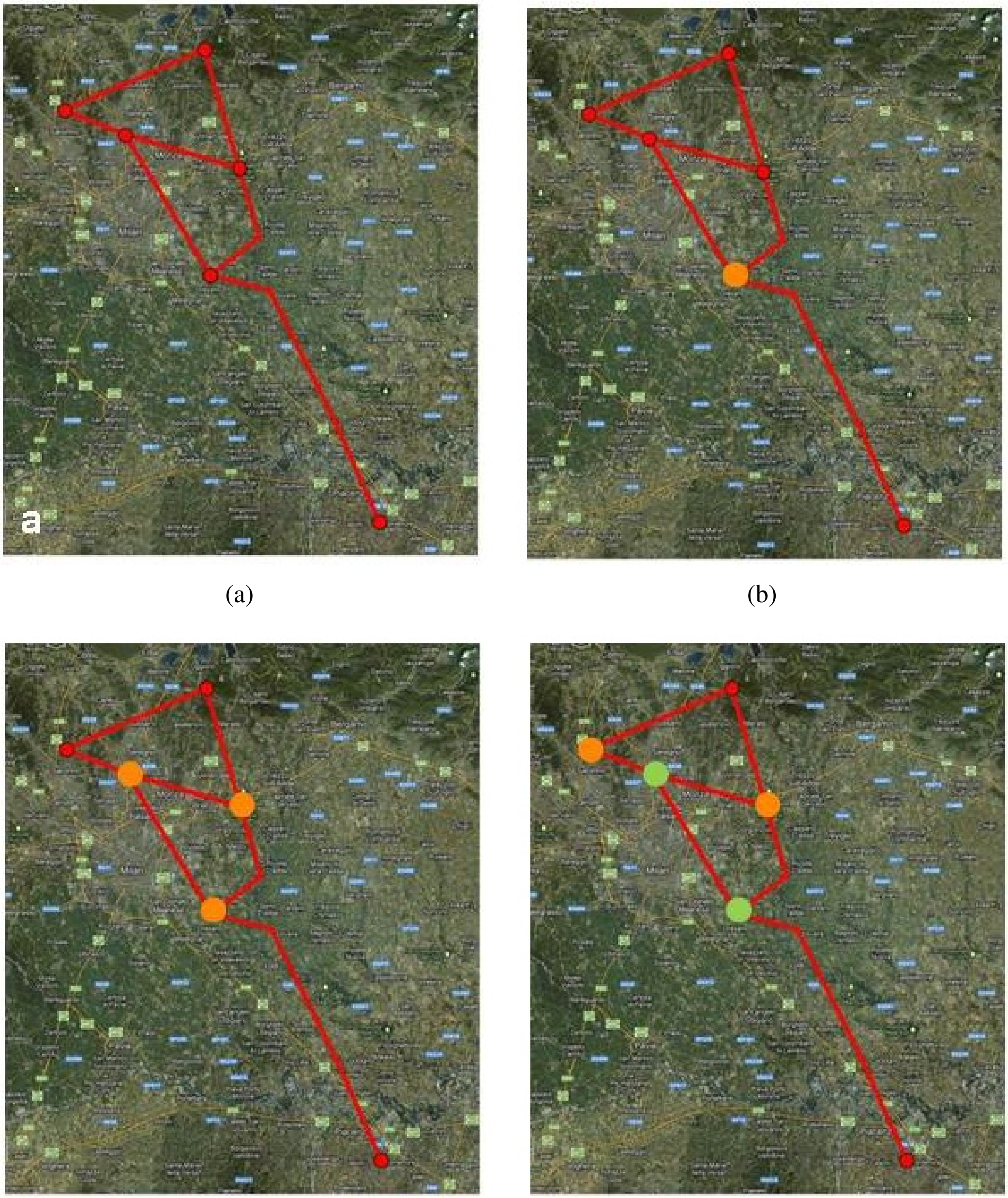


Figure 2.6: *SIMULINK model of the directly affected node*

node, the perturbation on the remaining nodes and the full network can be simulated by choosing the duration of the event. The simulation results can be easily visualised using plots of level of service versus time, as presented in Figure 2.9, or on the GIS system, as shown in Figure 2.7(c) and 2.7(d). Moreover, the results can be saved in MS Excel files, which can be easily accessed and used for further analysis by other systems.

The results presented in Figure 2.9 showed that, for the network analysed, the failure of Node 2 (Figure 2.9(a)) would lead to a complete failure of the network (Figure 2.9(b)). The values of the failure and recovery rates are set to the value of 1 time unit for all the nodes, while the thresholds are set to the value of 0.5. The failure time of Node 2 is set to 2.5 time units. Although nodes, 3,4, and 5, respectively, manage to recover for a short period of time (Figures 2.9(c) 2.9(e)), the failure and late recovery of Node 6 (Figure 2.9(f)) will ultimately lead to the complete failure of the critical infrastructure network. Thus the network configuration and each node's parameters are critical in order to understand its dynamic behaviour in case of disruption. Furthermore this is the point where the concept of resilience enters the stage. As future development of the present work a resilience assessment module is foreseen to be plugged in.

To sum up, with this methodology and implementation tool it is possible to assess



(a)

(b)

(c)

(d)

Figure 2.7: *a) Extraction of topology from the GIS network; b) Disturbance injection into the critical infrastructure network; c) Failure propagation in the critical infrastructure network; d) Partial recovery of the critical infrastructure network*

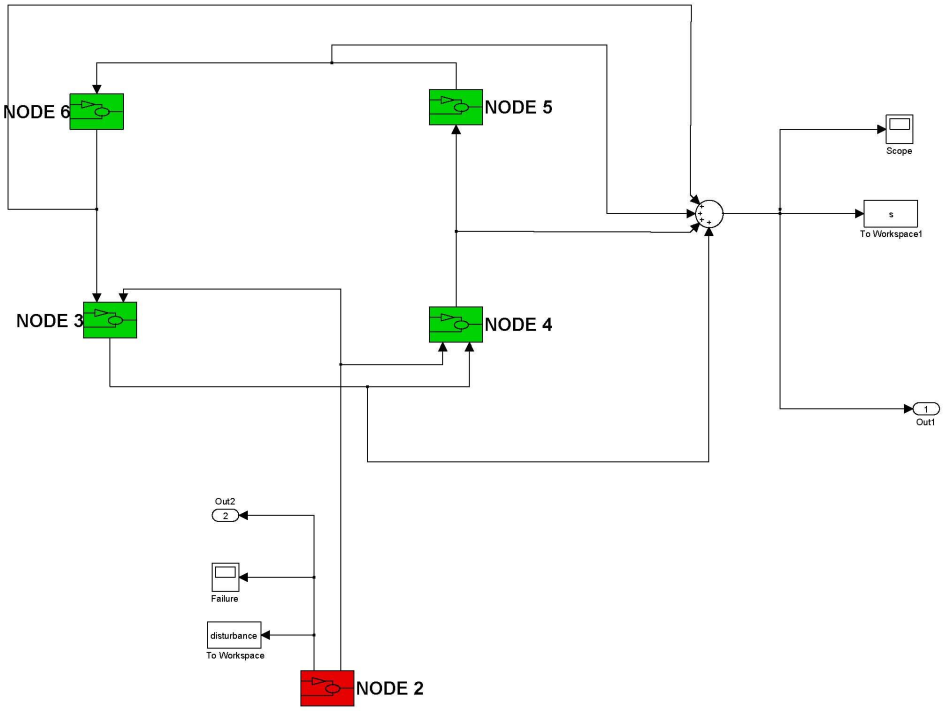


Figure 2.8: *SIMULINK model of the critical infrastructure network*

the impact of a disruptive event on networks of critical infrastructures. This completes an assessment at asset level (not shown in the present work) and actually the asset level assessment can provide the input for defining the parameters for the perturbation to be inserted in the affected node/infrastructure of the present model.

2.6 Conclusions and future work

In this chapter we provided an overview of the modelling approach that has been applied in order to assess the behaviour of networks of critical infrastructures due to a disruptive event. The methodology can be applied to assess both a sector or interdependent sectors of critical infrastructures. It complements the various efforts that exist for the assessment of risks at asset level with minimum data requirements which is critical for policy makers that need a tool for having simulations in short periods of time. Clearly this

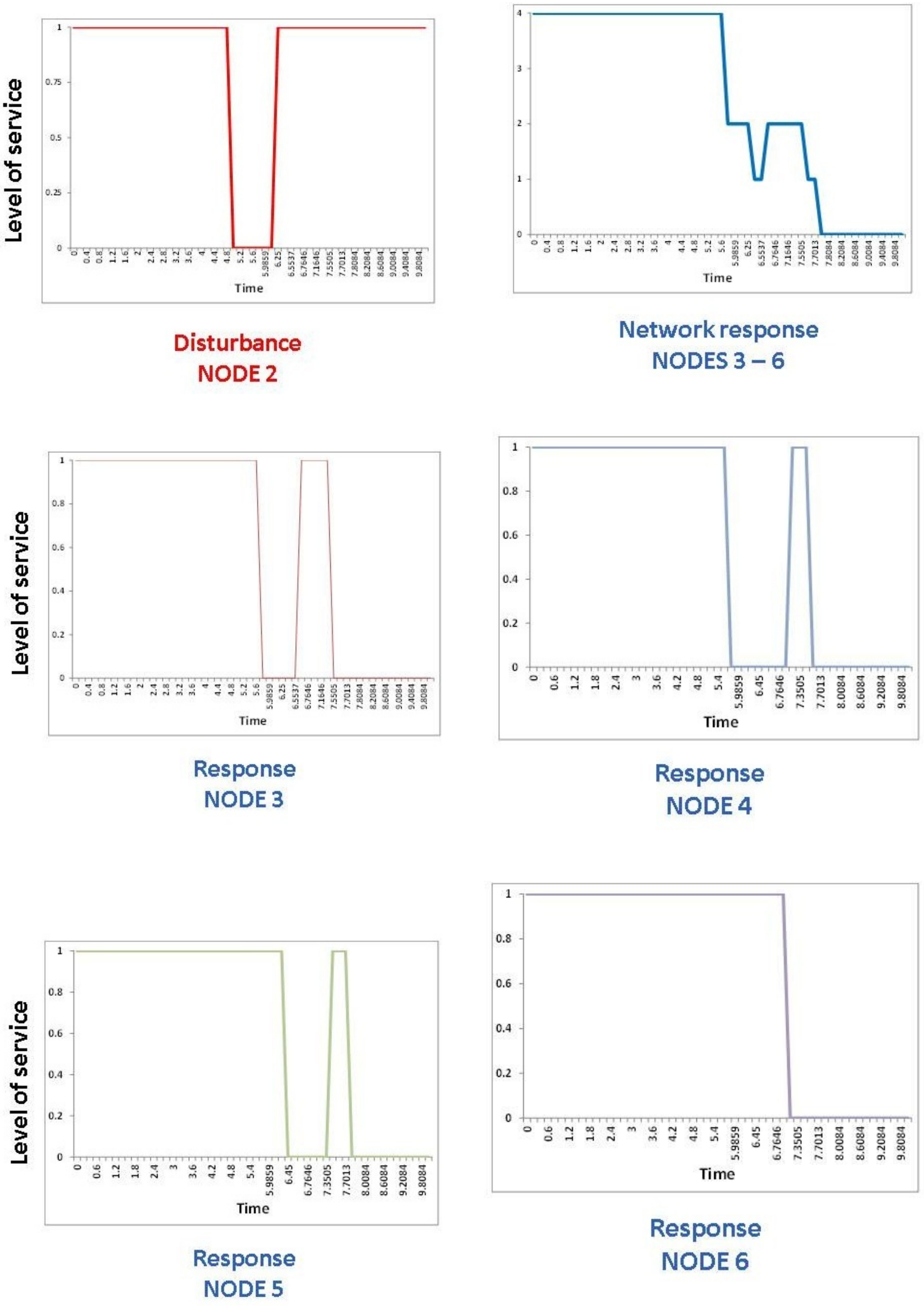


Figure 2.9: *Simulation results of the critical infrastructure network SIMULINK model: a) Disturbance on the directly affected node; Response of the b) remaining network; c) Node 3; d) Node 4; e) Node 5; f) Node 6 to the failure of the directly affected node f)Reporting and visualisation of the results*

methodology requires a certain level of information abstraction. Using the input from this analysis, it is possible to assess the economic impact of critical infrastructures disruption using the I/O modelling approach that is explained in the next chapter.

The information required by the system-engineering model, is dependent not only on the type of critical infrastructure considered, but it could be as well a function of the type of threat that causes the disruption. For this reason, the development of a library of models for the systems behaviour based on these two categories is required and will be consider for the future development of the present version of the model. Moreover, the GIS will be able to automatically recognise the type of data required for each of the plugged models and adapt the input fields accordingly. A further development of the system-engineering model is the representation of the critical infrastructure behaviour based on an inoperability input-output model ([26]) in order to expand its applicability to systems with topological interdependencies that entail flows of goods in a continuous way. It will be thus possible to model such systems at a high level of abstraction.

Chapter 3

Economic modelling of critical infrastructure disruption

3.1 Introduction

The disruption of critical infrastructures may have a significant impact at economic level, especially for large scale infrastructures such as energy sector, telecommunications sector, etc. The notion of economic impact of critical infrastructures is clearly mentioned in the EPCIP Directive. The cross-cutting criteria refer to the economic impact of critical infrastructure disruption as a means to verify the criticality of an infrastructure at European level. Thus it is clear that when it comes to risk assessment of critical infrastructures the economic risk should be certainly considered.

The risk assessment methodology in the present work is focused on the economic impact of critical infrastructure disruption. The high level objectives for the economic impact component are the following:

- Quantify the effects caused by various events (all-hazards approach)

- Quantify indirect effects, so effects that cascade from one CI to the other due to interdependencies
- Quantify effects resulting from failure of all kinds of infrastructures
- Regard the “workforce” as a CI
- Take into account the spatial dimension of the effects
- Incorporate elements of resilience
- Consider also effects on supply chains
- Consider a probabilistic approach
- Be applicable at European level (all 27 Member States).

A literature study ([27]) revealed that several methods for calculating the economic impact of infrastructure service interruptions have been developed. This study has been used for guidance in order to select the appropriate method for evaluating the economic impact of critical infrastructure disruption. The conclusion of [27] was that I-O(Input-Output) modelling is the most suitable. I-O models have been praised for its simplicity and at the same time are criticised for their limitations. However, in recent years many limitations of this type of models have been tackled. Nowadays, they have the ability to include recovery dynamics and allow for probabilistic analyses, only to mention a few of the past shortcomings for which this methodology has been heavily criticised.

3.1.1 The IIM

The type of I-O model chosen is an IIM model. It is derived from Wassily Leontiefs I-O model of the economy ([28], [29]). The formulation of the original I-O model is given in Equation 3.1, where x_i represents the total production output of sector i. The technical coefficient a_{ij} represents the ratio of the input from sector i to sector j and the overall production requirements of sector j. Finally c_i indicates the final demand of the i^{th} sector.

$$x_i = a_{ij}x_j + c_j \tag{3.1}$$

Taking this classic model as a starting point, Santos and Haimes ([30]) proposed the demand-reduction IIM using the following formulation:

$$q = A^*q + c^* \tag{3.2}$$

Where q is the inoperability vector expressed in terms of relative loss. The elements of the vector q represent the ratio of unrealized production with respect to the "as-planned" production level of the industry sectors. A^* is the interdependency matrix that indicates the degree of coupling of the industry sectors. The elements in a particular row of this matrix (see Equation 3.3) indicate the amount of additional inoperability that is contributed by a "column" industry to the "row" industry. x̂ is the production potential of industry i. Finally, c^* is a demand-side perturbation vector expressed in terms of relative degraded final demand.

$$A^* = \begin{pmatrix} a_{11}\left(\frac{\hat{x_1}}{\hat{x_1}}\right) & \dots & a_{1j}\left(\frac{\hat{x_j}}{\hat{x_1}}\right) & \dots & a_{1n}\left(\frac{\hat{x_n}}{\hat{x_1}}\right) \\ \dots & \dots & \dots & \dots & \dots \\ a_{i1}\left(\frac{\hat{x_1}}{\hat{x_i}}\right) & \dots & a_{ij}\left(\frac{\hat{x_j}}{\hat{x_i}}\right) & \dots & a_{in}\left(\frac{\hat{x_n}}{\hat{x_i}}\right) \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1}\left(\frac{\hat{x_1}}{\hat{x_n}}\right) & \dots & a_{nj}\left(\frac{\hat{x_j}}{\hat{x_n}}\right) & \dots & a_{nn}\left(\frac{\hat{x_n}}{\hat{x_n}}\right) \end{pmatrix} \tag{3.3}$$

Equation 3.3 is rewritten as:

$$q = (I - A^*)^{-1} c^* \tag{3.4}$$

Let us then define $(I - A^*)^{-1}$ as B^*. Supposing that B^* exists (in mathematical terms $det(I - A^*)^{-1} \neq 0$), the elements b_{ij} of B^* represent the overall inoperability transmission, i.e., the amount of the inoperability injected in the system by an external failure c^* that is transmitted to the i^{th} infrastructure taking into account first, second and higher order dependencies. Note that this is different from the elements a^*_{ij} of matrix A^*, which only take into account direct influences. Finally, in order to estimate the economic losses δx, the inoperability of sector i (q_i) is multiplied with its corresponding "as-planned" production (x_i), which is:

$$\delta x = diag(q)x \tag{3.5}$$

Where $diag(q)$ is a diagonal matrix formed from q.

As a consequence, two metrics are produced by the IIM: inoperability (q) and economic losses (δx). The term inoperability connotes the level of a system's dysfunction expressed as a percentage of its "as-planned" production capacity. The inoperability caused by deliberate attacks, accidents or natural hazards can set of a chain of cascading impacts on other interconnected systems. So, inoperability refers to normalised production loss which can be defined as ([30]):

$$\text{Normalized production loss} = \frac{\text{“As-planned” production - Degraded production}}{\text{Nominal production}} \tag{3.6}$$

Each element of the vector q falls between the interval $[0, 1]$. If an element of this vector is 0, it means "business as usual" operation; if an element is 1, it implies that the corresponding industry is completely inoperable or fully incapable of production.

Economic losses can be defined as stock damage or flow losses (or business interruption losses). In economics, flows refer to the services or outputs of stocks over time while stocks refer to a quantity at a single point in time. Property damage represents a decline in stock value and usually leads to a decrease in service flows. Flow losses originate only in part from a company's own property damage and can occur without the presence of property damage [31]. Both, stock damage and flow effects can be of direct or indirect nature. Direct effects are sustained by the sector that is hit by a particular hazard. Indirect effects impact on sectors that are located in the close vicinity of the initially hit sector (indirect stock damage) or that are dependent on the initially hit sector through supply and demand relationships (indirect flow effects). Table 3.1 summarises the different types of economic impact.

Table 3.1: *Classification of economic impacts*

	Stock damage	**Flow effects/losses**
Direct	Property damage in hit sector	Business interruptions in hit sector
Indirect	Via hazardous material releases from originally hit sector	Via suppliers/ customers relations

Input-Output (I-O) models, and thus also the IIM, ignore stock damages and only take into account direct and indirect flow losses. Including both stock damages and flow losses would result in double counting. The value of an asset, which, for example, could be equipment pertaining to an infrastructure, is the discounted flow of net future returns from its operation. So suppose that a machine with a 1-year lifespan is destroyed, and not replaced for a year, then the economic loss is equal to either the value of a replacement machine with a 1-year lifespan or the discounted flow of not produced output for one year ([32]).

Greenberg et al. ([33]) claim that the IIM is one of the ten most important accomplishments in risk analysis in the past 30 years. The prove for this statement can be found in for example, Crowther and Haimes ([34]), Barker and Haimes ([35], [36]), Lian and Haimes

([37]) or Lian et al. ([38]). The next section is focused on the position of IIM analysis in risk assessment.

3.1.2 The IIM and risk assessment

The IIM presents a perspective of interdependencies to calculate the cascading effects from a deliberate attack, natural disaster, or security measures. The flowchart in Figure 3.1 illustrates how these perspectives can be used in risk assessment. Direct impacts (perturbations in the c^* vector) from sector risks are input to the IIM for interdependency analysis. Jonkeren et al. ([39])[1] demonstrate a good example of how the IIM can be applied for risk assessment purposes. The study performs interdependency analysis for an assessment of the total consequences to an EU Member State (Italy) resulting from a disturbance to the power infrastructure. The IIM is fed by the systems engineering model described in previous chapter. Once the probability of disturbances is known, in combination with the model output on economic losses, the risk which the infrastructure system is subject to, can be determined.

3.1.3 The IIM and resilience: the DIIM

Because several applications of the static IIM have proven its feasibility for research on economic consequences of Critical Infrastructure failure ([40], [41]), the model was extended with the economic resilience aspect. In Rose ([42]) defines economic resilience as the ability of an entity or system to maintain function when shocked. The first type of resilience that was added to the IIM is restorative resilience or the speed of recovery after a disruption (Haimes et al. [43]; [44]). Including this type of resilience changes the static IIM into a DIIM (Dynamic IIM). Depending on the rate of recovery for economic sectors,

[1] A more recent version of this paper was submitted to the International Journal of Critical Infrastructure Protection and is under review at the time of writing this report.

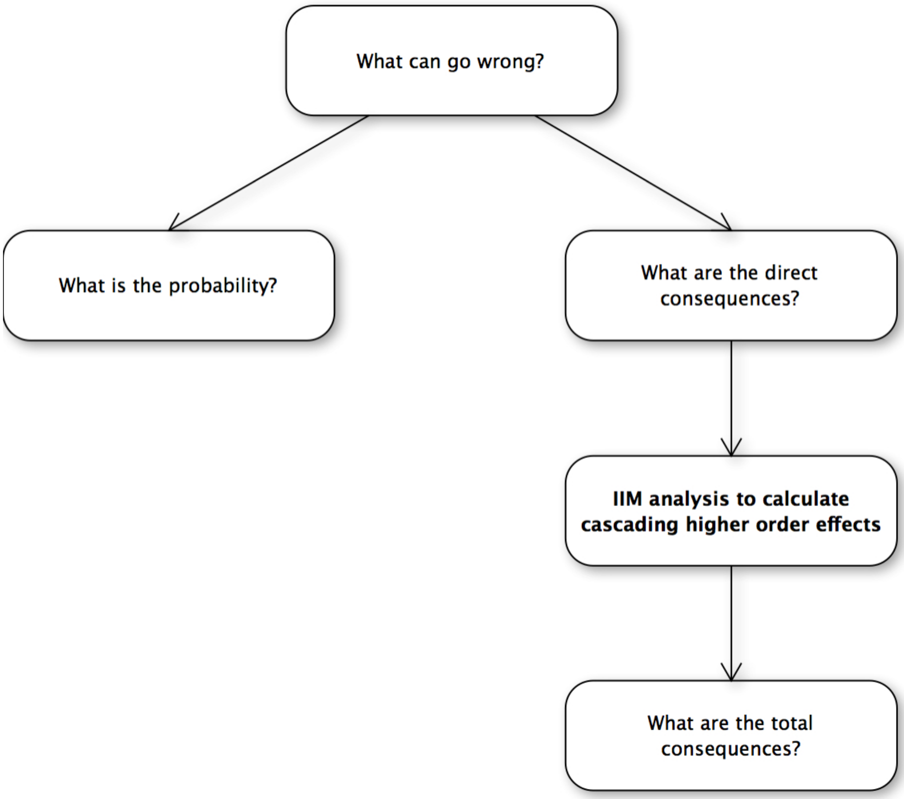

What can go wrong?
What is the probability?
What are the direct consequences?
IIM analysis to calculate cascading higher order effects
What are the total consequences?

Figure 3.1: *IIM analysis in risk assessment process (Source: Crowther and Haimes, 2005)*

inoperability levels and economic losses are estimated for each time period t (which can be defined in days, weeks or months) and for each sector. Mathematically the model is described in Equation 3.7.

$$q(t+1) = q(t) + K\left[c(t) - q(t) + Aq(t)\right] \tag{3.7}$$

where K is the sector resilience matrix which has values between 0 and 1 on its diagonal and zeros elsewhere. Each resilience coefficient k_i in the matrix K is determined by the nature of the individual sector itself as well as the controls on it via risk management policies. Hardening of infrastructures and other risk mitigation efforts in the economic sectors increase k_i. Consequently, inoperability levels and economic losses are reduced with shorter recovery times.

A second type of economic resilience is “adaptive resilience” which refers to the change in the speed of recovery of a sector during the recovery period. Recovery speed could vary over time because recovery accelerates for example. This may happen when the workforce available for repair works to destroyed gas pipelines in a particular region increases with t. The values of k_{gas} in the K matrix increase over time in this example. The last type of resilience we explicitly take into account in our model is “absorptive resilience” which is a measure for the buffering capacity of a sector. With the two previously mentioned types of resilience, the DIIM lacks the ability to capture risk management strategies that maintain essential services, or delay the onset of inoperability. By combining the DIIM with the concept of “inventory”, absorptive resilience can be included in the model. Inventory can be represented by finished goods or some other method by which the infrastructures ability to provide goods or services to other infrastructures, sectors and final consumers is maintained while the infrastructure is disrupted. For example, inventory in the oil and gas sector could include excess stored gasoline ready for use, and redundancies in the electric power sector, where energy cannot be stored, could include back up generators that can provide some amount of total output to be maintained ([45]). Inventory is included in the model by adding an extra variable to Equation 3.7. In order to make this report not too technical the mathematical details of this extension are left out. The resilience types described in this section are summarised in Figure 3.2.

In the Inventory-DIIM, Equation 3.7 is taken as a starting point and then extended with two extra variables, namely the production inoperability $p_i(t)$ and the inventory level $X_i(t)$ (see Equation 3.8).

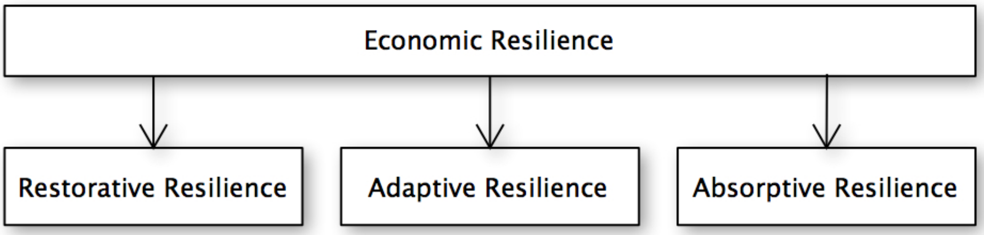


Figure 3.2: *Types of economic resilience.*

$$
q_i(t+1) = \begin{cases}
q_i(t) + k_i[c_i^*(t) - q_i(t) + \sum_{j=1}^{n} a_{ij}^* q_j(t)] & \text{if } X_i(t) \geq p_i(t+1)x_i(t+1) \\
max \begin{cases} p_i(t+1) - \frac{X_i(t+1)}{x_i(t+1)} \\ q_i(t) + k_i[c_i^*(t) - q_i(t) + \sum_{j=1}^{n} a_{ij}^* q_j(t)] \end{cases} & \text{if } 0 < X_i(t) < p_i(t+1)x_i(t+1) \\
max \begin{cases} p_i(t+1) \\ q_i(t) + k_i[c_i^*(t) - q_i(t) + \sum_{j=1}^{n} a_{ij}^* q_j(t)] \end{cases} & \text{if } X_i(t) = 0, X_i(t) > 0 \\
q_i(t) + k_i[c_i^*(t) - q_i(t) + \sum_{j=1}^{n} a_{ij}^* q_j(t)] & \text{if } X_i(t+1) = X_i(t) = 0
\end{cases} \tag{3.8}
$$

The production inoperability of sector i at the end of time t, describes inoperability of the production process due only to a physical disturbance in that process. The inventory level $X_i(t)$ quantifies the amount of inventory in sector i remaining at the end of time t ([45]). Sector inoperability is initialised with Equation 3.9. The term $X_i(t)$ describes the total output anticipated to be produced by sector i between the end of time $t-1$ and the end of time t. Naturally, if enough inventory is available to cover the output reduction caused by the initial production inoperability, defined as $p_i(0)x_i(0)$, then $q_i(0) = 0$. If some inventory is available, but not enough to cover the output reduction, sector inoperability is a function of the fraction of inventory used to meet the output reduction. Finally, if no inventory is available, the initial sector inoperability is brought about entirely by the physical production inoperability experienced by the sector.

$$q_i(0) = \begin{cases} 0 & \text{if } X_i(0) \geq p_i(0)x_i(0) \\ 1 - \frac{X_i(0)}{p_i(0)x_i(0)} & \text{if } 0 < X_i(0) < p_i(0)x_i(0) \\ p_i(0) & \text{if } X_i(0) = 0 \end{cases} \tag{3.9}$$

3.1.4 Data required for the I-O model

The A^* matrices at the country level in the IIM are fed with I-O data provided by the WIOD(World Input-Output Database)[2]. On April 16 2012 the World Input-Output Database (WIOD) was opened for the general public. This database has been developed to analyse the effects of globalisation on trade patterns, environmental pressures and socio-economic development across a wide set of countries and can also be used for economic loss analyses. The database covers 27 EU countries and 13 other major countries in the world for the period from 1995 to 2009. The WIOD project is funded by the European Commission, Research Directorate General as part of the 7^{th} Framework Programme, Theme 8: *Socio-Economic Sciences and Humanities*.

The WIOD national I-O tables consider 35 industries within an economy. Eight of them can be identified as critical infrastructure industries and four as being a KRSC (Key Resource Supply Chain) industry. Annual detailed enterprise statistics provided by EUROSTAT (under de topic of “Structural Business Statistics”) allow us to perform economic loss analyses on a more detailed industrial level than the I-O data allow us. For example, these data enable us to assess economic losses for the electricity, gas or water supply industry of an EU country instead of the aggregated “electricity, gas and water supply” industry as considered in the a national I-O table from the WIOD. Table 3.2 provides an overview of the CI and KRSC industries considered in WIOD (where some

[2] See http://www.wiod.org/index.htm

Table 3.2: *CIs and KRSCs considered in the model*

Aggregated (WIOD)	**Disaggregated**
Critical Infrastructure industries	Critical Infrastructure industries
Air transport	Air transport
Electricity, gas, steam and hot water supply	Electricity
Post &TLC	Gas
Water transport	Water
Land transport; transport via pipelines	TLC
Financial intermediation, except insurance and pension funding	Road
Health and social work	Rail
Workforce	Pipeline
	Inland waterway transport
Key Resources Supply Chain industries	Maritime transport
Food, beverages, tobacco	Finance
Transport equipment	Health
Wholesale trade	Workforce
Retail trade	
	Key Resources Supply Chain industries
	Food, beverages, tobacco
	Automotive
	Wholesale trade
	Retail trade

are aggregated with others) and the industries after the disaggregation process. Assume, for example, that due to some event the SE model estimates that the electricity industry in Italy becomes inoperable for 40% and that we know on the basis of the detailed enterprise statistics for Italy that the electricity industry is responsible for 75% of the output of the "Electricity, gas, steam and hot water supply" (WIOD) industry. So, we introduce an inoperability of $(0.75 * 0.40) = 0.30$ into this WIOD industry. Hence, 0.30 is the (starting) value for $p_{elec}(0)$ in Equation 3.9 in this example. Data on inventory levels is also derived from the EUROSTAT annual detailed enterprise statistics via the "ratio of stocks of finished products and work in progress to production value" per industry on the country level. This ratio can be interpreted as the amount of inventory available relative to the amount of production. A ratio of 0.5 for the "food, beverages and tobacco" industry in Italy for example implies that there is enough inventory for a duration of $0.5t$ (half a days, week or month) for this industry in this country. Note that for the electricity industry for example, the ratio is likely to be close or equal to zero as it is impossible to store electricity.

3.1.5 Analysis on the regional level

In addition to the Member State level the SE-DIIM is also able to perform economic loss analysis and risk assessments on a lower regional level. However, as the WIOD data only enables us to estimate interdependencies on the national level, performing a spatially explicit analysis requires the recalculation of A^*. After all, intraregional interdependencies are likely to differ from those on the national level. The regional interdependency coefficients are generally estimated using regional multipliers that are constructed from measures of regional production compared to the national ones. In our model, these multipliers are formulated from location quotients, which are ratios that represent the relative production of a sector in a region compared to the nation (see Equation 3.10). Equation 3.11 describes the application of location quotients in estimating intraregional technical coefficients. If industry i is less concentrated in the region than at national level $(lq_i^s < 1)$, it is seen as being less capable of satisfying regional demand with its output. However, if industry i is more highly concentrated in the region than at national level $(lq_i^s \geq 1)$, then it is assumed that the national input coefficients from industry i, a_{ij}^*, apply to the region, and the regional surplus produced by i will be “exported” to the rest of the nation ([46]).

$$lq_i^s = \frac{x_i^s / x^s}{x_i^N / x^N} \tag{3.10}$$

$$a_{ij}^{*s} = \begin{cases} lq_i^s a_{ij}^*, & lq_i^s < 1, \\ a_{ij}^*, & lq_i^s > 1, \end{cases} \tag{3.11}$$

where lq_i^s is the proportion of demand for sector i in region s that is satisfied internally compared to other regions in the nation. x_i^s, x_i^N is the total production output of sector i in region s or the nation N, respectively. x^s, x^N is the total production output of all sectors in region s or nation N. a_{ij}^{*s} is the amount of inoperability experienced in sector i due to total inoperability in sector j in region s. a^*_{ij} is the amount of inoperability experienced in sector i due to total inoperability in sector j in the nation.

The location quotients are based on national and regional employment data provided by EUROSTAT, which is a well-accepted proxy for output data. Note that the dimensions of the regional A^{*s} matrices are equal to the national A^* matrix. The individual entries of the regional matrices have decreased in value or remained the same because each regional matrix, belonging to the same country, is derived from the same national matrix and from location quotients that are strictly between 0 and 1. Intuitively, the values should decrease, because smaller regions are accounted for, and in this case, the degree of interconnectedness between sectors within the individual region decreases as well ([47]).

3.2 Conclusions and future work

At the moment the DIIMs that can be found in the literature assume that economic recovery starts immediately after a disruption of an infrastructure occurs. However, it is likely that in the immediate aftermath of a disaster, industries are not able to start recovery activities because of several practical obstacles. A repair workforce may not be able to reach damaged gas pipelines after an earthquake because the roads are damaged as well for example. Hence, the SE-DIIM should be able to analyze an immediate post disaster period in which there is no recovery (during the first few time periods e.g.) and in which inoperability levels only deteriorate due to inoperability transmission. Figure 3.3 presents the different post-disaster phases that should be distinguished. At $t = 10$ inoperability of the CI is equal to zero again.

Equation 3.8 applies only to the phases 2 and 3. To be able to include phase 1 as well, Equation 3.8 needs to be extended with phase 1. Therefore we have rewritten Equation 3.8 leaving out the recovery aspect (the K variable). The result can be seen in

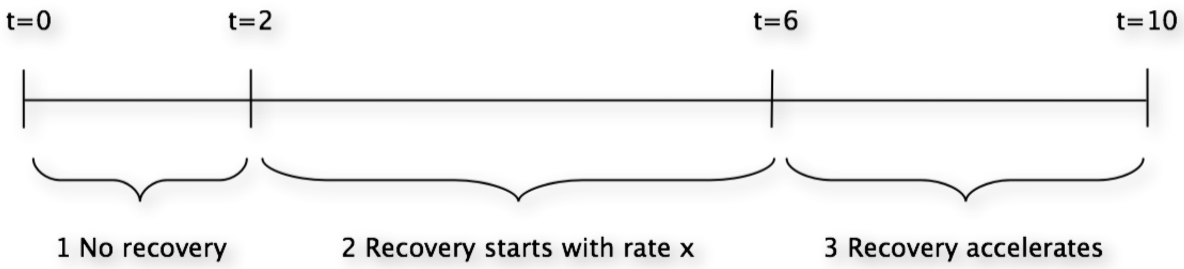


Figure 3.3: *Different phases in post-disaster period*

Equation 3.12. So, together Equation 3.8 and Equation 3.12 cover the three phases visualised in Figure 3.3 and we call the resulting model the Resilience-DIIM. In Equation 3.12, depending on the inventory situation, there are, like in Equation 3.8, four possible scenarios (which are mutually exclusive) to determine inoperability for the next time period. This future inoperability is equal to the maximum of (1) the level of inoperability in the current time period plus any additional inoperability created by a loss of demand or inoperability transmission, or (2) the production inoperability introduced in the next time period.

$$q_i(t+1) = \begin{cases} q_i(t) + c_i^*(t) + \sum\limits_{j=1}^{n} a_{ij}^* q_j(t) & \text{if } X_i(t) \geq p_i(t+1)x_i(t+1) \\ max \begin{cases} p_i(t+1) - \frac{X_i(t+1)}{x_i(t+1)} \\ q_i(t) + c_i^*(t) + \sum\limits_{j=1}^{n} a_{ij}^* q_j(t) \end{cases} & \text{if } 0 < X_i(t) < p_i(t+1)x_i(t+1) \\ max \begin{cases} p_i(t+1) \\ q_i(t) + c_i^*(t) + \sum\limits_{j=1}^{n} a_{ij}^* q_j(t) \end{cases} & \text{if } X_i(t) = 0, X_i(t) > 0 \\ q_i(t) + c_i^*(t) + \sum\limits_{j=1}^{n} a_{ij}^* q_j(t) & \text{if } X_i(t+1) = X_i(t) = 0 \end{cases} \tag{3.12}$$

Although the development of the model for the first post disaster phase is finished, a practical application of it does not exist yet. This is foreseen for the very next future. In section 3.1.3 three types of economic resilience were presented. These resilience types are all at the industry or sectoral level. However, because the amount of inoperability transmission from one infrastructure to the other will be subject to changes in the post disaster phase , there is a need to model resilience at the system or network level as well. This can be achieved by allowing the a_{ij}s (the interdependencies) in the model, which represent the amount of inoperability transmission between industries, to change over time. The key challenge here, is to find a credible method which estimates how these a_{ij}s should change. Setola et al. ([48]) offer an interesting approach here (which is further developed in Oliva et al. ([49])). They estimate IIM parameters for infrastructures whose size depends on the duration of the inoperability of the industries they depend on, using fuzzy logic. They consider five time frames: 1 h, 1-6 h, 6-12 h, 12-24 h and 24-48 h and they assume that there are no recovery activities during these first 48 hours after the disaster event has occurred. So, 48 hours after the disaster event the interdependencies are highest and inoperability transmission is strongest. Then, recovery is assumed to start. What Setola et al. ([48]) do not address however, is what happens to the size of the interdependencies once the recovery phase has started. It is likely that they start shrinking again and at the moment when the system of CIs is fully recovered from the disaster (at $t = 10$ in Figure 3.3) the A^* matrix is likely to be the same A^* matrix as the one at $t = 0$. After all, the system is back in its old equilibrium state then. According to this reasoning, it immediately follows that there should exist a relation between the rate of recovery (K) and the change in interdependencies (A^*). For us, to apply the fuzzy logic methodology to estimate how interdependencies change over time, is time consuming and costly, especially because we work with a larger system (the 35x35 A^* matrices WIOD tables) than Setola et al. ([48]) who use an 11x11 system. We will therefore explore the possibility of estimating functions for the change in interdependencies for the system of CIs presented in Setola et al. ([48]) and use these functions for our set of CIs. Finally, the original formulation of the Resilience-DIIM only allows for a single perturbation vector.

In the future however, the DIIM is foreseen to be able to account for disturbances to industries in the economy that are probabilistic, which implies to allow the Resilience-DIIM to use a perturbation matrix as inputs to the model. This will result in inoperability and economic loss matrices as being the output of the model. For an example of this extension see [50].

Bibliography

[1] European Commission, *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*, Official Journal of the European Union, L345/75, 2008

[2] Ghorbani, A.A., Bagheri, E. *The state of the art in critical infrastructure protection: a framework for convergence, International Journal of Critical Infrastructures*, Vol.2, No.4, 312, 2008

[3] Georgios Giannopoulos, Muriel Schimmer, *VII Workshop on the Implementation and Application of the Directive 2008/114/EC*, Pubsy JRC72080

[4] Sergio Contini, Vaidas Matuzas, *Analysis of large fault trees based on functional decomposition*, Reliability Engineering & System Safety, Vol. 96, no. 3, 383-390

[5] Georgios Giannopoulos, Roberto Filippini, Muriel Schimmer, *Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art*, EUR 25286

[6] Sole, R.V., Casals, M.R., Murtra, B.C., Valverde, S. *Robustness of the European power grids under intentional attack*, Physical Review E, 77, 0206102, 2008

[7] Trucco, P., Cagno, E., De Ambroggy, M. *Dynamic functional modelling of vulnerability and interoperability of critical infrastructures*, Reliability Engineering and System Safety, 105,

[8] Bloomfield, R., Chozos, N., Nobles, P. *Infrastructure interdependency analysis: requirements, capabilities and strategy*, Adelard document reference: D/422/12101/4, 2009, http://www.csr.city.ac.uk/projects/cetifs/d422v10_review.pdf

[9] Yusta, J.M., Correa, G.J., Lacal-Arantegui, R. *Methodologies and applications for critical infrastructure protection: State-of-the-art*, Energy Policy, 39, 6100, 2011

[10] Carcano, A., Coletta, A., Guglielmi, M., Masera, M., Nai Fovino, I., Trombetta, A. A multidimensional critical state analysis for detecting intrusions in SCADA systems, IEEE Transactions on Industrial Informatics, 7, 179, 2011

[11] Eusgeld, I., Nan, C., Dietz, S. *System-of-systems approach for interdependent critical infrastructures*, Reliability Engineering and System Safety, 96, 679, 2011

[12] Merabti, M., Kennedy, M., Hurst, W. Critical infrastructure protection: A 21st century challenge, International conference on communications and information technology, 2011

[13] Di Mauro, C., Bouchon, S., Logtmeijer, C., Pride, R.D., Hartung, T., Nordvik, J.P. *A structured approach to identifying European critical infrastructures*, International Journal of Critical infrastructures, 6, 3, 277, 2010

[14] Filippini, R., Silva. A. *Resilience analysis of networked systems-of-systems based on structural and dynamic interdependencies*, Proceedings of the 11th International probabilistic safety assessment and management conference and the Annual European safety and reliability conference, Curran Associates, Inc., ISBN 978-162-276-436-5, 2012

[15] Georgios Giannopoulos, Roberto Filippini, *Interdependencies and Resilience assessment methodology for CI*, Pubsy 75761

[16] Andersson, G. *Modelling and analysis of electric power systems*, Lecture 227-0523-00, Swiss Federal Institute of Technology (ETH) Zurich, 2008

[17] Rigole, T., Deconinck, G. *A survey on modelling and simulation of interdependent critical infrastructures*, 3^{rd} IEEE Benelux Young Researchers Symposium in Electrical Power Engineering, Paper 44, 2006

[18] Wilde, W.D., Warren, M.J. *Visualisation of critical infrastructure failure*, Proceedings of the 9^{th} Australian information warfare and security conference, 48, 2008

[19] Steven M. Rinaldi, James P. Peerenboom, Terrence K. Kelly, *Identifying, understanding, and analysing critical infrastructure interdependencies*, IEEE Control Systems Magazine, December 2001, pages 11-25.

[20] Bird, B.R., Stewart, W.E., Lightfoot, E.N. *Transport phenomena*, John Wiley & Sons, 2002

[21] Oliva, G., Panzieri, S., Setola, R. *Agent-based input-output interdependency model*, International journal of critical infrastructure protection, 3, 76, 2010

[22] Min, H.S., Beyeler, W., Brown, T., Son, Y.J., Jones, A. *Toward modelling and simulation of critical national infrastructure interdependencies*, IIE Transactions, Vol. 39, No. 1, 57, 2007

[23] Georgios Giannopoulos, Ivano Azzini, Structural analysis of critical infrastructure networks, Pubsy Report JRC 78274, Luxemburg: Publications Office of the European Union

[24] Krausmann E., Girgin S., *Rapid Natech Risk Assessment and Mapping Tool for Earthquakes: RAPID-N*, Chemical Engineering Transactions, vol. 26, no 1, 93-98, 2012

[25] Matlab 7.10.0 (R2010a), The Mathworks Inc., 2010

[26] Santos, J.R., Haimes, Y.Y. *Modelling the demand reduction input-output (I-O) Inoperability due to terrorism of interconnected infrastructures*, Risk Analysis, 24, 6, 1437, 2004 51, 2012

[27] Jonkeren, O.E., *Assessment of potential methodologies to analyse (micro level) economic impact of infrastructure failure*, Pubsy report JRC 65993, Luxembourg: Publications Office of the European Union.

[28] Leontief W. W. *Input-output economics*, Sci Amer 185, 4, 15-21, 1951

[29] Leontief W. W. *The structure of the american economy*, 1919-1939, 2nd edition, Oxford University Press, New York, 1951

[30] Santos J. R., Haimes Y. Y. Modeling the Demand Reduction Input-Output (I-O) Inoperability Due to Terrorism of Interconnected Infrastructures, Risk Analysis, 24, 6, 1437-1451, 2004

[31] Rose A Z. *A Framework for Analyzing the Total Economic Impacts of Terrorist Attacks and Natural Disasters*, Journal of Homeland Security and Emergency Management, 6, 1, art.9, 2009

[32] Rose A Z., Lim, D. *Business interruption losses from natural hazards: conceptual and methodological issues in the case of the Northridge earthquake*, Environmental Hazards, 4, 1-14., 2002

[33] Greenberg M., Haas, C, Cox Jr. A, Lowrie K, McComas K, North W. *Ten Most Important Accomplishments in Risk Analysis*, 1980-2010, Risk Analysis, 32, 5, 771-781, 2012

[34] Crowther K.G., Haimes Y.Y. *Application of the Inoperability Input-Output Model (IIM) for Systemic Risk Assessment and Management of Interdependent Infrastructures*, Systems Engineering, 8, 4, 323-341, 2005

[35] Barker K., Haimes Y.Y., *Assessing uncertainty in extreme events: Applications to risk-based decision making in interdependent infrastructure sectors*, Reliability Engineering and System Safety, 94, 819-829, 2009

[36] Barker K., Haimes Y.Y., *Uncertainty analysis of Interdependencies in Dynamic Infrastructure Recovey: Applications in Risk-Based Decision Making*, Journal of Infrastructure Systems, 15, 4, 394-405, 2009

[37] Lian C., Haimes Y.Y., *Managing the Risk of Terrorism to Interdependent Infrastructure Systems Through the Dynamic Inoperability Input-Output Model*, Systems Engineering, 9, 3, 241-258.

[38] Lian C., Santos, J.R., Haimes, Y.Y. *Extreme Risk Analysis of Interdependent Economic and Infrastructure Sectors*, Risk Analysis, 27, 4, 1053-1064, 2007

[39] , Jonkeren, O.E., Ward, D., Dorneanu, B., Giannopoulos, G. *Interdependencies and economic assessment of critical infrastructure in the EU: A combined system engineering and economic model*, Proceedings of the 11^{th} International probabilistic safety assessment and management conference and the Annual European safety and reliability conference, Curran Associates, Inc., ISBN 978-162-276-436-5, 2012

[40] Jonkeren, O., Dorneanu, B., Giannopoulos, G., Ward, D., *Regional economic assessment of Critical Infrastructure failure in the EU: A combined systems engineering and economic model*, ERSA Conference paper, number ersa12p92.

[41] Jonkeren, O., Ward, D. *Modelling Economic Consequences of ICT Infrastructure Failure in support of Critical Infrastructure Protection Policies*, in: Bologna, S.; Theron, P. (eds.): Critical Information Infrastructure Protection and Resilience in the ICT Sector, IGI Global, forthcoming, 2013

[42] Rose A. Z., *Economic resilience to natural and man-made disasters: Multidisciplinary origins and contextual dimensions*, Environmental Hazards, 7, 383-398, 2007

[43] Haimes, Y.Y., Horowitz, B.M., Lambert, J.H., Santos, J.R., Lian, C., Crowther, K.G. *Inoperability input-output model for interdependent infrastructure sectors. I: Theory and methodology*, Journal of Infrastructure Systems, 11, 2, 67-79, 2005

[44] Haimes, Y.Y., Horowitz, B.M., Lambert, J.H., Santos, J.R., Crowther, K.G., and Lian, C. *Inoperability Input-Output Model for Interdependent Infrastructure Sectors. II: Case Studies*, Journal of Infrastructure Systems, 11, 2, 80-92, 2005

[45] Barker K., Santos, J.R. *Measuring the efficacy of inventory with a dynamic input-output model*, International Journal of Production Economics, 126, 130-143, 2010

[46] Miller R E., Blair P D. *Input-Output Analysis: Foundations and Extensions*, 2nd edition, Cambridge University Press, Cambridge., 2009

[47] Crowther K.G., Haimes Y.Y. *Development of the Multiregional Inoperability Input-Output Model (MRIIM) for Spatial Explicitness in Preparedness of Interdependent Regions*, Systems Engineering, 13, 1, 28-46, 2010

[48] Setola R., De Porcellinis S., Sforna, M., *Critical infrastructure dependency assessment using the input-output inoperability model*, International Journal of Critical Infrastructure Protection, 2, 170-178, 2009

[49] Oliva G., Panzieri S., Setola R. *Fuzzy dynamic input-output inoperability model*, International Journal of Critical Infrastructure Protection, 4, 165-175, 2011

[50] Orsi, M.J., Santos, J.R., *Incorporating Time-Varying Perturbations Into the Dynamic Inoperability Input-Output Model*, IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans, 40, 1, 100-106., 2010

[51] Rocco, S.C.M, Ramirez-Marquez, J.E., Salazar, A.D.E. *Some metrics for assessing the vulnerability of complex networks: An application to an electric power system*, Advances in safety, reliability and risk management, Berenguer, Grall and Guedes Soares, ISBN 978-0-415-689379-1, 2256, 2012

European Commission
EUR 25745 EN – Joint Research Centre – Institute for Protection and Security of the Citizen

Title: **Risk Assessment Methodology for Critical Infrastructure Protection**

Authors: Georgios Giannopoulos, Bogdan Dorneanu, Olaf Jonkeren

Luxembourg: Publications Office of the European Union

2012 – 63 pp. – 21.0 x 29.7 cm

EUR - Scientific and Technical Research series - ISSN 181-9424 (online), ISSN 1018-5593 (print)

ISBN 978-92-79-28181-5

doi:10.2788/78850

Abstract

The European Programme for Critical Infrastructure Protection is the main vehicle for the protection of critical infrastructures in Europe. The Directive 2008/114/EC is the legislative instrument of this programme. Risk assessment is an important element that is mentioned throughout the Directive text. However, there is no harmonized methodology in Europe for the assessment of interconnected infrastructures. The present work describes such a methodology and its implementation for the assessment of critical infrastructures of European dimension. The methodology takes into account an impact at asset level, evaluates the propagation of a failure at network level due to interdependencies and assess the economic impact of critical infrastructure disruption at national level.

LB-NA-25745-EN-N

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new standards, methods and tools, and sharing and transferring its know-how to the Member States and international community.

Key policy areas include: environment and climate change; energy and transport; agriculture and food security; health and consumer protection; information society and digital agenda; safety and security including nuclear; all supported through a cross-cutting and multi-disciplinary approach.

Publications Office

ISBN 978-92-79-28181-5