

Université  
de Toulouse

# THÈSE

En vue de l'obtention du

## DOCTORAT DE L'UNIVERSITÉ DE TOULOUSE

Délivré par :

Institut National Polytechnique de Toulouse (INP Toulouse)

---

**Présentée et soutenue par :**

**Daouda KAMISSOKO**

le lundi 25 novembre 2013

**Titre :**

Aide à la décision pour l'analyse de la vulnérabilité des réseaux d'infrastructure  
face aux crises de catastrophes naturelles

---

**École doctorale et discipline ou spécialité :**

EDSYS : Génie Industriel 4200046

**Unité de recherche :**

Institut de Recherche en Informatique de Toulouse (IRIT) - Laboratoire Génie de Production (LGP)

**Directeur(s) de Thèse :**

François PÉRÈS, Professeur des Universités, ENIT - LGP

Pascale ZARATÉ, Professeur des Universités, IRIT - UT1C

**Jury :**

Shaofeng LIU - Professeur, Université de Plymouth, Royaume-Uni - Rapporteur

Adolfo Crespo MARQUEZ - Professeur, Université de Séville, Espagne - Rapporteur

Scira MENONI - Professeure associée, Polytechnique de Milan, Italie - Examinatrice

Myriam MERAD - Chercheur, HDR, INERIS, France - Examinatrice

Zineb SIMEU-ABAZI - Maître de Conférences, HDR, INP Grenoble, France - Examinatrice

Pascal HAURINE - Responsable du bureau des Risques Naturels et Technologiques, DDT des Hautes-Pyrénées, France - Invité



**Decision support for infrastructure  
network vulnerability assessment in  
natural disaster crisis situations**

**Aide à la décision pour l'analyse de la  
vulnérabilité des réseaux  
d'infrastructure face à une crise de  
catastrophe naturelle**

To those who  
Fight the evil;  
Defend the good;  
Work for freedom;  
Cultivate peace;  
Seek the truth;  
Dream of justice;  
Believe in equality;  
Learn continuously;  
Endure patiently;  
Hope tirelessly;

To my family and friends

To all citizens of the world

In memory of my father and my brother Djiba

À ceux qui  
Combattent le mal  
Défendent le bien  
Travaillent pour la liberté  
Cultivent la paix  
Ont foi en la vérité  
Rêvent de justice  
Croient en l'égalité  
Apprennent sans cesse  
Endurent patiemment  
Espèrent sans relâche

À ma famille et ami(e)s

À tous les citoyens du monde

À la mémoire de mon père et de mon frère Djiba

## ACKNOWLEDGMENT

By writing these lines, I'm thinking of a substantial number of people who have always stood me during this thesis.

I begin quite naturally by my two supervisors: Professor Pascale ZARATÉ and Professor François PÉRÈS. Without their careful supervision and the relevance of their comments, this thesis certainly could not be achieved. Beyond their scientific and pedagogical qualities, they knew bear me tirelessly, understand me in difficult moments and share the joys inherent in the research work.

I thank the two reviewers of this thesis: Professor Shaofeng LIU and Professor Adolfo Crespo MÁRQUEZ. I was very honoured by the welcome that Professor LIU has given me during my stay in England. Our exchanges always rewarding have been a source of inspiration and have strengthened my rigor spirit.

I also thank the other members of the committee: Madame Scira MENONI, Madame Myriam MERAD, Madame Zineb SIMEU-ABAZI, and Mister Pascale HAURINE. The exchanges with Madame MERAD during this work allowed me to have the necessary detachment to pursue the thesis with serenity. The help of Mr HAURINE and his team has been crucial to validate our models. With their help, we were able to get some data on the city of Lourdes where we deployed the case study.

My thanks go also to the colleagues of the three laboratories where I had the pleasure of staying: The Laboratory Production Engineering in Tarbes, the Toulouse Research Institute in Computer Science and the Plymouth Management School in England. That everyone finds in these lines my deep appreciation and gratitude.

I thank all of my teachers during those long years: Mr SEKOU, Mr SORY, Mr BEN ABDELLAH, Mr BELMIR, Mr FOFANA, Mr SAFOUANE, Mr HAMACI, Mr COUDERT etc. to name a few. You have all at one time influenced my insight. That God recognize you.

A great thought also to my friends: those of Aviation, Martin Luther King Club, Morocco, EPMI, army, social networks. I thank you for your unfailing support, fun and relaxation moments.

I don't know how to thank my family. My dear mother who one day, took me to school to learn how to "sing". My sister Hadja who taught me my first letters of the alphabet. My sister Domanin. My brother N'khôro, Moussa, Kê, Sory, Laye, Kèlèti. My aunts, uncles, and cousins, I am so proud to have you in my life. Thanks for this complicity. I often doubted, but you-ever. Thanks for everything.

Whom those I was able to forget would not blame me for that. They will find in these lines my gratitude and my apologies. I bet that if I should rewrite this acknowledgment, more than one name will appear.

I also thank the woman who shares my life. One day love, love for ever. She is the most beautiful among the intelligent women and the most intelligent among the beautiful women.

Finally I thank the Lord who continually gave me his grace and his charities.

# REMERCIEMENTS

En écrivant ces lignes, je pense à un nombre considérable de personnes qui n'ont cessé de me soutenir durant cette thèse.

Je commence tout naturellement par mes deux directeurs de thèse : Professeur Pascale ZARATÉ et Professeur François PÉRÈS. Sans leurs encadrements minutieux et la pertinence de leurs remarques, cette thèse n'aurait certainement pas pu aboutir. Au-delà des leurs qualités scientifiques et pédagogiques, ils ont su me supporter sans relâche, me comprendre dans les moments difficiles et partager les joies inhérentes au travail de recherche.

Je remercie les deux rapporteurs de ce manuscrit : Professeur Shaofeng LIU et Professeur Adolfo Crespo MARQUEZ. J'ai été très honoré de l'accueil qui m'a été réservé par Professeur LIU lors de mon séjour en Angleterre. Nos échanges - toujours enrichissants, ont été une source d'inspiration et ont renforcé mon esprit de rigueur.

Je remercie aussi les autres membres du jury. Madame Scira MENONI, Madame Myriam MERAD, Madame Zineb SIMEU-ABAZI, et Monsieur Pascale HAURINE. Mes échanges avec Madame MERAD, durant ces années de thèse m'ont permis d'avoir le recul nécessaire et de poursuivre la thèse avec sérénité. L'aide de Mr HAURINE et de son équipe a été déterminante pour valider nos modèles. Grace à leurs concours, nous avons pu obtenir certaines données sur la ville de Lourdes où nous avons déployé le cas d'étude.

Mes remerciements vont également aux collègues des trois Laboratoires où j'ai eu l'immense plaisir de séjourner : Le Laboratoire Génie de Production à Tarbes, L'Institut de Recherche en Informatique de Toulouse et le « Plymouth Management School » en Angleterre. Que chacun trouve dans ces lignes toute ma reconnaissance et ma gratitude.

Je remercie l'ensemble des mes enseignants durant ces longues années : Mr SEKOU, Mr SORY, Mr BEN ABDELLAH, Mr BELMIR, Mr FOFANA, Mr SAFOUANE, Mr HAMACI, Mr COUDERT, etc. pour ne citer que ceux-ci. Vous avez tous à un moment donné influencé mon regard sur la science. Que Dieu vous le reconnaisse.

Une grande pensée aussi pour mes ami(e)s : Ceux de l'aviation, du club Martin Luther King, du Maroc, de l'EPMI, de l'armée, des réseaux sociaux. Je vous dis merci pour votre soutien infaillible, les moments de rigolade et de détente.

Je ne sais comment remercier ma famille. Ma chère maman qui un jour m'amena à l'école pour apprendre à « chanter ». Ma sœur Hadja qui m'a appris les premières lettres de l'alphabet. Ma sœur Domanin. Mes frères N'khôrô, Moussa, Kê, Sory, Laye, Kèlèti. Mes tantes, oncles, cousins et cousines, Je suis si fier de vous avoir dans ma vie. Merci pour cette complicité. J'ai souvent douté, mais vous-Jamais. Merci pour tout.



Que ceux dont j'ai pu oublier ne m'en tiennent pas rigueur. Qu'ils trouvent dans ces lignes toute ma reconnaissance et mes excuses. Je parie que si je devrais réécrire ces remerciements plus tard, plus d'un nom y figureront.

Je remercie aussi la femme qui partage ma vie depuis. Amour d'un jour, amour de toujours. La plus belle parmi les intelligentes, la plus intelligente parmi les belles.

Enfin je remercie le seigneur qui m'a continuellement accordé sa grâce et sa bienfaisance.

# ABSTRACT

This thesis deals with infrastructure network vulnerability analysis in the natural disaster context. It starts from the observation that infrastructure such as water supply or power grid has significant influence on natural disasters' indirect consequences. The aim is to model the vulnerability to take efficient decisions.

The scientific approach is divided into two complementary parts. The first one deals with the vulnerability assessment, while the second one focuses on the decision aiding process to be implemented for the assessed vulnerability management.

The proper vulnerability analysis is based on the analysis objects modelling. In order to achieve this, we will adopt graph theory representation. A literature review will allow us to identify the graph model which best suits the context of the thesis. In a multi network analysis environment, interdependences, i.e. relationships between components of the same or different networks - are a determining factor for any vulnerability model. We have thus proposed an approach to model interdependence compatible with the graph theory. There are two types of relationships: the one first is functional (dependence), while the second one is dysfunctional (influence). The vulnerability is assessed by a simulation-based approach. It is composed of one part relating to the system ability to resist the feared event; and another part relative to its ability to be back on its nominal state after the feared event.

When the vulnerability is determined, the next step will be to take the necessary decisions to manage it. This part on the decision aiding is itself divided into two sub parts: first of all the process to be used for the crisis management is established. Then a methodology for decision aiding is proposed and a Decision Support System prototyped.

**Key words:** Vulnerability, Risk, Robustness, Resilience, Network, Graph, Decision, ELECTRE, Java, UML, Interdependence, DB, System, Complexity

## RÉSUMÉ EN FRANÇAIS

Cette thèse traite de la vulnérabilité des réseaux d'infrastructure face aux catastrophes naturelles. Elle part du constat que les infrastructures telles que les réseaux d'eau, d'électricité influencent considérablement les conséquences indirectes des catastrophes naturelles. Elle vise donc à modéliser la vulnérabilité dans de telles situations pour une prise de décision efficace.

La démarche scientifique est divisée en deux parties complémentaires. La première traite de la vulnérabilité des dits réseaux, tandis que la seconde se concentre sur le processus d'aide à la décision à mettre en œuvre en vue de gérer la vulnérabilité.

L'analyse proprement dite de la vulnérabilité repose sur la modélisation des objets de l'analyse. Pour ce faire nous adopterons une représentation par la théorie des graphes. L'état de l'art à ce niveau nous a permis d'identifier les modèles de graphe les mieux adaptées au contexte de cette thèse. Dans un environnement d'analyse multi réseau, les interdépendances, c'est-à-dire les relations entre les composants du même réseau ou entre ceux de réseaux différents-sont un facteur déterminant pour tout modèle de vulnérabilité. Nous avons ainsi proposé un modèle compatible avec la théorie des graphes. Sont distingués deux types d'interdépendances. La première est fonctionnelle (dépendance), et la seconde est dysfonctionnelle (influence). La vulnérabilité quant à elle, est déterminée par une approche basée sur la simulation. Elle est composée d'une première partie relative à l'aptitude du système à résister à l'évènement redouté ; et d'une seconde partie relative à son aptitude à recouvrer des conditions opérationnelles spécifiées après l'occurrence de l'évènement redouté.

Le calcul de la vulnérabilité est un point d'entrée pour assister la prise de décision. La deuxième partie aborde ce thème. Elle est elle-même divisée en deux sous parties : La première aborde le processus à mettre en œuvre pour la gestion de la crise ; la deuxième le Système Interactif d'Aide à la Décision réalisé. Celui-ci implémente le processus d'aide à la décision.

**Mots clés :** Vulnérabilité, Risque, Robustesse, Résilience, Réseau, Infrastructure, Graphe, Décision, Interdépendance, ELECTRE, Java, UML, BDD, Système, Complexité.

# CONTENTS

Acknowledgment.....	vi
Remerciements.....	vii
Abstract.....	ix
Résumé en français.....	x
Contents.....	xi
Table of figures.....	xviii
List of tables.....	xxi
Style definition.....	xxii
General Introduction.....	1
✓ Motivation.....	1
✓ Objectives and delimitations.....	2
✓ Research process.....	3
Introduction générale.....	5
✓ Motivations.....	5
✓ Objectifs et délimitations.....	6
✓ Processus de recherche.....	7
Chapter I Literature review.....	9
Introduction.....	11
I.1: Infrastructure network management literature review.....	11
I.1.1 Graph theory.....	14
✓ Scale-free Network.....	14
✓ Random graph.....	15
✓ Small word network.....	15
I.1.2 Vulnerability metrics.....	15
✓ Betweenness centrality.....	18
✓ Average Path Length.....	19

✓ Clustering coefficient.....	20
✓ Connectivity .....	20
✓ Integrity .....	20
✓ Probability .....	21
✓ Vulnerability function.....	21
I.2: Decision aiding Literature Review .....	21
I.1.3 Decision aiding process .....	23
✓ Linear decision aiding process .....	24
✓ Cyclical decision aiding process .....	25
✓ Hybrid process .....	26
I.1.4 Decision aiding methods.....	27
I.1.4.1 Classical method or single synthesis criterion .....	29
✓ Weighted sum.....	31
✓ Laplace criterion .....	31
✓ Bernoulli criterion.....	31
✓ The expected value criterion .....	31
✓ Criterion of expected utility .....	32
I.1.4.2 Multicriteria decision aiding .....	32
✓ Choice.....	38
✓ Sorting.....	40
✓ Ranking.....	41
Conclusion.....	44
Chapter II Modelling.....	45
Introduction.....	47
I.3: Vulnerable system representation .....	47
II.1.1 Complex system.....	47
II.1.2 Critical system .....	48
II.1.2.1 Criticality concept applied to infrastructure .....	49
II.1.2.2 components of a Critical infrastructure system.....	51

✓ Territory.....	51
✓ Stakes .....	52
✓ Flow.....	52
✓ External environment .....	53
✓ Feared event.....	53
I.4: Network Modelling .....	56
II.1.3 Network Definition .....	56
II.1.4 Network Representation Features.....	58
II.1.4.1 Modelling rules .....	58
✓ Edges are direction .....	58
✓ Edge weight.....	59
✓ The node type.....	60
II.1.4.2 relationship typology .....	61
✓ Lack of interdependence modelling .....	63
✓ Relationship classification.....	63
II.1.5 Network Modelling Techniques .....	65
II.1.5.1 Relationship representation.....	65
✓ Dependence modeling .....	65
✓ Influence modeling .....	65
II.1.5.2 Network component connexions.....	66
✓ Relationship Node -Node.....	66
✓ Relationship Node-Edge .....	66
✓ Relationship Edge -Node .....	67
✓ Relationship Edge-Edge .....	67
II.1.5.3 Dynamic factors .....	68
✓ Circulation laws .....	68
✓ Mitigation and aggravation factors .....	68
I.5: Vulnerability Modelling.....	69
II.1.6 Difference between vulnerability and risk .....	70

II.1.7 Vulnerability analysis framework.....	72
II.1.8 Vulnerability assessment.....	73
✓ Robustness.....	74
✓ Resilience.....	76
✓ Vulnerability.....	79
Conclusion.....	82
Chapter III Decision aiding.....	83
Introduction.....	85
I.6: Decision making difficulties.....	85
I.7: Decision process.....	87
III.1.1 Decision context characterisation.....	90
III.1.1.1 Crisis level.....	90
III.1.1.2 Risk situation.....	92
III.1.1.3 Decision levels.....	93
III.1.1.4 Decision makers identification.....	94
III.1.1.5 Decisions.....	95
III.1.1.6 Decision problems.....	96
✓ Problem $\omega$ acceptance and change management.....	97
✓ Problem $\kappa$ of planning.....	97
III.1.2 System modelling.....	98
III.1.3 Structuration.....	98
III.1.3.1 Potential decision.....	98
III.1.3.2 Preferences systems.....	99
III.1.3.3 Consequences.....	100
III.1.3.4 Evaluation mode.....	100
III.1.4 Muticriteria aggregation.....	101
III.1.5 Integration.....	103
I.8: The Decision Support System (DSS).....	103
III.1.6 Definition and Features.....	104

III.1.7 The risk of the project .....	108
III.1.8 Software engineering process.....	109
✓ Waterfall model.....	110
✓ Prototyping model .....	111
✓ Spiral Model.....	111
✓ Adopted process .....	112
III.1.9 Context modelling .....	113
III.1.9.1 Identification of actors .....	114
III.1.9.2 The static context diagram.....	115
III.1.9.3 The relationship between use cases .....	115
III.1.9.4 Use cases by human actor.....	116
III.1.9.5 Sequence diagram of use case .....	117
III.1.9.6 Activity diagram by use case diagram.....	118
III.1.10 Architecture.....	120
III.1.10.1 The Human Computer Interface.....	121
✓ Connexion.....	122
✓ Import.....	122
✓ Drawing.....	122
✓ Parameter filling in.....	123
✓ Simulation .....	124
✓ Calculation .....	124
✓ Decision .....	124
✓ Final Recommendation .....	124
✓ Data base.....	124
III.1.10.2 The database .....	124
✓ The entity relationship model.....	125
✓ The object model.....	125
III.1.10.3 Model Base.....	126
III.1.11 Coding.....	127



III.1.12 DSS functionalities .....	127
III.1.12.1 Parameter calculation .....	128
III.1.12.2 Evolution of the parameter .....	129
III.1.12.3 Feared event or scenario.....	130
III.1.12.4 The feared event occurrence point .....	130
III.1.12.5 Time to break down .....	131
III.1.12.6 Minimum value of one parameter .....	132
III.1.12.7 Effect of interdependence.....	132
III.1.12.8 Request on database.....	133
Conclusion.....	134
Chapter IV Cases Study.....	135
Introduction.....	137
I.9: Generated Case Study.....	137
IV.1.1 Context.....	138
✓ Environment .....	138
✓ Territory.....	138
✓ Flow.....	139
✓ Feared events.....	139
✓ Mitigation or aggravations factors .....	140
IV.1.2 System final state .....	140
IV.1.3 Results .....	141
I.10: Lourdes Case Study .....	143
IV.1.4 Data collection .....	143
✓ Decision makers' identification .....	143
✓ The feared event.....	144
✓ Mitigation and aggravation factors .....	146
✓ Territory.....	146
✓ Infrastructure .....	146
✓ Flow.....	147

✓ Stake .....	148
✓ External Environment.....	148
IV.1.5 results .....	148
Conclusion .....	152
General conclusion .....	154
✓ Contribution .....	154
✓ Perspectives .....	155
Conclusion générale .....	157
✓ Contribution .....	157
✓ Perspectives .....	158
References .....	160
Personal publication .....	170
Glossary .....	171
Annexes.....	172

## TABLE OF FIGURES

Figure I-1: Linear decision process by [57] .....	25
Figure I-2: Cyclic decision aiding [58] .....	26
Figure I-3: Hybrid process by [49] .....	26
Figure I-4: Decision aiding methods .....	28
Figure I-5: Type of risk analysis by [54] .....	35
Figure I-6: Multicriteria decision aiding methods for risk analysis type by [54] .....	36
Figure I-7: Preference relations .....	37
Figure II-1: Global System overview .....	49
Figure II-2: Undirected network .....	58
Figure II-3: Directed network .....	59
Figure II-4: Weighted graph .....	59
Figure II-5: Network of same type of node .....	60
Figure II-6: Network with different types of node .....	60
Figure II-7: Example of cascading diagram by [87] .....	63
Figure II-8: Dependence relationship .....	65
Figure II-9: Dependence relation .....	65
Figure II-10: Dependence Node-Node .....	66
Figure II-11: Virtual components .....	66
Figure II-12: Relationship Node-Edge .....	67
Figure II-13: Influence Node-Edge .....	67
Figure II-14: Relationship Edge-Edge .....	67
Figure II-15 Elements of vulnerability .....	70
Figure II-16: Elementary system to analyse .....	70
Figure II-17: Risk and vulnerability analysis .....	71
Figure II-18: Vulnerability view .....	72
Figure II-19: Analysis framework .....	73
Figure II-20: Robustness evolution .....	76
Figure II-21: Resilience for t1 equal constant .....	78
Figure II-22: Resilience for t2 equal constant .....	78
Figure II-23: Vulnerability Classes .....	79
Figure II-24: Robustness and resilience .....	80
Figure II-25: vulnerability graph .....	81

Figure III-1 : Decision context .....	87
Figure III-2 : Decision-making process: source [120].....	88
Figure III-3: Decision phases .....	89
Figure III-4: Decision aiding process elements .....	90
Figure III-5: Crisis level.....	91
Figure III-6: Crisis situation inspired from [54] .....	92
Figure III-7: Decision level.....	93
Figure III-8: ELECTRE methods by [62].....	102
Figure III-9: Client-Server functioning.....	106
Figure III-10: Application Service Provider functioning.....	106
Figure III-11: Processes .....	109
Figure III-12 : Water-fall model by [138].....	110
Figure III-13: Spiral model by ref [138].....	111
Figure III-14: The process of developing a DSS for vulnerability management.....	112
Figure III-15 : Step .....	113
Figure III-16: Static Context Diagram .....	115
Figure III-17: Relation between use cases.....	116
Figure III-18: Use case for local operator .....	117
Figure III-19: Sequence diagram for vulnerability analysis .....	118
Figure III-20: Activity diagram for vulnerability analysis .....	119
Figure III-21: Decision Support System structure by [121].....	120
Figure III-22: Human Computer Interface with Balsamiq .....	121
Figure III-23: Log in Panel .....	122
Figure III-24: Network drawing.....	123
Figure III-25: Node Parameter .....	123
Figure III-26: Class diagram with StarUML .....	126
Figure III-27: Functionalities of VESTA .....	128
Figure III-28: Parameter calculation .....	129
Figure III-29: Evolution of a parameter .....	129
Figure III-30: Feared event or scenario .....	130
Figure III-31: Feared event occurrence point.....	131
Figure III-32: Time to break down.....	131
Figure III-33:Effect of interdependance .....	132
Figure IV-1: Case study.....	137
Figure IV-2: Network after feared event occurrence.....	141
Figure IV-3: Midi-Pyrenées Seismic zoning .....	145
Figure IV-4 : Lourdes networks.....	147

Figure IV-5: Lourdes network modelling .....148  
Figure IV-6: Results of the Lourdes case study.....150  
Figure IV-7: Vulnerability of Lourdes network components .....151

## LIST OF TABLES

Table I-1 : Infrastructure vulnerability review by [1] .....	13
Table I-2: Vulnerability definitions .....	17
Some definitions of the decision are proposed in Table I-3. ....	22
Table I-4: Decision definition .....	22
Table I-5: Elementary methods by [63] .....	30
Table I-6: Outranking methods by [63] .....	34
Table II-1: Network classification .....	56
Table II-2: Critical networks according to European Union, 2004 .....	57
Table II-3 : Relationship between networks .....	64
Table II-4: Robustness definitions .....	74
Table II-5: Resilience definitions .....	77
Table II-6: Vulnerability truth table .....	80
Table III-1: Phases by crisis level .....	92
Table III-2: Martel's decision maker identification .....	94
Table III-3: Decision maker categories .....	95
Table III-4: Decision maker per crisis level .....	95
Table III-5: Problem per phase .....	97
Table III-6: Relational preference systems.....	99
Table III-7: Decision making criteria .....	100
Table III-8: Aggregation methods .....	103
Table III-9: Decision Support System definitions .....	105
Table III-10: Decision Support System in the literature .....	128
Table III-11: Minimum value of one parameter .....	132
Table IV-1: Feared event parameters.....	139
Table IV-2: Aggravation factor parameters .....	140
Table IV-3: Results .....	142
Table IV-4: Earthquakes in Lourdes Region .....	145

## STYLE DEFINITION

The objective of this part is to facilitate the reading of the thesis by presenting the used style.

The body of the manuscript is written using Arial Narrow style with police 12. Below is presented some examples.

When citing the work of another author the IEEE citation style is used [0].

*Examples are in inserts*

*Table and figure caption are in Arial Narrow 11. The first number is the number of the chapter followed by an incremental number. For instance Table 1.3 is the third table of the chapter 1.*

Lists are presented as following:

- First element;
- Second element;
- Etc;

***Definition 0-4: Definitions provided in this thesis are in Arial Narrow 11, bold and italic. They are numbered. The first number is that of the chapter and the second is an incremental number.***

"The beginning is thought to be more than half of the whole"

Aristotle





## General Introduction

### ✓ *Motivation*

---

Natural disasters have stricken populations everywhere in the world in the past years. For example in 2004, the Indian Ocean tsunami caused 220,000 deaths. Next, the cyclone Nargis in Myanmar made 138,373 deaths in 2008. In the same year an earthquake in China killed 87,449 people. Two years later in 2010, 230,000 people were killed by an earthquake of 7.0 in Haiti. More recently, in March 2011, a tsunami in Japan made 18,079 deaths.

These few examples show the devastating character of natural disasters for human being. Caused deaths might be induced by disaster direct impact (trauma, asphyxia, drowning, burying, burning,) or by its indirect impact (thirsting, secondary infection of wounds, contamination, epidemic ...).

Major causes of deferred deaths problems are partly due to networks disturbance. Consequently, natural disasters are not the only cause of society's disruption. Infrastructure network failure is among the worst causes. For instance in July 2012, a blackout in India affected over 620 million people. Moreover our societies are depending more and more on these networks (power grid, water, gas, telecommunications systems, etc.). Regarding consequences to population, most feared scenarios are when a natural disaster affects infrastructure networks. Consequences are then amplified. Another aggravation factor is interdependence among networks. In addition, materials, services, energies and information exchanged may aggravate or mitigate consequences. Due to interdependences, failure of a part of a network is likely to spread to the others. This situation makes difficult any risk or vulnerability analysis. For instance, because of interdependence in air travel, the 2010 volcanic eruption in Iceland affected about 20 countries. Despite the advancement in the vulnerability and risk analysis, it is always difficult to make decisions in crisis situations. Disaster is source of stress and anxiety for decision makers which judgment could be affected in such a situation.

France and Europe are not safe from these elements and other furies of the nature. They are subject to all existent feared events on the planet. Witness is the heat wave which occurred in the summer 2003. This heat was responsible for 35,000 deaths in the European continent. In France, departmental files about major risks are established by the prefects and give an overview of natural disasters distribution on the national territory. Today, with widely varying severities, 23,500 communes are exposed to one or more natural disasters: cyclones, storms, floods, avalanches, landslides, earthquakes, volcanic eruptions, forest fires etc. Given this diversity of disasters, their amplitudes and frequencies, it is interesting to investigate the indirect consequences. In particular those induced by network failure.

For these reasons we have been motivated to pursue these years of research on the analysis of network vulnerability to natural disaster.

### ✓ *Objectives and delimitations*

---

Deaths caused by natural disasters can be induced by direct impact (trauma, asphyxia by drowning or burial, burning) or indirect impact (superinfecting of wounds, contamination, epidemics). This thesis focuses only on indirect impacts. It assumes that individuals still alive after the natural disaster occurrence could die for reasons related to the assistance inability to respond in a reasonable time on affected areas, or to implement effective health action. This situation is common after the occurrence of an earthquake. The Haiti earthquake is there unfortunately to remind us of that. A disaster by definition is an ordeal that disrupts society and leaves the individual alone face to the crisis for a longer or shorter time. In crisis time, people have to deal with multiple disabilities: stress, public service disruption, time to activate assistance, isolation situation etc.

We argue that major causes of deferred death are often due to network disruption. By network we mean interconnected entities facilitating the circulation of useful goods (food, medicines, clothing, blankets etc.), equipment (tools, excavation machines, health infrastructure etc.), services (water, electricity) or information (internet, telephone). This thesis deals with network vulnerability to natural disasters as an entry point to a problem that may increase indirect damage caused to the population. Damage could be aggravated by a lack of decision or by inappropriate decision making.

Taking into account each network separately helps providing interesting but not sufficient information to make the right decision in full knowledge of causes and consequences. The organizational dimensions and decision-making necessary to highlight preventive or corrective solutions in natural disasters context involve working in collaborative mode. These operation modes require adequate tools, adapted to the contexts and profiles of potential users. Decision support tools should be developed on the basis of multi-decision makers model (experts, decision-makers, users), multi-views (before, during, after the disaster) and multi-scales (global or local context).

The techniques of safety operation (reliability, maintainability, availability, security) and risk management (assessment, prevention, mitigation, risk mapping) used in industrial fields will allow the establishment of a vulnerability model. Information extracted from this model will be an input of the decision-making. In a temporal sequence, these techniques can be applied:

- To a Pre-event: Organization and implementation of operational emergency services, assessment of the impact of technological innovation on the consequences, estimation of the occurrence probability of a particular event;
- During the event: Assessment of the event risk repetition, level of damage estimation depending on the intensity and first testimonials, estimation of assistance means to be used;
- To a Post-event: Estimation of the insurance premiums by insurance professionals, evaluation of

assistance program for concerned populations, establishment of recovery plans.

This thesis encompasses all these phases. Its objectives are to overcome these problems by:

- Modelling interdependent critical infrastructure;
- Determining vulnerability of network, component, territory and stakes;
- Modelling and determining the impact of interdependence on the vulnerability;
- Correlating the intensity of a feared event and the damage to stakes;
- Identifying the worst scenarios;
- Determining a decision process for the crisis management;
- Building a Decision Support System for disaster management.

### ✓ *Research process*

---

To describe and try to find solutions to the described problems, the investigation relied on two scientifically complementary laboratories: the Laboratory Engineering Production (LGP) specialized in industrial engineering and the Toulouse Research Institute in Computer Science (IRIT) specialized in computer science. The thesis program was thus articulated in 2 separated parts on scientific terms but with a common goal:

- Part 1: Analysis of network vulnerability

This part was realized in the team Decisional and Cognitive Systems (SDC) of LGP. This laboratory is part of the Tarbes National School of Engineers (ENIT). We worked on infrastructure network vulnerability problems assessment against natural disaster.

*Scientific problem:* Representation of a sociotechnical system, correlation between intensity of the feared event and damage to the system element, vulnerability and interdependence modelling.

*Deliverable:* Socio-technical model for the vulnerability assessment.

After this part, we had a stay of four months at the University of Plymouth. The aim was to develop the collaboration with the School of Management and exchange our points of views about decision making in uncertain environment.

- Part 2: Decision Aiding in crisis situation

This part was realized in the Cooperative Multi-Agent Systems team at IRIT. We worked on the development of a decision aiding process and a Decision Support System in crisis situation.

*Scientific problems:* Identification of the passage from nominal situation to a crisis situation, negotiation and decision-making in an uncertain environment.

*Deliverable:* A decision process implemented in a Decision Support System based on the model developed in part 1.

The vulnerability model developed in part 1 should be substantiated according to the descriptive information of the current situation. The results of the simulation carried out through the vulnerability model will constitute inputs for the Decision Support System implemented in part 2.

## Introduction générale

### ✓ Motivations

---

Ces dernières années, les catastrophes naturelles ont touché divers populations et infrastructures un peu partout dans le monde. Par exemple, en 2004, le tsunami de l'océan indien provoqua 220 000 morts. Ensuite, ce fut le tour du cyclone Nargis en 2008 à Myanmar. On dénombra 138 373 morts. La même année un tremblement de terre en Chine sera à l'origine de 87 449 décès. Deux ans plus tard en 2010, 230 000 personnes seront tuées par un séisme de 7 en Haïti. Plus récemment, en mars 2011, un tsunami au Japon causera 18 079 décès.

Ces exemples montrent le caractère dévastateur des catastrophes naturelles pour l'être humain. Les morts sont causés soit par impact direct (traumatisme, asphyxie, noyade, brûlure, blessure) ou par impacts indirects (soif, surinfection des plaies, épidémie...). Nous soutenons que la cause principale des décès différés est liée en partie aux perturbations réseaux. Les défaillances des réseaux d'infrastructure font partie des pires causes de déstabilisation de la société. Par exemple en juillet 2012, une panne d'électricité en Inde a touché plus de 620 millions d'abonné.

En ce qui concerne les conséquences pour la population, le scénario le plus redouté est quand une catastrophe naturelle affecte des réseaux d'infrastructures. Les conséquences sont alors amplifiées. Un autre facteur d'aggravation est l'interdépendance susceptible d'exister entre les réseaux. En outre, les matériaux, services, énergies et informations échangés peuvent aggraver ou atténuer les conséquences. À cause des interdépendances, la défaillance d'une partie du réseau est susceptible de se propager aux autres. Cette situation rend difficile toute analyse de risque ou de vulnérabilité. Par exemple à cause de l'interdépendance dans le transport aérien, l'éruption volcanique de 2010 en Islande affecta une vingtaine de pays. Malgré l'avancé des techniques d'analyse de la vulnérabilité et du risque, il est toujours difficile de prendre des décisions dans une situation de crise. En effet, une catastrophe est source de stress et d'anxiété pour les décideurs, dont les jugements peuvent être affectés.

La France et l'Europe ne sont pas à l'abri de ces éléments et des autres colères de la nature. Ils sont soumis à tous les événements redoutés existantes sur la planète. Témoin en est la vague de chaleur qui a sévi en été 2003. Cette chaleur a fait 35 000 morts sur le continent européen. En France, l'ensemble des dossiers départementaux des risques majeurs établis par les préfets permet de dresser un panorama de la répartition des risques naturels sur le territoire national. Aujourd'hui, avec des gravités très variables, 23500 communes sont exposées à un ou plusieurs risques naturels : cyclones et tempêtes, inondations sous ses différentes formes (de plaine, torrentielle, par remontées des nappes ou submersion), avalanches, mouvements de

terrain (glissement, chute de blocs, cavités souterraines et marnières, retrait-gonflement des argiles), tremblements de terre, éruptions volcaniques, feux de forêt. Compte tenu de cette diversité des catastrophes, de leurs amplitudes et de leurs fréquences, il est intéressant d'étudier les conséquences indirectes. En particulier celles induites par une défaillance réseau.

Ce sont ces raisons, qui nous ont motivé à poursuivre ces années de recherche sur l'analyse de la vulnérabilité des réseaux d'infrastructure.

### ✓ *Objectifs et délimitations*

---

Cette thèse se concentre sur l'impact indirect des catastrophes naturelles sur les enjeux à travers les réseaux d'infrastructure. Les enjeux peuvent être la population ou une infrastructure vitale au fonctionnement de la société. Elle suppose que des personnes encore vivantes après l'occurrence ou le passage de la catastrophe naturelle meurent pour des raisons liées à l'incapacité des secours à intervenir dans des délais raisonnables - sur des zones touchées ou à mettre en œuvre des actions sanitaires efficaces. De telles situations sont fréquentes après un tremblement de terre. Celui d'Haïti est malheureusement là pour nous le rappeler. Une catastrophe est par définition une épreuve qui perturbe la société et laisse l'individu seul face à la crise pendant une période de temps plus ou moins longue. En temps de crise, les décideurs doivent faire face à des multiples situations : stress, perturbation des services publics, situation d'isolement, etc.

La majorité des conséquences différées sont en lien avec une perturbation des réseaux d'infrastructure. On entend par réseau un ensemble d'entités interconnectées facilitant la circulation de biens (nourriture, médicaments, vêtements, couvertures), matériels (outils, machines de déblaiement, infrastructures sanitaires), services (soins, électricité) ou informations (téléphone, internet). Cette thèse traite de la vulnérabilité des réseaux aux catastrophes naturelles comme point d'entrée d'une problématique qui peut accélérer ou augmenter par contrecoup les dommages causés à la population suite à une absence de décision ou une prise de décision inappropriée.

La prise en compte de chaque réseau séparément apporte des informations intéressantes mais non suffisantes pour prendre la bonne décision en toute connaissance de causes et de conséquences. Les dimensions organisationnelle et décisionnelle nécessaires à la mise en évidence de solutions préventives ou correctives pour affronter les catastrophes naturelles impliquent de travailler selon des modes collaboratifs. Ces modes de fonctionnement requièrent des outils adéquats, adaptés aux contextes et aux profils des utilisateurs potentiels. Ces outils d'aide à la décision doivent être développés sur la base de modèles multi-acteurs (experts, décideurs, usagers), multi-vues (avant, pendant, après la catastrophe) et multi-échelles (contexte local ou global).

Les techniques de sûreté de fonctionnement (Fiabilité, Maintenabilité, Disponibilité, Sécurité) et de gestion des risques (évaluation, prévention, atténuation, risk mapping) utilisées dans les domaines industriel et financier permettront d'établir un modèle de vulnérabilité. Les informations extraites de cette modélisation constituent des données d'entrée pour la prise de décision. Elles peuvent être utilisées dans le cadre de la

gestion des événements catastrophiques et prendre en compte les opinions de plusieurs acteurs (décideurs publics, experts, opérationnels) lors des prises de décision :

- Pré-événements : Organisation et implantation des services opérationnels de secours, évaluation de l'impact d'une innovation technologique sur les conséquences éventuelles, estimation de la probabilité d'occurrence d'un événement particulier ;
- Pendant l'événement : Évaluation des risques de répétition du phénomène, estimation du niveau des dommages en fonction de l'intensité et des premiers témoignages, estimation des moyens de secours à mettre en œuvre ;
- Post-événement : Estimation des primes d'assurances par les professionnels d'assurance, évaluations des programmes de soutien des populations concernées, établissement des plans de redressement.

Cette thèse comprend toutes ces phases. Ses objectifs sont de surmonter ces problèmes par :

- La modélisation des infrastructures critiques interdépendantes ;
- La détermination de la vulnérabilité d'un réseau, d'un composant, d'un territoire et d'un enjeu ;
- La modélisation et l'évaluation des répercussions de l'interdépendance sur la vulnérabilité ;
- La corrélation entre l'intensité d'un événement redouté et les dommages aux enjeux ;
- L'identification des pires scénarios ;
- La détermination d'un processus de décision pour la gestion de crise ;
- La caractérisation d'un système d'aide à la décision pour la gestion des catastrophes.

#### ✓ *Processus de recherche*

---

Pour décrire et tenter d'apporter des solutions à la problématique décrite, notre recherche s'appuiera sur deux laboratoires du PRES (Pôle de Recherche et d'Enseignement Supérieur) de Toulouse scientifiquement complémentaires : Le Laboratoire Génie de Production (LGP), spécialisé en génie industriel et l'Institut de Recherche en Informatique de Toulouse (IRIT) - spécialisé en informatique. Le plan de la thèse est alors reparti en deux volets différents sur le plan scientifique, mais avec un objectif commun :

- Volet 1 : Analyse de vulnérabilité des réseaux

Cette partie a été réalisée dans l'équipe Systèmes Décisionnels et Cognitifs (SDC) du Laboratoire Génie de Production. Ce laboratoire fait partie de l'École Nationale d'Ingénieurs de Tarbes. Nous avons travaillé sur les problématiques d'évaluation de la vulnérabilité des réseaux d'infrastructures dans un contexte des catastrophes naturelles.



*Verrous Scientifiques* : Représentation d'un système sociotechnique, corrélation entre l'intensité de l'événement redouté et les dommages causés au système, Modélisation de la vulnérabilité et des interdépendances.

*Livrable* : Modèle socio-technique pour l'évaluation de la vulnérabilité.

Après cette partie, nous avons fait un séjour de quatre mois à l'Université de Plymouth au Royaume-Uni. L'objectif était de consolider la collaboration avec la « School of Management » et d'échanger nos points de vue sur la prise de décision en environnement incertain.

- Volet 2 : Aide à la décision en situation de crise

Cette partie a été réalisée dans l'équipe Systèmes Multi-Agents Coopératifs (SMAC) à l'Institut de Recherche en Informatique de Toulouse. Nous avons travaillé sur l'élaboration d'un processus d'aide à la décision et d'un système d'aide à la décision en situation de crise.

*Verrous scientifiques* : Identification du passage d'une situation nominale à une situation de crise, négociation et prise de décisions dans un environnement incertain.

*Livrable* : Un processus de décision mis en œuvre dans un système de d'aide à la décision basée sur le modèle développé dans le volet 1.

Le modèle de vulnérabilité développé dans la partie 1 doit être justifié selon les informations descriptives de la situation actuelle. Les résultats de la simulation réalisée par le biais du modèle de vulnérabilité constitueront des entrées pour le système d'aide à la décision mis en œuvre dans le volet 2.

# CHAPTER I

# LITERATURE

# REVIEW

## **Résumé en Français**

Ce chapitre traite de l'état de l'art dans de domaine de l'analyse de la vulnérabilité des réseaux d'infrastructure. Elle est divisée en deux parties : La première partie se focalise sur le concept de vulnérabilité et des modèles structurels associés. Une modélisation par la théorie des graphes étant préconisée, les différentes catégories de graphes sont présentées. Par la suite nous identifions les métriques de la vulnérabilité : Centralité, Intégrité, Connectivité, ainsi que d'autres fonctions.

La deuxième partie aborde les processus d'aide à la décision. Nous groupons l'ensemble des processus existants en trois catégories : Les processus linéaires, les processus cycliques et les processus hybrides. Les méthodes d'agrégation multicritère sont également catégorisées. Pour chaque méthode présentée, l'applicabilité à l'analyse de la vulnérabilité des réseaux est investie. Un accent est mis sur les méthodes de type ELECTRE. Pour cette dernière catégorie, le groupement est effectué en fonction des problématiques de base.

“There is nothing so strange and so unbelievable that it has not been said by one philosopher or another”

Descartes

## INTRODUCTION

In the science of vulnerability analysis as in many others, words such as risk, system are polysemic and interpreted in different ways. The objective of this state of the art is to present studies related to the field of the vulnerability analysis. It is divided into two parts: the first is about the concept of vulnerability and associated structural models. Since the modelling is based on the graph theory, different categories of graphs will be presented. Following on, the existing vulnerability metrics: centrality, integrity, connectivity, as well as other vulnerability functions will be introduced. The second part deals with the decision aiding process. We classified existing processes into three categories: linear processes, cyclic processes and hybrid processes. Multicriteria aggregation methods are also categorized. For each presented method, the applicability to the network vulnerability analysis is investigated. A focus is done on the ELECTRE methods. For this latter category, the grouping categories are performed based on basic problems. The results of this part allowed us to propose a vulnerability model overcoming literature shortcomings. We begin by the infrastructure network management literature review presented in the next section.

### I.1: INFRASTRUCTURE NETWORK MANAGEMENT LITERATURE REVIEW

<i>Feared event and type of approach</i>	<i>Vulnerable elements (vulnerability type)</i>							
	Population		Institutional	Building	Network		Economic activity	Urban System
Seismicity	Social	Corporal		Structural	Structural	Functional		
Damage observation	Colbeau-Justin & de Vanssay, 1996 - Leone & Mavoungo, 2000	Mahue-Giangreco et al., 2001	Colbeau-Justin & de Vanssay, 1996	ATC-20 - AFPS	Hassani & Takada, 1995	Chang, 1996	Mazzocchi & Montini, 2002	Menoni, 2001
Vulnerability diagnostic	Mavoungo, 2006	?	?	HAZUS - ATC-88 - Gémitis	Durville & Meneroud, 1987	?	Gémitis-Nice	Gémitis-Nice (Lutoff, 2000)
Scenario	?	HAZUS -	?	HAZUS -	HAZUS -	HAZUS	HAZUS	Gémitis-Nice

		Coburn et al., 1992		ATC-85 - Gémitis	ATC-91			
Volcano								
Damage observation	de Vanssay & ColbeauJustin, 2000	Baxter et al., 1997	Leone & Gaillard, 1999 - Voight, 1990	Spence et al., 1996	?	D'Ercole & Metzger, 2000	Gaillard, 2001	D'Ercole & Metzger, 2000
Vulnerability diagnostic	D'Ercole, 1991- Dibben & Chester, 1999	?	Lesales, 2005	Pomonis et al., 1999	?	?	?	D'Ercole & Metzger, 2004
Scenario	?	Baxter et al., 1998	?	Leone, 2004 - Pomonis et al., 1999	Stieltjes & Mirgon, 1998	?	?	Gomez-Fernandez, 2000
Land slide								
Damage observation	Leone, 1996	?	?	Alexander, 1988 - Leone, 1996	Leone, 1996	Leone, 1996	Leone, 1996	?
Vulnerability diagnostic	Cospar	?	Cospar	?	?	?	?	Finlay, 1996
Scenario	?	Finlay, 1996 - Leone, 1996	?	Hulbergern & Carree, 1987 - Leone, 1996	Leone, 1996- Panizza et al, 2002	Leone, 1996	Mora, 1992	Mora, 1992
Wind								
Damage observation	Sarant et al. , 2003	?	Sarant et al., 2003	Hamparian , 1999	?	?	?	?
Vulnerability diagnostic	Pagney & Suédois, 1999	?	Sarant et al., 2003	Bonfanti, 2004- HAZUS	?	?	?	?
Scenario	?	?	?	Khanduri &	?	?	Khanduri &	?

				Morrow, 2003 - HAZUS			Morrow, 2003 - HAZUS	
Flood								
Damage observation	?	Jonkman et al., 2002	?	Kelman & Spence (2004)	?	?	Torterotot, 1993	NRC, 1999
Vulnerability diagnostic	DEFRA/FHR C, 2003	DEFRA/FHR C, 2003 Green, 1988	Lagadec, 1995	?	?	?	Ledoux & Sageris, 1999 Barbut et al., 2004	Hardy, 2003 Reghezza, 200
Scenario	?	Ruin & Lutoff, 2004	Gilbert & Bourdeaux, 1999 Lagadec, 1995	HAZUS	?	?	HAZUS	Liu Renyi & Liu Nan (2002) Islam (1997) Légende : 1- Disponibilité opérationnelle (approche standardisée et reproductible

Table I-1 : Infrastructure vulnerability review by [1]

Infrastructure network management has been studied for many areas. [2] studied the vulnerability of roads. The financial aspect related to infrastructure network failure was investigated in [3]. [1] made a comprehensive literature review in this topic summarized in Table I-1. Blue cells stand for standardized and reproducible approaches, yellow cells for non-standardized but reproducible approaches and green cells for approaches under research. It shows that with regards to networks study, there is a lack of study concerning many feared events. Infrastructure network failure is an issue which has not been much investigated. There is a lack of research at the structural or functional level. The structural level is related to the infrastructure architecture, and the function one to how it accomplishes its functions through flow circulation.

The review performed in this thesis and presented in next section is divided into two parts. The first one focusses on the network modelling through the graph theory. The second introduces some vulnerability metrics.

### I.1.1 GRAPH THEORY

The first step of network vulnerability analysis is modelling. In the modelling step, graph theory is mostly used. The foundations of the graph theory were built by Leonhard Euler (1707-83) when he presented the solution Königsberg bridges [4]. Since then, the theory has evolved considerably. Nowadays, it is applied to many disciplines like organic chemistry modelling [5], mechanical system reliability analysis [6], representation of engineering systems [7] etc.

A finite graph  $G = (V, E)$  is defined by a finite set of nodes  $= \{V_1, V_2 \dots V_N\}$ ; ( $|V| = N$ ) and a finite set of edge  $E = \{E_1, E_2 \dots E_M\}$ ; ( $|E|=M$ ).

In the field of infrastructure network modelling, graph theory is mainly used in the literature. When infrastructure networks are related to graph, many classifications are then possible. One of them separate infrastructure networks into social network (Facebook, LinkedIn), information network (World Wide Web, or knowledge network), biological network (food networks) and technological network (power grids).

Another classification is based on the network structure. From this point of view, networks can be classified according to their degree distribution [8]. This classification gives rise to three categories of network [9] : scale-free network, random graphs, and small world network. These categories are presented in the next three sections.

#### ✓ *Scale-free Network*

---

For many real networks the degree distribution follows a power law [10], [9], [8]. This kind of network is named Scale-free Network. But only their degree distribution is scale-free. For Scale-free Network, the node fraction with a degree  $k$  follows a power law:

$$P(k) \sim k^{-\gamma} \quad (I-1)$$

$\gamma$  is the power law exponent,  $k$  is the degree.

*This is the case of networks like the power grids [10], the World Wide Web, the internet, and the air transportation networks [11].*

In the literature the degree of distribution could also be exponentials, such as those seen in the power grid, railway networks, and power laws with exponential cutoffs, such as those seen in the network of movie actors and some collaboration networks [12].

### ✓ *Random graph*

Random graph are also known as Erdős-Rényi graph. In general, in this model of graph, the probability that a node is of degree  $k$  is given by the binomial law [8], [9]:

$$P(k) = \binom{N-1}{k} p^k (1-p)^{N-1-k} \quad (1-2)$$

$N$  is the number of node. The average distance for these networks is proportional to  $\log N$  [9].

*Social networks belong to this category of network.*

### ✓ *Small world network*

This model was proposed by Watts and Strogatz. The distance between two nodes in small world network decreases very slowly with the number of nodes [13]. It reflects the fact that although the number of vertices in the graph is high, the average distance is relatively short. These networks combine a high degree of agglomeration and a low average distance [9].

*Neural networks belong to this type of networks.*

Structural characteristics resulting from each of these types are interesting and well analysed in the literature. From above definitions, it appears that infrastructure networks seem to belong to the category of scale-free network.

Once networks are modelled by graphs, there are many models of vulnerability that can be applied. These models are presented in the next section.

## I.1.2 VULNERABILITY METRICS

The concept of vulnerability is used in several disciplines: psychology, sociology, political science, economic, epidemiology, biology, environmental and geoscience [14]. Many terms are related to vulnerability concept in the literature: service-ability, reliability, availability, survivability. With respect to infrastructures, vulnerability analysis aims are pointed out by [14]. The author argues that it consists in answering the following questions:

- What can fail?
- What are the consequences?
- How can this happen?
- How to retrieve a nominal state?



To answer the first question, we must focus on network components. Indeed, the resulting vulnerability is strongly linked to that of the components. The second question is more difficult to answer. The range of consequences is large and may take various forms. The third question refers to the feared events. With respect to the listed questions, the implementation of corrective actions is required to solve the problem. The issues pointed out by [14] allow the Decision Maker understanding the context, but they do not take into account one of the aspects of the analysis: what can aggravate or mitigate the consequences? The answer to this question is given in II.2.3.3.

These questions show that vulnerability emphasizes the degree in which people and their possessions are exposed to feared events. It indicates the level of damages which a certain phenomenon may produce and it is expressed on a scale varying from 0 to 1, 1 standing for the total destruction of material assets and loss of human lives in the affected area [15].

Vulnerability is defined in several ways in the literature. Table I-2 resumes some of them.

<b>Definitions</b>	<b>Author</b>
Probability of a complete or partial failure of infrastructures and loss of their ability to maintain their important functions for a certain period	[16]
Propensity to damage or malfunction of various elements exposed to risk (commodities, peoples, activities, functions, systems) constituent a territory and a given society	[1]
System time progressive property to support failure in function of its state	[17]
How a system, organization, or human performance is degraded if some hazard or threat exploits the vulnerability	[18]
Ability of the system to withstand hazard or threat	[19]
System overall susceptibility to lose due to a negative event, ie the magnitude of the damage given a specific strain	[19]
Susceptibility of rare, thought big, risks, while the victims can hardly change the course of events and contribute little or nothing to recover	[20]
Susceptibility to incidents that can result in considerable reductions in road network service-ability. These incidents may then be more or less predictable, caused voluntary or involuntary, by man or nature	[21]
Manifestation of the inherent states of the system (e.g., physical, technical, organizational, cultural) that can be exploited to adversely affect (cause harm or damage to) that system	[18]
Characteristic of a critical infrastructure's design, implementation, or operation of that renders it susceptible to destruction or incapacitation by a threat	[22]
Vulnerability refers to how a system, an organization or human performance is degraded if some hazards or threats exploits the vulnerability	(Haimes 2006) in [19]
Consequences that arise when a system is exposed to a strain for à given type and	[19]

magnitude	
Flaw or weakness in the design, implementation, operation and/or management of an infrastructure system, or its elements that render it susceptible to destruction or incapacitation when exposed to a hazard or threat or reduces its capacity to resume new stable conditions	(Kröger et Nan) in [23]
Susceptibility (sensitivity) to threats and hazards that substantially will reduce the ability of the system to maintain its intended function	[14]
Collection of properties of an infrastructure system that might weaken or limit its ability to maintain its intended function, or provide its intended services, when exposed to threats and hazards that originate both within and outside of the boundaries of the system	Holmgren and Molin (2005) in [14]
Degree of loss or damage to the system when exposed to a perturbation of a given type and magnitude	[24]
The probability of damage to all or part of an infrastructure and the loss of its ability to maintain its important functions during a certain period	[16]

*Table I-2: Vulnerability definitions*

Defintions given in Table I-2 highlight two viewpoints:

- System-based view: focuses on how the considered system will fail or change from one state to another. This view is shared by [24], [17] and [18].
- Event-based view: considers the amplitude and/or the frequency of one or more events. This view is shared by [16], [1] and [19].

These two points of views are complementary. The vulnerability perception of a system remains dependent on considered states, and analysts' views.

*For instance, the state of the system could be related to its performance [18] quoted by [19], to its reliability or to any others criteria.*

In the literature, survivability is used as an antonym of vulnerability. Survivability is generally used when talking about a disaster when it has already occurred while vulnerability concern the characteristics of an asset to resist to the feared event before its occurrence [25]. The survivability is defined as the capability of a system to fulfil its mission in a timely manner in the presence of attacks, failures, or accidents [18] and concerns the system's performance after the occurrence of a feared event while vulnerability is the susceptibility of system facing feared events [26].

From definitions in Table I-2 we pointed out many attributes associated with vulnerability:

- Vulnerability is time dependent;
- A vulnerable system assumes the existence of a feared event;
- Vulnerability is related to the system incapacity to play the role it has been designed for

In our view, vulnerability is necessarily associated with the system it characterizes. For this reason the following definition is provided.

**Definition I-1: Vulnerability is the incapacity of a stake to resist to the occurrence of a feared event and to recover efficiently its nominal function during a given period of time.**

The concepts of stake and feared event will be introduced in II.1.2.2.

As further shown below, many vulnerability metrics in the literature are based on the network structure. In fact, some authors consider that the effectiveness of network functions realization is affected by its structure [27]. In [28] the authors argue that at the occurrence of a feared event, loss and damage depend on the structural organization and vary from one network to another. Then, analysing the topology of the network allows a better comprehension of the dynamic phenomena that affects its performances [29], the identification of its weaknesses [30] and the estimation of its vulnerability [29], [31].

Network parameters for vulnerability analysis include the degree, the clustering coefficient, the average distance, and the load [29]. Besides these parameters, one can observe four other classes namely: efficiency, integrity, probability and others vulnerability functions. Whatever the function used, the vulnerability might not increase with the addition of edge [29] and its analysis should help to measure the system's response after a feared event occurrence [28]. These parameters are presented in the following sections.

#### ✓ *Betweenness centrality*

---

The betweenness centrality  $C_B$  stands for the fraction of path going through a node  $V_x$  [32] quoted by [33].

$$C_B(V_x) = \sum_{V_i \neq V_j \in V} \frac{\sigma_{V_i V_j'}(V_x)}{\sigma_{V_i V_j}} \quad (I-3)$$

where  $\sigma_{V_i V_j}$  is the number of geodesics (paths) between  $V_i$  and  $V_j$ , and  $\sigma_{V_i V_j'}(V_x)$  is the number of geodesics between  $V_i$  and  $V_j$  that passes  $V_x$ . The load is defined in the same way for an edge  $E_i$  [33].

$$C_B(E_x) = \sum_{V_i \neq V_j \in V} \frac{\sigma_{V_i V_j'}(E_x)}{\sigma_{V_i V_j}} \quad (I-4)$$

Where  $\sigma_{V_i V_j'}(E_x)$  is the number of geodesics between  $V_i$  and  $V_j$ , that includes the edge  $E_x$ .

The centrality determines the importance of a node in a network [33].

For vulnerability estimation, the centrality of one component is calculated before and after the occurrence of the feared event (which means the removal of one or many nodes/edges) [11], [34], [35]. The centrality is a good indicator of the structural importance of a node or an edge in the graph. But from our view, it does not adjudicate on the vulnerability. Indeed, the vulnerability is induced by several failure modes. These modes result from component constitution, but also because of the overall dynamics.

### ✓ Average Path Length

The average path length between two nodes is the mean of the edges number of shortest paths [9].

$$\ell = \frac{1}{N(N-1)} \sum_{v_i \neq v_j \in V} D(v_i, v_j) \quad (I-5)$$

To avoid infinite mean (the distance is infinite if no link exists between the nodes), the inverse of the average path [34] and [33] is commonly used.

$$\ell' = \frac{1}{N(N-1)} \sum_i \sum_j \frac{1}{D(v_i, v_j)} \quad (I-6)$$

The average path measures the dispersion of the network and expresses the difficulty of communication between two nodes [36]. It also indicates the flow of traffic on the network. In our view, the average path length is a good indicator of structural vulnerability. The smaller is the parameter, the less vulnerable will be the global network.

$\ell'$  is described in [11], [36], [37] and [38] as the efficiency and related to the network performance. The efficiency of a path between two vertices is the average efficiency of all the edges constituting the path. Resilience, which is one of the measures of vulnerability, is the drop of efficiency induced by the deterioration of edges [36], [35]. We will define this concept later in II.1.8. Vulnerability is then seen as the lack of network performance and is defined by.

$$VUL(E_i) = \frac{E(G) - E'(G)}{E(G)} \quad (I-7)$$

Where  $E(G)$  is the overall efficiency of the system and  $E'(G)$  is the efficiency of the network after removal of the edge  $E_i$ . The overall vulnerability of the graph is then defined by:

$$VUL(G) = \max[V(E_i)] \quad (I-8)$$

Finally, some authors consider the loss of performance caused by the removal of a node instead of an edge [39], [28]. The vulnerability of the graph and its nodes are assessed in the same way. This way of estimating the vulnerability is very interesting. Interest focuses on the structure but not on the real circulation of flows in the network. Furthermore this approach does not take into account the intrinsic reliability of each component.

✓ **Clustering coefficient**

---

Let us consider three nodes  $V_i, V_j$  et  $V_s$ . If the node  $V_i$  is linked to the node  $V_j$ , and the node  $V_j$  to the node  $V_s$ , the transitivity is the average probability that the node  $V_i$  is linked to the node  $V_s$ . It measures the density of triangles in the network [9]. The number of possible connections for a node of degree  $D(V_i)$  is [9]:

$$\binom{D(V_i)}{2} = \frac{D(V_i)[D(V_i)-1]}{2} \quad (I-9)$$

By noting  $M_i$  the number of links between vertices incident to node  $V_i$ , the clustering coefficient of node  $V_i$  is then [9]:

$$C_i = \frac{M_i}{\binom{d(V_i)}{2}} \quad (I-10)$$

The clustering coefficient of a graph will be then [9] , [33]:

$$C(G) = \frac{1}{N} \sum_i C_i \quad (I-11)$$

The clustering coefficient is a good indicator of network vulnerability. However, it does not give any idea on the vulnerability of a component. Indeed, the more, there will be of a triangle in the network, the less it will be vulnerable.

✓ **Connectivity**

---

Node connectivity is called cohesion, and edge connectivity is called adhesion. The node connectivity (respectively edge) of a graph is the minimum number of nodes (respectively edges) to be removed from the graph to disconnect it [40], [29]. A disconnected graph is a graph for which some flow cannot reach its destination. Connectivity is a vulnerability measure [9]. The higher the connectivity the less vulnerable will be the network.

✓ **Integrity**

---

Integrity is the ratio  $N_i/N_0$ . Where  $N_i$  is the size of the graph after damage of a fraction  $i$  of nodes compared with the initial size  $N_0$ . Vulnerability can be seen as a lack of integrity [13], [41], [41] and [42]. Other authors define integrity in relation to the weight, the geodesic distance and the range (ratio between the distance and weight) [37]. The integrity is related to the graph robustness. It does not give any indication on the graph, node or edge resilience.

### ✓ Probability

The vulnerability of a system is measured in [9] and [14] as the probability  $P(\max_{t \in T} X(t) > x)$  for a given period of time  $T$ , that the negative consequence  $X(t)$  of the disturbance is greater than a value  $x$ . Taking into account the occurrence of a feared event  $A_i$ , the total probability would be the sum of probabilities.

$$P(\max_{t \in T} X(t) > x) = \sum_i P(A_i) * P(\max_{t \in T} X(t) > x / A_i) \quad (I-12)$$

Where  $A_i$  is the initiating event. The main concern with these functions is the correlation between consequences and feared events. The range of consequences is large. An estimation on the basis of the expertise is certainly interesting but insufficient for an objective assessment of the vulnerability.

### ✓ Vulnerability function

Several authors suggest vulnerability functions in the literature. In [27] the authors define a vulnerability function for a graph with  $N$  nodes and  $M$  edges by:

$$V(G) = \exp\left(\frac{\sigma}{N} + N - M - 2 + \frac{2}{N}\right) \quad (I-13)$$

Where  $\sigma$  is the standard deviation of the degree distribution. This function does not take into account the vulnerability indicators such as cohesion (vertices degree) and adhesion (edges degree) [29], [40]. Moreover, the term does not allow the comparison between networks of different sizes and structures [29].

In this part, we have introduced the concept of vulnerability and approaches to estimate it. The majority of scientific approaches ignore the flow dynamics. We overcome these gaps with a simulation-based approach. We will thus introduce in II.1.8 some essential elements for the vulnerability estimation: flow, feared event, aggravation and mitigation factor etc.

Vulnerability assessment is often a prerequisite to decision-making. We thus present in the following a review of decision-making process in the field of the infrastructure networks vulnerability analysis.

## I.2: DECISION AIDING LITERATURE REVIEW

Decision theory aims to justify, analyse and streamline actions susceptible to have negative consequences [43]. Historically, decision theory comes from the hazard formalization on board games. Later, in the period just before the World War II, decision aiding knows a major development. It exists studies conducted by the British Army as part of the installation of radar systems and German communications decoding efforts (1936-37) [44]. The boost of the discipline will come with the success of operational research, linear programming and the game theory. Later in 1948, the development of project such as RAND [45] will give a new impulse to the discipline. Many theories will emerge to make the discipline increasingly relevant.

At this point in time, decision theory touches varied and diverse domains like management, politics, economics, mathematics, psychology, risk analysis and conflict of interest situations [43]. The scope is so broad that a complete literature review is not possible [44]. This wide application area makes the decision aiding activity a scientific and professional one with some formalism and abstraction [44]. Formal and abstract approach allows then the decision-maker to better analyse, understand, and justify the issues and/or the solutions. The formalism is justified by the use of formal languages to reduce human language ambiguity. The abstraction refers to the use of languages independently to the realm of the discourse. Despite the used formalism and abstraction, the concept of decision and decision aiding is diversified. For this reason some definitions are provided. Decision aiding is defined in several ways in the literature. In [45] and [46], ontological elements are introduced to define decision components. This implies:

- Decision object: Purpose, program operation, instrument;
- Decision organ: Organization, group, individual;
- Decision type: Routine, creative, program application;
- Decision scope: Strategic, tactical, and operational;
- Decision elements control: Good, average.

Some definitions of the decision are proposed in Table I-3.

<b>Definition</b>	<b>Author</b>
A decision is an action that is taken to deal with a difficulty or respond to an environment change, that is to say, to solve an individual or organization problem	[46]
A decision is the act of a single individual (decision maker) which has a free choice between several possible actions at a given moment in time	[47]
A decision, whether individual or resulting from a work group can be defined as engaging in an action, that is to say, an explicit intention to act	[48]

*Table I-4: Decision definition*

From the definitions given in Table I-4, decisions could be classified in many ways. In [49] the authors distinguished normalized and non-normalized decisions according to their nature. One decision is normalized if it exists an explicit process. A non-normalized decision is threatened by a non-programmed procedure [50]. At the structuration level, decision are classified by [51] in three categories: Structured decisions, bad structured decisions, and non-structured decisions. In structured decision the problem is established in technical terms and data are assumed as reliable. Bad structured problems require a big effort to formalize data which are qualitative, unstable, difficult to access etc. In non-structured decisions, problems are not clearly addressed. This point of view is also shared in [49] where decisions are classified into Structured, Semi structured, and Not structured decision.

The definition of decision aiding adopted in this thesis is the one proposed in [52].

**Definition I-2: Decision aiding is the activity of a person (analyst) who, resting on models clearly explained and more or less completely formalized, searches some answer elements of an intervener in the decision process. (Decision Maker), elements contributing to shine the decision and normally prescribe behaviour likely to increase the coherence between the evolution of the process on one hand, the objectives and the value system of whom service this in intervener is placed one the other hand.**

This definition leads to some problem pointed out in [53] and [50]:

- Description: problems associated with the actual characterization of the current state of the organization;
- Investigation: associated with the relationship between two or more problems data or phenomena;
- Explanation: problems associated with establishing a causal relationship;
- Prediction: Problems associated with the future projection based on data feedback;
- Prescription: problems associated with the normative projection based on data feedback;

Decision aiding relies on postulates pointed out by [47] quoted by [50]:

- First order reality assumption: the main aspects of the reality in which the decision aiding relies on are related to knowledge objects. These objects can be viewed as stable data;
- Assumption of the decision maker: any decision is made by a decision-maker, actor clearly identified, with full powers, acting under a rational preference system with some axioms excluding ambiguity and incomparability, that are not modified by the decision aiding;
- Assumption of optimum: in any situation leading to a decision, there is at least an optimal decision. For this decision, it is possible to establish objectively that there are not strictly better decisions. The optimal decision is supposed to remain neutral towards the decision process.

Decision aiding is related to process presented in the next section.

### I.1.3 DECISION AIDING PROCESS

Vulnerability and risk analysis are presented in [54] as a problem of individual or collective decision to reduce the complexity by supporting the problem formulation. From this observation, we can also say that analysing the vulnerability aims at making decisions in a certain environment. The vulnerability analysis and decision aiding are so intertwined.



In [49] the author was one of the first to argue that decision is not an action but a process carried out to solve problem. The author says also that decision is composed of four steps not always distinct: Intelligence; Design; Choice; Review. In [54] three phases are pointed out in the area of risk management: problem formulation, exploitation and recommendation. Decision aiding process pointed out by these authors focuses on the way decision makers collect and use information in order to understand and assist others stakeholders [55].

In a classification perspective, different decision processes are categorized by [56] depending on the level of authority and the proximity of the danger. The authors distinguished thus:

- Office automation- analytical: Actions are taken by identified decision makers;
- Political: Selection of actions under conflict of interest between stakeholders ;
- Managerial: Actions are based on a satisfactory strategy. They are taken by considering consequences but on the basis of rules and code of conduct;
- Routine operations: Actions result from automatism and rarely from conscientious analysis. Implicit rules and experience are used;
- Crisis Management: Actions to reduce negative consequences of a phenomenon.

This classification does not allow processes differentiation. One process could be political and include crisis management. That is why we propose another classification based on the type of the process itself. We then distinguished three categories according to decision phases' succession: linear, cyclical, and mixed. An example of each of them is presented in the next sections.

### ✓ *Linear decision aiding process*

---

Linear decision aiding process consists in sequential steps. Figure I-1 presents a process described in [57]. The particularity of this kind of process is the succession of its phases. Linear processes are suitable for the problem with minor stakes. But as soon as the context is of a certain complexity, linearity becomes source of amplification of the consequences by preventing any feedback loop. The cyclical process presented in the following section allows overcoming this lack.

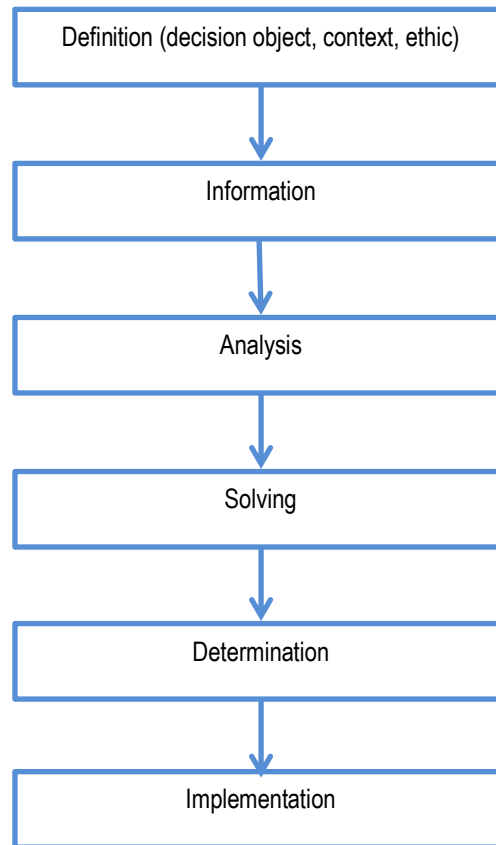


Figure I-1: Linear decision process by [57]

#### ✓ Cyclical decision aiding process

---

Cyclic decision processes are presented in form of cycle. The Figure I-2 presents an example of cyclic process [58] [59]. Cyclic processes are adapted to middle complexity problems. It is possible to return to the phase source of error after a cycle time whose duration varies according to the situation. The main difficulty for the analyst is to short down this time. The hybrid processes presented in the next section can be used to tackle this problem.

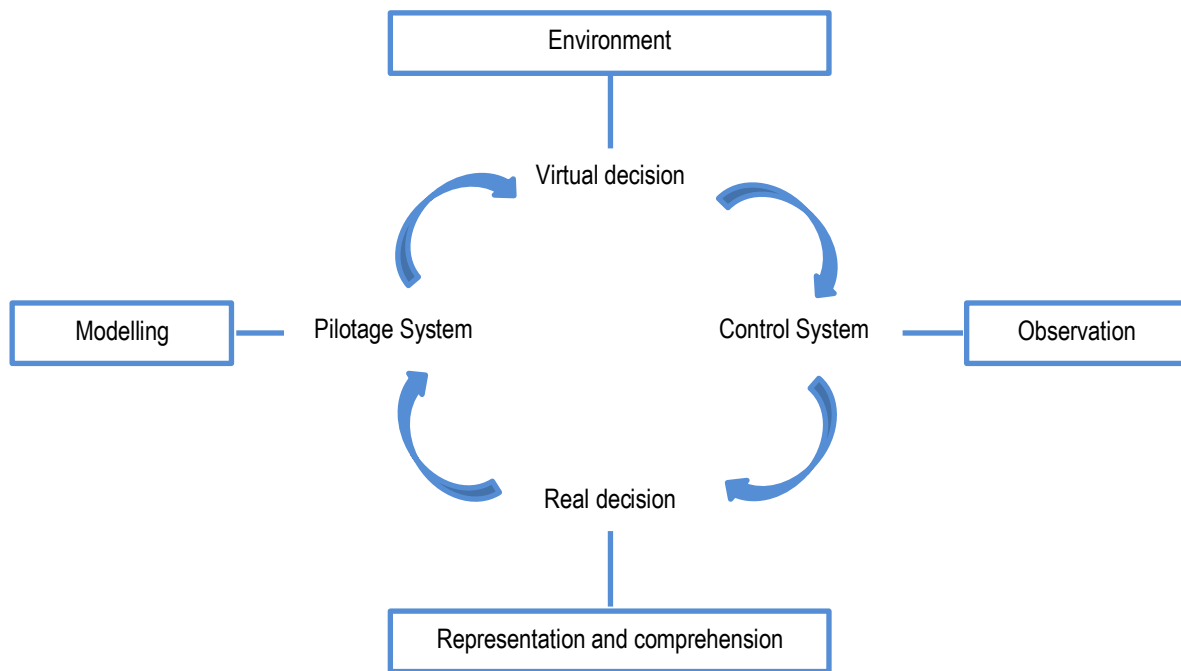


Figure I-2: Cyclic decision aiding [58]

✓ **Hybrid process**

Hybrid processes are the combination of linear and cyclic process. One example is proposed in [49]. An hybrid decision process for decision maker selection is proposed in [60]. She argues that decision is a process enrolled in time called Decision Time Line.

Hybrid decision processes are adapted to many contexts whose complexity may differ. Whatever the type of the decision process, it is fitted of some linear elements pointed out by [61]. The author argues that elements of the decision process are constitutive of:

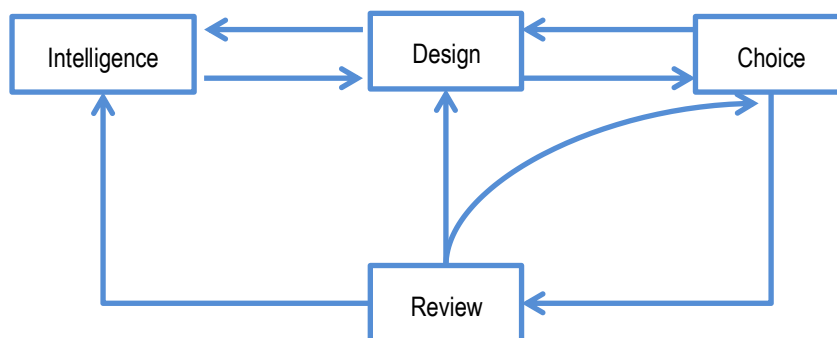


Figure I-3: Hybrid process by [49]

- A research process to find goals;
- The exact formulation of objectives;
- The selection of alternatives to achieve these goals;

- The results evaluation.

Methods that could be used in these processes are presented in the next section.

#### **I.1.4 DECISION AIDING METHODS**

It turns out to be very difficult to make a full presentation of all decision aiding methods [44]. In a general way, in decision aiding, comparison of several actions is rarely a single criterion. That is due to the fact that when we have multiple objectives, it is difficult to reach them all at once [62]. Bernard Roy shows that optimization is not often the only neither the best approach to get a solution [54].

Speaking about research type in decision aiding in general, there are two types of methods pointed out in [59] and shown on Figure I-4: Analytical approach and descriptive approach. Decision aiding Approach can be seen as the passage from problem situation to decision model [44]. Analytical approach aims to translate decision problem into mathematical functions to be optimized. Descriptive methods are used to describe decision making problems. In this approach the decision maker tries to use strategies already used by other decision makers in similar situations.

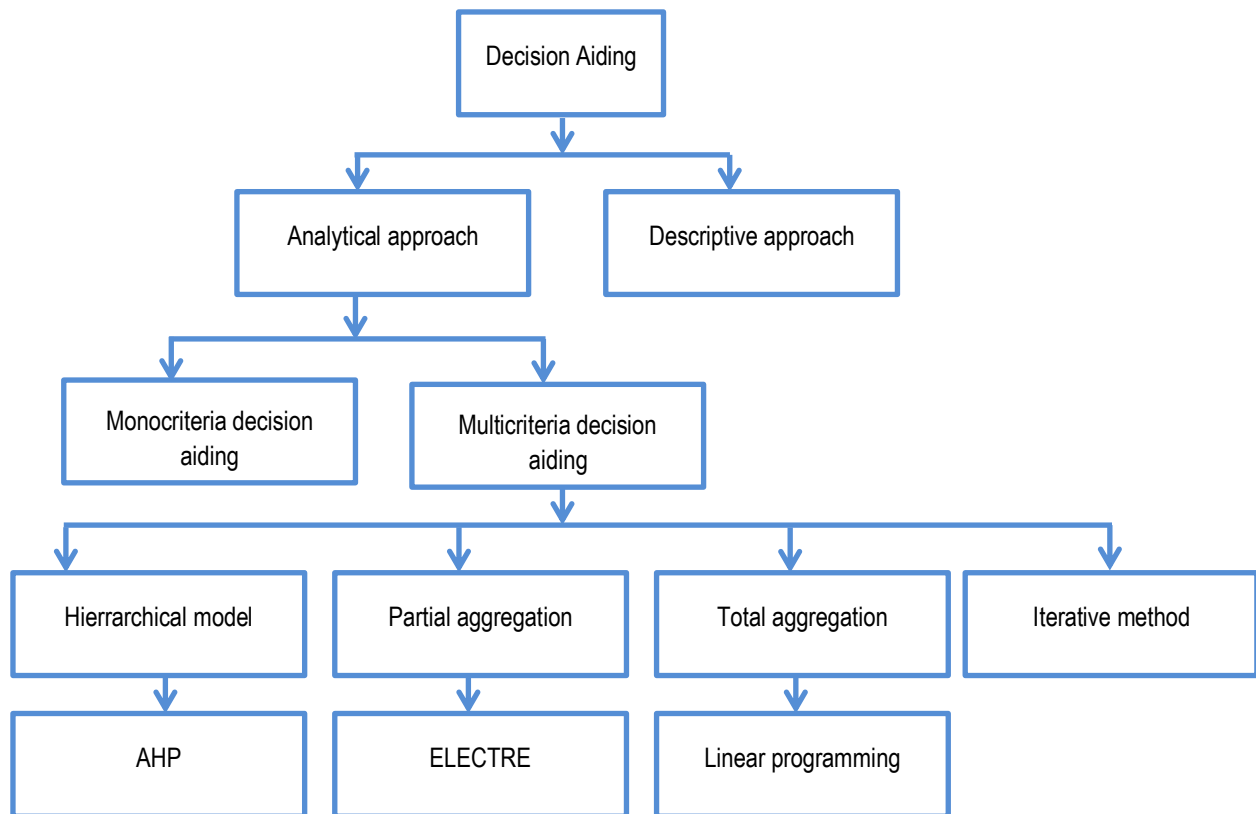


Figure I-4: Decision aiding methods

- Analytic or prescriptive approach: The objective of these approaches is to provide to decision maker tools for taking optimal decision in a given situation through mathematical models [50];
- Descriptive approach: These approaches intended to model decision makers decision process to describe the context , analyse and exploit decisions if possible[50].

Let's consider the problem of analysing the vulnerability of interdependent networks. A set of action was defined with more or less predictable consequences. The classical approach consists in associating to each system state probability the actions' consequences. We can then use a utility function on consequences whose maximum value allows determining actions to apply.

The existence of this function is guaranteed by a number of axioms stating that, in theory, there is a rational behaviour for decision maker. Preferences are transitive so the probabilities are independent [44]. This is not the case in our analysis. Indeed, different probabilities are dependent on each other. This approach is called normative because decision makers must adapt their behaviour and preferences to the axioms [44]. The descriptive approach will consist in adopting some strategy to make a decision under similar conditions.

In [44], the author notes that descriptive methods are again of imposing rationality model to problem situation independency. This approach is difficult to apply in situations of natural disaster, given that each situation is isolated and crisis management is made by cooperating authorities but not necessarily on a feedback.

In the reality of natural disasters, problems are difficult to identify. Values of decision makers who define their preferences are difficult to understand in the allotted time. In the context of infrastructure network failure the question is related to the possibility of identifying every state of the system. In other words, looking for the solution of a problem well formulated is always possible. The risk is to seek a solution to a problem that does not exist [44].

In this literature review we have separated the two groups of methods presented in the following: Elementary methods and multicriteria methods. This separation is made by the complexity of the method. The next following sections will present some of them.

#### I.1.4.1 CLASSICAL METHOD OR SINGLE SYNTHESIS CRITERION

Table I-5 shows some elementary methods.

<b>Methods</b>	<b>Reference</b>	<b>Description</b>
Weighted sum	[21,40,54]	The global performance of an alternative is computed as the weighted sum of its evaluations along each criterion. The global performance is used to make a choice among all the alternatives
Lexicographic method	[40,79]	Based on the logic that in some Decision Making Situation (DMS) a single criterion seems to predominate. The procedure consists in comparing all the alternatives with respect to the important criterion, and proceed with the next one until only one alternative is left
Conjunctive method	[40,20]	An alternative which does not meet the minimal acceptable level for all criteria is rejected. The minimal acceptable levels for each criterion are used to screen out unacceptable alternative
Disjunctive method	[40,20]	An alternative is selected on the basis of its extreme score on any criterion. Desirable levels for each attribute are used to select alternatives which equal or exceed thresholds
Maximin method	[40]	The overall performance of an alternative is determined by its weakest or strongest evaluation
Single synthesizing criterion		
TOPSIS (technique for order by similarity to ideal solution)	[40]	The chosen alternative should have the profile which is the nearest (distance) to the ideal solution and farthest from the negative-ideal solution
MAVT (multi-	[43,45]	Aggregation of the values obtained by accessing partial value functions on

attribute value theory)		each criterion to establish a global value function $V$ . Under some conditions, such a function $V$ can be obtained through an additive, a multiplicative or a mixed technique
UTA (utility theory additive)	[41]	Estimate the value functions on each criterion using ordinal regression. The global value function is obtained through an additive technique.
SMART (simple multi-attribute rating technique)	[26,27,62]	Simple way to implement the multi-attribute utility theory by using the weighted linear averages, which gives extremely close approximation to utility functions. There are many improvements associated with this method like SMARTS [28], SMARTER [8].
MAUT (multi-attribute utility theory)	[19,43,93]	Aggregation of the values obtained by accessing partial utility functions on each criterion to establish a global utility function $U$ . Under some conditions, $U$ can be obtained through an additive, a multiplicative or a distributional technique.
AHP (analytic hierarchy process)	[81,82]	Converting subjective assessments of relative importance into a set of weights. This technique applies the decomposition, the comparative judgments on comparative elements and measures the relative importance through pairwise comparison matrices which are recombined into an overall rating of alternatives.
EVAMIX	[94]	Two dominance indexes are calculated: one for ordinal evaluations and one for cardinal evaluations. The combination of these two indexes leads to a measure of the dominance between each pair of alternatives.
Fuzzy weighted sum	[4,23,46]	These procedures use a-cut technique. A level sets are used to derive fuzzy utilities based on the simple additive weighted method
Fuzzy maximin	[10,98]	This procedure is based on the same principle as the standard maximin procedure. The evaluations of the alternatives are fuzzy numbers.

Table I-5: Elementary methods by [63]

The unique synthesis criterion is to synthesize the family of criteria into a single criterion. In this method, there is no incomparability. It consists in building a single criterion synthesis using an aggregation function  $V$  by putting:

$$g(a) = V(g_1(a), g_2(a), g_3(a), \dots, g_n(a)) \quad (I-14)$$

Function  $V$  usually takes one of the following forms [64].

### ✓ *Weighted sum*

---

$$\begin{cases} \text{aggregation by weighted sum: } g(a) = \sum_{j=1}^n k_j g_j(a) \\ \text{additive aggregation : } g(a) = \sum_{j=1}^n k_j v_j [g_j(a)] \end{cases} \quad (I-15)$$

Where  $k_j$  is the criterion weight  $\sum_{j=1}^n k_j = 1$  and  $v_j \in [0,1]$  is the veto threshold. In [65] the authors showed the sensitivity of the method of weighted sums throughout the criterion scale. This represents a major disadvantage since the changing of scale is a simple operation that decision makers may have to do during the process of decision aiding [62].

*For example one decision maker can choose the Euro and another the Pound as monetary unit.*

The second weakness of the weighted sum is compensation between criteria [62]. In fact, action negatively evaluated on a criterion may catch if it is positively evaluate on another.

### ✓ *Laplace criterion*

---

Historically, the Laplace criterion is known as the first to be introduced. It was proposed a century earlier by Huygens. For an action resulting in  $n$  consequences, it is given by:

$$L(a) = \frac{1}{n} \sum_{i=1}^n c_i(a) \quad (I-16)$$

Where  $c_i(a)$  is the consequence of the decision  $a$  for the state  $i$  and  $n$  is the number of state. This criterion is not applicable to the networks vulnerability analyses because the consequences are often in different units. It does not take into account either uncertainties about the consequences.

### ✓ *Bernoulli criterion*

---

Bernoulli criterion is similar to the one of Laplace. The difference is in the use of the logarithmic function to make difference between low and high changing of the consequences [43].

$$B(a) = \frac{1}{n} \sum_{i=1}^n U[c_i(a)] \quad (I-17)$$

Where  $U$  is a logarithmic function.

### ✓ *The expected value criterion*

---

Taking into account the probability of every state, Laplace criterion becomes the expected value criterion.



$$E(a) = \sum_{i=1}^n p_i c_i(a) \quad (I-18)$$

Where  $p_i$  is the probability associated with state  $i$ .

#### ✓ *Criterion of expected utility*

---

Theory of expected utility has been developed as part of risk situations where consequences probabilities are known. Formally a decision problem is said at risk if, for each action there is a probability distribution on the consequences [43].

$$V(a) = \sum_{i=1}^n p_i U[c_i(a)] \quad (I-19)$$

The fundamental principle of the theory of expected utility is that in risk situation, decision maker's behaviour is entirely determined by the preferences on probability distributions (lotteries) on the action consequences. In such situations, decision maker is called rational if the choice of its decisions is consistent with its preferences on lotteries. Theory of expected utility is a representation of preferences over lotteries. It allows defining a criterion (expected utility) by which lotteries may be compared [43].

The utility theory is based on the following axioms:

- Preferences define a total order on lotteries: this means that all lotteries can be ranked and compared;
- For the lottery  $l$ , if all lottery of a lottery set  $ln$  are preferred to  $l$  and if this suite has a limit  $l_0$ , then this limit is preferred to  $l$ ;
- Given the two lotteries  $l$  and  $l'$  such as  $l$  is preferred to  $l'$ , and a number  $t$  between 0 and 1, for a third lottery  $l''$ , the composed lottery  $tl + (1 - t)l''$  should be preferred to  $tl' + (1 - t)l''$ ;

There are other criteria like those of Wald, Hurwicz, Savage but not presented in this chapter. The reader is invited to see [43] for more information.

#### **I.1.4.2 MULTICRITERIA DECISION AIDING**

Multicriteria decision aiding relies then on a coherent family of criteria instead of one single criterion. Multicriteria aggregation procedure enables going from a partial judgment (on an indicator / criteria) to an overall judgment of the study object to take adequate measures [66]. Multicriteria decision approaches can be grouped according to many characteristics: decision makers rationality, decision universe, provided action type [59]. A classification proposed in [59], [44], suggested four categories: Hierarchical approaches, Total aggregation approaches, partial aggregation approaches and iterative approaches. Similar classification is given in [47] and [67]. The difference between these aggregation approaches is indistinct [68]. It resides in multicriteria aggregation procedures [ also called exploitation phase [54].

Outranking methods consists among others in: ELECTRE, QUALIFLEX, ORESTE, REGIME, PROMETHEE, PRAGMA/MACCAP, N-TOMIC, MACBETH. These methods are based on ELECTRE method. In outranking methods, two procedures are used: the first is to build outranking relations while the second is an exploitation procedure. Outranking consists in moving from a relationship based on comparison of each criterion to a global relation of comparison. Table I-6 shows some outranking methods.

<b>Methods</b>	<b>References</b>	<b>Description</b>
ELECTRE I	[70]	The concept of outranking relationship is used. The procedure aims to reduce the size of non-dominated sets of alternatives (kernel). The idea is that an alternative can be eliminated if it is dominated by other alternatives to a specific degree. The procedure is the first one to seek to aggregate the preferences instead of the performances.
ELECTRE IS	[79]	This procedure is exactly the same as ELECTRE I, but it introduces the indifference threshold.
ELECTRE II	[78]	ELECTRE II use two outranking relations (strong and weak).
ELECTRE III	[71]	The outranking is expressed through a credibility index.
ELECTRE IV	[80]	This procedure is like ELECTRE III but did not use weights.
ELECTRE TRI	[79]	This procedure is like ELECTRE III and use the conjunctive and disjunctive techniques to affect the alternatives to the different categories (ordered).
PROMETHEE I	[18]	PROMETHEE I is based on the same principles as ELECTRE and introduces six functions to describe the Decision Maker (DM ) preferences along each criterion. This procedure provides a partial order of the alternatives using incoming and outgoing flows.
PROMETHEE II	[17]	PROMETHEE II is based on the same principles as PROMETHEE I. This procedure provides a total preorder of the alternatives using an aggregation of the incoming and outgoing flows.
MELCHIOR	[50]	MELCHIOR is an extension of ELECTRE IV
ORESTE	[69]	This procedure needs only ordinal evaluations of the alternatives and the ranking of the criteria in terms of importance.
NAIADE (novel approach to imprecise assessment and decision environments)	[60]	This procedure uses distance semantics operator to assess the pairwise comparisons among alternatives. The fuzzy evaluation are transformed in probabilities distributions and as PROMETHEE, this procedure compute incoming and outgoing flows.

Mixed methods		
QUALIFLEX	[64]	This procedure uses a successive mutations to provide a ranking of the alternative corroborating with the ordinal information.
Fuzzy conjunctive/disjunctive method	24]	When data are fuzzy, the match between values and standard levels provided by the DM and the evaluations becomes vague and a matter of degree. The degree of matching is computed using the possibility measure and the necessity measure. The alternatives with the highest degree of matching are considered the best.
Martel and Zaras method	[56,57]	This procedure uses the stochastic dominance to make pairwise comparison. These comparisons are used as partial preferences and an outranking relation is built based on a concordance index and discordance index.

*Table I-6: Outranking methods by [63]*

In the field of risk management another classification is given by [54]. This classification is based on the context shown in Figure I-5.

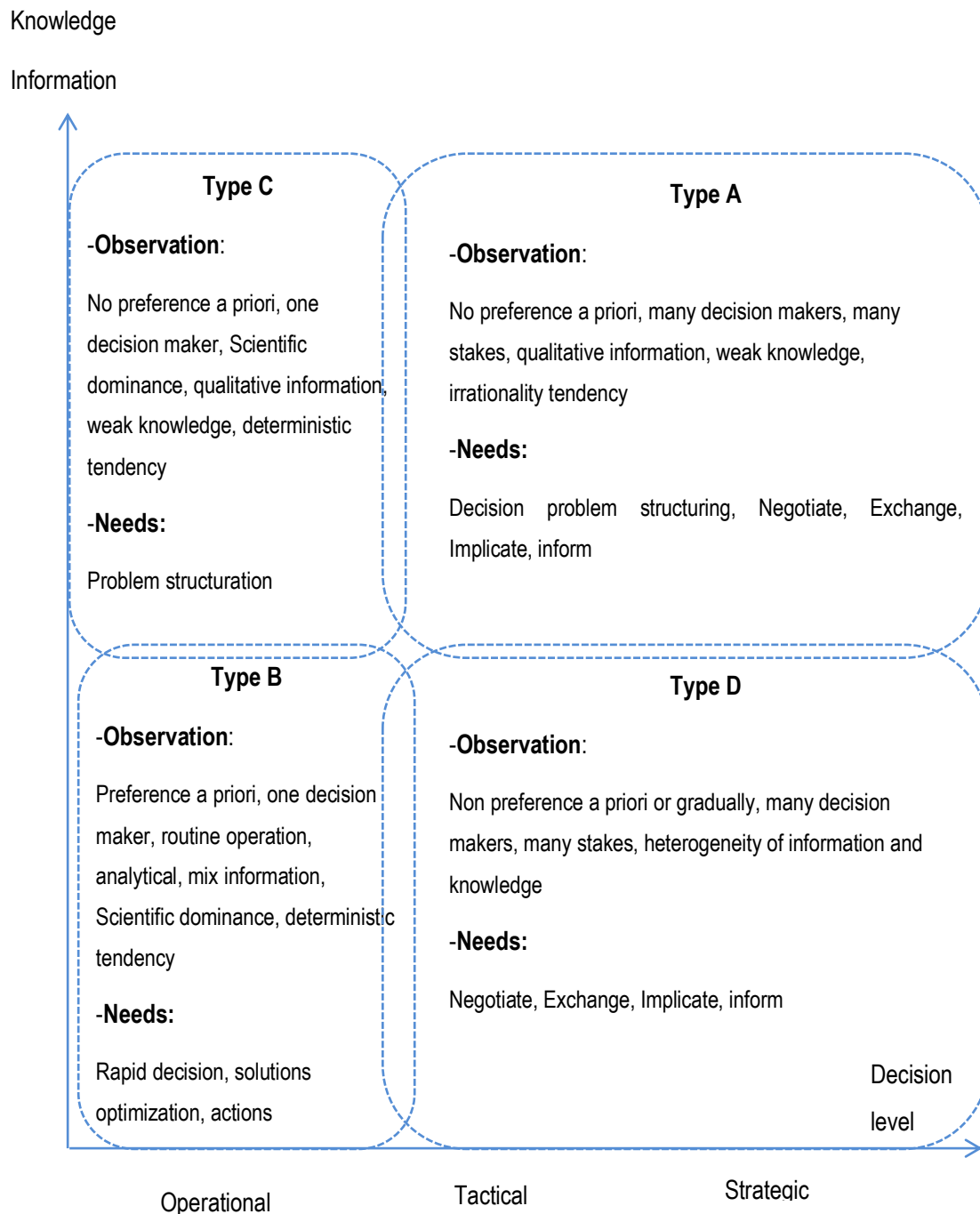


Figure I-5: Type of risk analysis by [54]

This figure classified decisions according to the preference, the number of decision maker, the operation type, etc. The axis knowledge/Information is related to the need of knowledge and information. These elements are placed according to the degree of information and knowledge needed. It follows then four categories A, B, C, D. For instance for the category A, we have weak knowledge about the context. So the need of information is higher for this category. From these categories the authors determined four types of methods. These are shown in the Figure I-6.

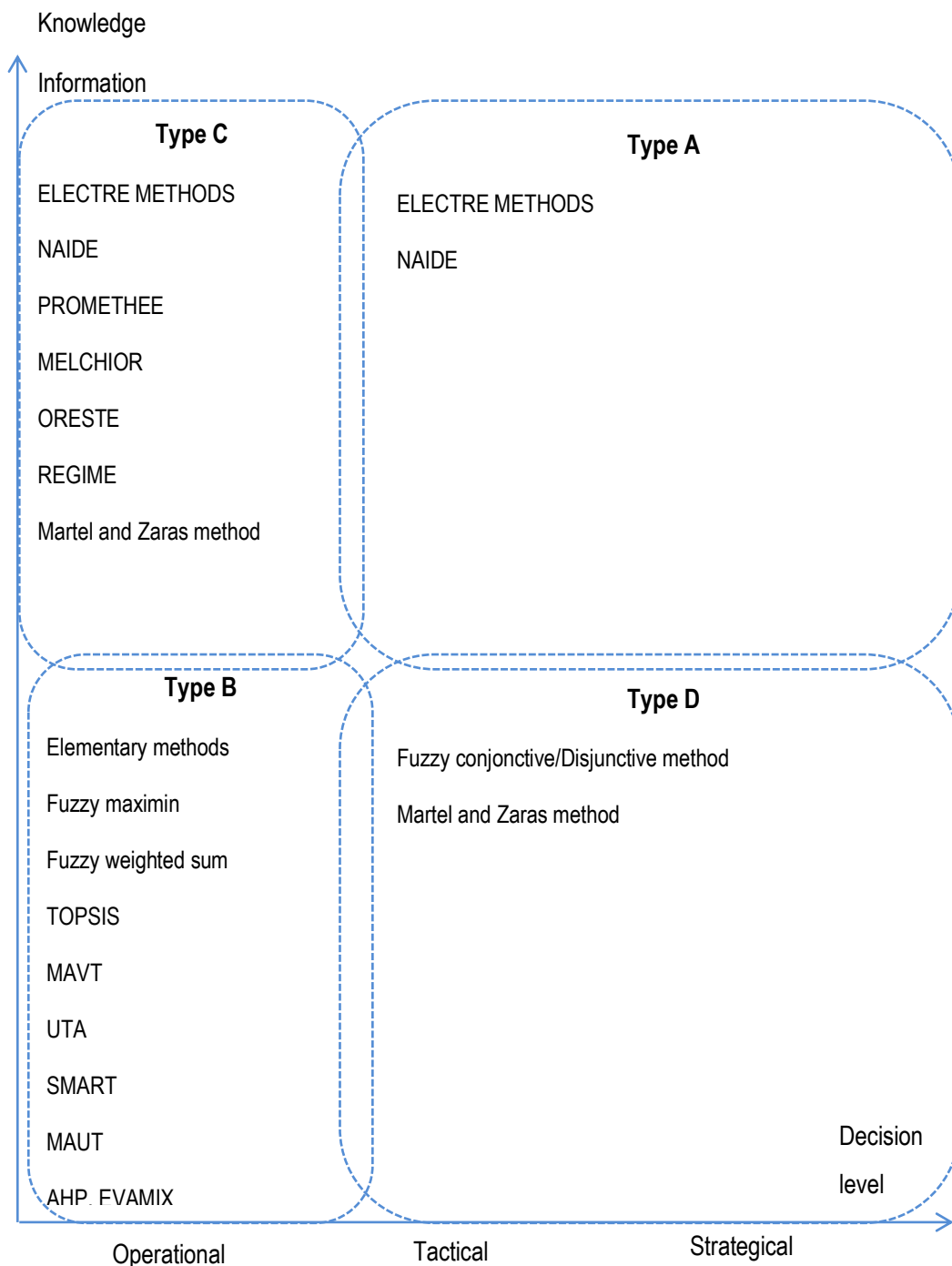


Figure I-6: Multicriteria decision aiding methods for risk analysis type by [54]

It can be noticed that the ELECTRE (Elimination Et Choix Traduisant la Réalité- Elimination and Choice Expressing the Reality) methods suit to A and C categories. There are few methods for the situation D on the contrary of the situation B.

To determine decision maker's preference system, Bernard Roy determined four relations:

- Indifference: Corresponds to equivalence between two actions;
- Strict preference: Corresponds to a significant preference of one of the two actions;
- Low preference: Corresponds to the existence of clear and positive reason that imply a strict preference for one of the two actions, but these reasons are insufficient to infer either a strict preference to the other or an indifference between these two actions;
- Incomparability: Corresponds to the absence of clear and positive reasons justifying one of the three previous situations.

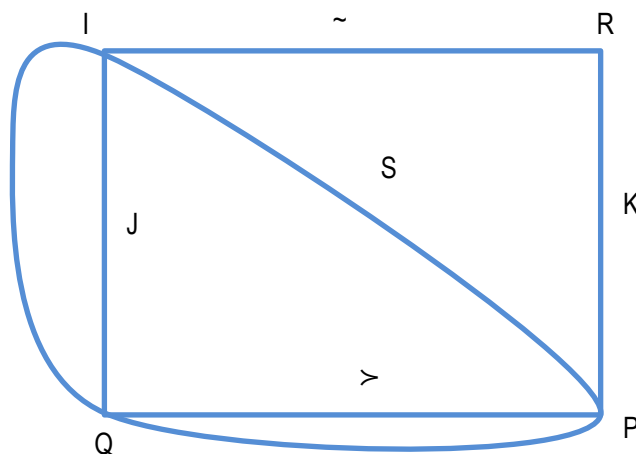


Figure I-7: Preference relations

From these four relations, five hybrid relations are shown in Figure I-7. Through these relations, it is possible to build decision makers relational preference system. These relational systems are used in many methods and issues.

[69] determined relevant context for ELECTRE methods. Our analysis shows that the context of this thesis suits ELECTRE utilization for many reasons:

- There are many criteria;
- Actions are evaluated for at least on criterion on an ordinal scale;
- A strong heterogeneity related with the nature of evaluation exists among criteria (Human, Environment, Economy, Patrimony etc.).

For those reasons, ELECTRE methods literature review is presented below. They are grouped by problem type.

## ✓ Choice

**ELECTRE I:**

Adapted to choice problem, ELECTRE I method can identify subset of action offering best possible compromises by defining real-criteria [64]. It consists in partitioning the set of actions  $A$  into two complementary subsets  $N$  and  $A / N$  (The complementary subset of  $N$ ). An outranking relation from the concept of concordance and discordance is defined. Thus an action  $A$  outranks action  $B$ , if the concordance and non discordance tests are verified.  $N$  is the kernel of the graph obtained by the outranking relation [62].

$$a_k \in A/N \Rightarrow \exists a_i \in N/a_i S a_k \text{ et } a_k \in N \Rightarrow \nexists a_i \in N/a_i S a_k \quad (I-20)$$

The concordance index for each pair of action  $(a_i, a_k)$  measuring the relevance of the assertion «  $a_i$  outranks  $a_k$  » is given by:

$$C_{ik} = \frac{P^+(a_i, a_k) + P^=(a_i, a_k)}{P} \quad (I-21)$$

Where:

- $P = P^+(a_i, a_k) + P^=(a_i, a_k) + P^-(a_i, a_k)$ ;
- $P^+(a_i, a_k) = \sum P_j, j \in J^+(a_i, a_k)$ , the sum of the weight of criteria belonging to  $J^+(a_i, a_k)$ ;
- $P^-(a_i, a_k) = \sum P_j, j \in J^-(a_i, a_k)$ ;
- $P^=(a_i, a_k) = \sum P_j, j \in J^=(a_i, a_k)$ ;
- $J^+(a_i, a_k) = \{j \in F | g_j(a_i) > g_j(a_k)\}$ : the set of criteria for which the action  $a_i$  is preferred to the action  $a_k$ ;
- $J^=(a_i, a_k) = \{j \in F | g_j(a_i) = g_j(a_k)\}$  the set of criteria for which the action  $a_i$  is equivalent to the action  $a_k$ ;
- $J^-(a_i, a_k) = \{j \in F | g_j(a_i) < g_j(a_k)\}$  the set of criteria for which the action  $a_k$  is preferred to the action  $a_i$ .

The discordance index is defined by;

$$D_{ik} = \begin{cases} 0 & \text{si } J^-(a_i, a_k) = \emptyset \\ \frac{1}{\delta_j} \text{Max}[g_j(a_k) - g_j(a_i)]; j \in J^-(a_i, a_k) \end{cases} \quad (I-22)$$

Where  $\delta_j$  is the amplitude of the scale associated to the criteria  $j$  for which there is the maximum of disagreement. The discordance test is satisfied if  $D_{ik} \leq d$ .  $\hat{c}$  and  $\hat{d}$  are respectively the limits of concordance and discordance. The concordance index is generally between  $[0.5, 1 - \min(k_j)]$ .

ELECTRE I is theoretically and educationally interesting, it is also adapted to some practical situations. Indeed, in practice, a vast cloud of qualitative or quantitative elementary consequences is usually constructed and heterogeneous criteria which are associated to ordinal scales. In addition, data collected are equipped with imprecision, uncertainty and indeterminacy [70]. Furthermore this method is sensitive to concordance and discordance [64]. It should only be applied if all criteria were coded on a numerical scale with identical scales [70]. In addition, it may be that in the outranking graph there are isolated actions. These actions do not belong to the nuclei (hence to  $N$ ). This is in our opinion a limitation of these methods that do not include all possible actions.

### ***ELECTRE IS (threshold)***

This method is designed to take into account the heterogeneity of the criteria scale and the vagueness of the data by using thresholds and pseudo-criteria instead of the true criteria [70]. The concordance index for each criterion and the overall index are calculated as following:

$$C_{ik} = \frac{\sum_{j=1}^m P_j c_j(a_i, a_k)}{\sum_{j=1}^m P_j} \quad (I-23)$$

Where:

- $c_j(a_i, a_k) = 0 \Leftrightarrow p_j < g_j(a_k) - g_j(a_i)$ ;
- $c_j(a_i, a_k) = \frac{g_j(a_i) + p_j - g_j(a_k)}{p_j - q_j} \Leftrightarrow q_j < g_j(a_k) - g_j(a_i) \leq p_j$  in this case  $0 < c_j(a_i, a_k) < 1$ ;
- $c_j(a_i, a_k) = 1 \Leftrightarrow g_j(a_k) - g_j(a_i) \leq q_j$ .

The discordance indices by criteria are binary and given by:

$$d_j(a_i, a_k) = \begin{cases} 0 & \text{if } g_j(a_k) - g_j(a_i) < v_j(a_i, a_k) - q_j(a_i, a_k) \frac{1 - c_j(a_i, a_k)}{1 - c_j} \\ 1 & \text{otherwise} \end{cases} \quad (I-24)$$

The discordance index is:



$$D(a_i, a_k) = \begin{cases} 0 & \text{if } d_j(a_i, a_k) = 0 \forall j = 1, \dots, n \\ 1 & \text{otherwise} \end{cases} \quad (I-25)$$

### **ELECTRE IV**

This method overcomes the scales heterogeneity. Regardless of the types of scales, it selects the best subset of compromised by the introduction of veto thresholds. The approach is similar to that of ELECTRE I, the difference is the condition of concordance, called the condition of non-veto [70].

$$g_j(a) + v_j(g_j(a)) \geq g_j(b) \quad (I-26)$$

To validate the assertion A outranks B, it is essential that among the minority of criterion opposing this assertion, none of them vetoed [70].

### ✓ **Sorting**

### **ELECTRE TRI**

In the sorting process, categories must be defined in advance. ELECTRE TRI is the most used sorting method based on outranking relation [67]. Each reference profile  $r$  of each action A is seen as a vector function of some criteria. To determine whether an action  $A_i$  outranks the profile  $r_k$ , a parameter  $\sigma(A_i, r_k)$  measuring the strength of the statement “ $A_i$  is as good as the profile  $r_k$ ” is defined. An action  $A_i$  is preferred to a profile  $r_k$  if  $\sigma(A_i, r_k) \geq \lambda$  and  $\sigma(r_k, A_i) < \lambda$ .  $\lambda$  is the limit point to be determined.

$$A_i I r_k \Rightarrow \sigma(A_i, r_k) \geq \lambda \text{ et } \sigma(r_k, A_i) < \lambda \quad (I-27)$$

$$A_i R r_k \Rightarrow \sigma(A_i, r_k) < \lambda \text{ et } \sigma(r_k, A_i) \geq \lambda \quad (I-28)$$

Once the outranking relation is constructed, its exploitation to sort alternatives is performed through several heuristic assignment procedures. In this method, two procedures respectively optimistic and pessimistic are used. In each procedure, each action is progressively compared with profiles  $r_{q-1}, r_{q-2}, \dots$ , until the occurrence of one of these situations:

- $(A_i P r_k) \wedge (r_{k-1} P A_i) \vee (A_i I r_{k-1})$ ;
- $(A_i P r_k) \wedge (A_i R r_{k-1}) \wedge (A_i R r_{k-2}) \wedge \dots \wedge (A_i R r_{k-l}) \wedge r_{k-l-1} P A_i$ ;

$K$  is the dimension of  $r$ . In the first case, both optimistic and pessimistic methods affect  $A_i$  to the group  $C_k$ . In the second case, the pessimistic procedure assigns  $A_i$  to  $C_k$  while the optimistic procedure assigns  $C_k$  to  $C_{k-l}$ .

---

 ✓ **Ranking**


---

**ELECTRE II**

This method arises from the ranking problem  $\gamma$ . The aim is to rank potential actions from the better to the worse by allowing tie [62]. The set  $A$  is provided with a structure and total pre order. This method is interesting from historical and pedagogical perspectives [70]. There are two outranking relations, strong and weak. This results in two outranking graphs whose exploitation is used for action classification.

The concordance index is defined the same way as in ELECTRE I:

$$C_{ik} = \frac{P^+(a_i, a_k) + P^-(a_i, a_k)}{P} \quad (I-29)$$

Three thresholds  $c$  instead of one are defined:  $c^+$ ,  $c^0$ ,  $c^-$  which correspond to the satisfaction of the test with certainty.

The concordance test is accepted if:

$$\left. \begin{array}{l} C_{ik} \geq c^+ \\ \text{ou} \\ C_{ik} \geq c^0 \\ \text{ou} \\ C_{ik} \geq c^- \end{array} \right\} \text{et } \frac{P^+(a_i, a_k)}{P^-(a_i, a_k)} \geq 1 \quad (I-30)$$

There are two discordance thresholds  $D_1$  and  $D_2$ . The discordance threshold can be resumed for  $j \in J^-(a_i, a_k)$  as following:

- If  $g_j(a_k) - g_j(a_i) \leq D_{2(j)}$  then there is a high uncertainty that the criterion  $j$  does not presents a major opposition to the outranking hypothesis;
- If  $D_{2(j)} < g_j(a_k) - g_j(a_i) \leq D_{1(j)}$  then there is a low certainty that the criterion  $j$  does not presents a major opposition to the outranking hypothesis.

The discordance index is:

$$D_{ik} = \begin{cases} 0 & \text{si } j \notin J^-(a_i, a_k) \\ [g_j(a_k) - g_j(a_i)] & \text{si } j \in J^-(a_i, a_k) \end{cases} \quad (I-31)$$

High and low outranking relation conditions are:

- $a_i S_F a_k$ :

$$g_j(a_k) - g_j(a_i) \leq D_{1(j)} \forall j \in F, \quad \left. \begin{array}{l} C_{ik} \geq c^+ \text{ et} \\ \frac{P^+(a_i, a_k)}{P^-(a_i, a_k)} \geq 1 \end{array} \right\} \text{ and /or } \left\{ \begin{array}{l} C_{ik} \geq c^0 \text{ and} \\ g_j(a_k) - g_j(a_i) \leq D_{2(j)} \forall j \in F, \text{ or} \\ \frac{P^+(a_i, a_k)}{P^-(a_i, a_k)} \geq 1 \end{array} \right.$$

- $a_i S_f a_k$ :

$$\left. \begin{array}{l} C_{ik} \geq c^- \text{ et} \\ g_j(a_k) - g_j(a_i) \leq D_{1(j)} \forall j \in F, \text{ and} \\ \frac{P^+(a_i, a_k)}{P^-(a_i, a_k)} \geq 1 \end{array} \right\}$$

This results in two outranking graphs to be exploited by an outranking algorithm.

### ELECTRE III

This method was designed to accommodate imprecise, inaccurate and unreliable data. It improves the method ELECTRE II, by the introduction of pseudo-criteria instead of the true criteria [70], [62]. A true criterion is a function criterion as such:

$$g(a) = g(a') \Rightarrow \begin{cases} a' I a \text{ if } g(a') = g(a) \\ a' P a \text{ if } g(a') > g(a) \end{cases} \quad (I-32)$$

The method introduced three so-called thresholds of indifference, strict preference and veto.

$$q_j < p_j < v_j \quad (I-33)$$

The thresholds p and q can be constant or defined according to situation.

A pseudo criterion is a function criterion to such as:

$$\frac{q_g[g(a)] - q_g[g(b)]}{g(a) - g(b)} \geq -1 \text{ and } \frac{p_g[g(a)] - p_g[g(b)]}{g(a) - g(b)} \geq -1 \quad (I-34)$$

$\forall a, a' \in A$ :

$$g(a') \geq g(a) \Rightarrow \begin{cases} a' I_g a \text{ if } g(a') - g(a) \leq q_g[g(a)] \\ a' Q_g a \text{ if } q_g[g(a)] < g(a') - g(a) < p_g[g(a)] \\ a' P_g a \text{ if } p_g[g(a)] < g(a') - g(a) \end{cases} \quad (I-35)$$

In terms of index, ELECTRE III uses two indices for concordance: the concordance index for each criterion and the overall concordance index. The concordance index by criteria stated how action is as good as another under this criterion. The discordance is expressed through the veto threshold. The veto threshold for criterion

$j$ , denoted  $v_j$  is the value of the difference  $g_j(a_k) - g_j(a_i)$  from which it appears prudent to deny any credibility of outranking of the action  $a_k$  by action the  $a_i$ , even if all criteria are consistent with this outranking.

### ***ELECTRE IV***

ELECTRE IV also addresses issues  $\gamma$ . It is often difficult to define relative importance criteria coefficients. This is due to the fact that in many situations, we are not able to determine these coefficients. With this method, we do not need the weights of the criteria.

Outranking assumptions, concordance and discordance are then abandoned. The method uses pseudo-criteria. The operating procedure is the same as in ELECTRE III. It is also based on five outranking relations [70].

## CONCLUSION

Natural disasters' analysis is investigated by many sciences. Some of them take interest in their causes when others focus on their consequences. Very often, consequences are assimilated to damages and prejudices that could affect population. At this level, there are immediate consequences which are estimable after the disaster; and indirect ones which are more difficult to assess. There are some models more or less efficient to determine economic consequences. Engineering sciences priorities have been logically oriented towards building construction techniques and disaster occurrence prevision. Among this category, some authors finally are interested by indirect effect to population. In recent years studies have addressed the concept of network and infrastructure as a direct component of people vulnerability. Our position is situated in this last category. In this category, researches are driven by local authorities in risk areas, resulted in maps, zoning and regulations for constructions.

The aims of this chapter were to make a literature review about the infrastructure network in the context of natural disaster. We have read the essential references in this area. The review is made through two axes:

- Vulnerability model: on this we find out that must of the authors are fused on the network structural parameters. We then aim to include flow circulation and the interdependences among networks;
- Decision aiding: We have determined the group of method that suit the context of this thesis.

On another level, the main challenge was to reconcile the different points of view on the concept of vulnerability. We were able to propose a vulnerability definition on the basis of this literature review. We determined the decision process that best suited the context of the thesis. We also analysed the aggregation methods. This analysis will enable us to propose the best suited in each crisis phase.

# CHAPTER II

# MODELLING

## **Résumé en Français**

Ce chapitre présente les modèles de réseau et de vulnérabilité que nous proposons. Nous commençons par confronter la notion d'infrastructure critique à celle de système complexe. Les composants du système final, justifiant cette complexité sont présentées. Nous introduisons ainsi les notions de Territoire, d'Enjeu, de Flux, d'Environnement Externe, d'Évènement Redouté, et de Facteurs d'aggravation ou d'Atténuation. Les modalités d'interaction de ces éléments et leurs paramètres pertinents dans le contexte de cette thèse sont décrits. Pour être compatible avec la théorie des graphes, une approche de modélisation des interdépendances est proposée. Les relations sont regroupées en deux classes. Dépendance pour la partie fonctionnelle et Influence pour la partie dysfonctionnelle. Ces relations sont modélisées pour toutes les combinaisons des composants du réseau. Du point de vue modèle, les réseaux sont composés d'arêtes et de sommets. Nous introduirons alors des composants virtuels pour rester conforme à la théorie des graphes. Les sommets réels sont divisés en plusieurs catégories en fonction du traitement effectué sur les flux. Les concepts de vulnérabilité et de risque sont alors ré-analysés. Cette analyse conduira à distinguer deux composants de la vulnérabilité : La robustesse et la résilience. Les formulations de ces éléments sont proposées.

“All models are wrong, but some are useful”

Box, 1979

## INTRODUCTION

As seen in the previous chapter, there are several vulnerability models in the literature. Most of these models are based on the network structure and disregard the flow circulation and the existence of interdependences. The objective of this chapter is to offer models that overcome these shortcomings.

We begin by confronting notion of critical infrastructure to that of complex system. The components of the final system, justifying this complexity are presented. Thus, we introduce the concepts of Territory, Stake, Flow, External Environment, Feared Event, and Aggravating or Mitigating Factor. Detailed interaction rules between these elements and their relevant parameters in the context of this thesis are described. To be compatible with the graph theory, an interdependence modelling approach is proposed. Relationships are grouped into two classes. Dependence is related to the functional part and Influence is related to the dysfunctional part. These relationships are modelled for all combinations of the network components. From a model perspective, network is a graph composed of edges and nodes. We will then introduce virtual components to remain consistent with the graph theory. The real nodes are divided into several categories depending on the processing performed on flow. The concepts of vulnerability and risk are then analysed. This analysis will lead to distinguish two components of vulnerability: the robustness and the resilience. The formulations of these elements are proposed.

## I.3: VULNERABLE SYSTEM REPRESENTATION

### II.1.1 COMPLEX SYSTEM

The term System commonly refers to complex entity treated (with respect to certain purposes) as a whole. It consists of elements and relationships between them, and defined according to the place they occupy in the totality [52]. Regarding system definitions in the literature, there are two schools of thoughts. The first one represents systems regarding their constitutions (structure). The second one defines them according to the provided services (dynamic and function). With respect to the first standpoint, a system is either a finite number of elements in relationship, forming a whole [71], or a set of interactive and interconnected elements [72], [73]. For the second point of view, a system is defined as a coherent set of elements or processes sharing objectives, responsibilities or common missions [17]. Each group disregards the aspects presented by the other group. Under these circumstances, we decided to propose a more generic definition.

The notions of, complexity concept is found in several scientific and philosophical disciplines. But historically complexity was more a philosophical than a scientific topic. [74] examines historical processes that have made of complexity for a scientific problem. The author supports the thesis of the progressive recognition of complexity in science. According to this theory, complexity can be seen as a process having evolved through three major steps since the 17th century: detection, recognition and reflection.



- *Detection*: From the 17th to the 19th century, this stage is denial and invisibility of the complexity in scientific paradigm. It is based on the paradigm of simplification. Knowledge is necessary based on reduction and disjunction (separate and isolate). This is the case in the mechanical models and Newtonian physics;
- *Recognition*: From the 19th to the 20th century it is the partial recognition of complexity. The complexity is then disorganized. For instance in statistical models and Thermodynamic;
- *Reflection*: The explicit complexity as described by Warren Weaver, appears in the middle of the 20th century (Systemic Models and Complex Systems). Complexity is seen then as a scientific object explicitly and systematically investigated.

Through these steps, complexity referred to several attributes (Emergence, Uncertainty, Chaos, Contradiction, Hazard, Temporality, Interaction, Inseparability, Inter definition, High Organization, etc.). These attributes are found in many modern scientific disciplines. Like cybernetic, general system theory, information theory, catastrophe theory, theory of complex systems etc.

The term infrastructure will be adopted in this thesis to characterize a system based on a network. With regard to infrastructure network, the complexity is justified by the high number of integrated technologies, system states, state variables and sensitivity to risk [75]. Moreover, infrastructures consists of large numbers of elements and relationships, with nonlinear interactions, time delays and unintended feedback loops that can lead to unpredictable behaviour [71]. From these attributes infrastructure network can be then considered as a complex system.

In another perspective, despite the number of component, complexity could be a view of an actor relative to the objective. For instance a mobile phone can be simple in use, but complex in its components integration. This same phone will not have the same complexity for its architect and a student in electronic. A complex system at a given time for an analyst is defined in this thesis as a system composed of several entities, from different nature, whose functional dynamics differs from that of its constituents.

This discussion brings us to the question “is every complex system a critical system”. The next definition tries to answer that question.

### II.1.2 CRITICAL SYSTEM

Components do not generate the same consequences in terms of failure. Their criticality depends on the fraction of provided service. [76] states that critical components are components whose failure could cause large negative consequences that affect system ability in providing allocated services [76]. This definition is not relevant in the context of interdependence. In such context, a minor component failure might have large negative consequences.

A critical system has been defined with respect to the risk incurred by stakes. Similarly we define a critical component in relationship to critical system vulnerability:

**Definition II-1 : Critical component is a component whose failure puts the constitutive system in an undesired vulnerability state.**

The concepts of vulnerability and its assessment will be presented in the section I.5.:

### II.1.2.1 CRITICITY CONCEPT APPLIED TO INFRASTRUCTURE

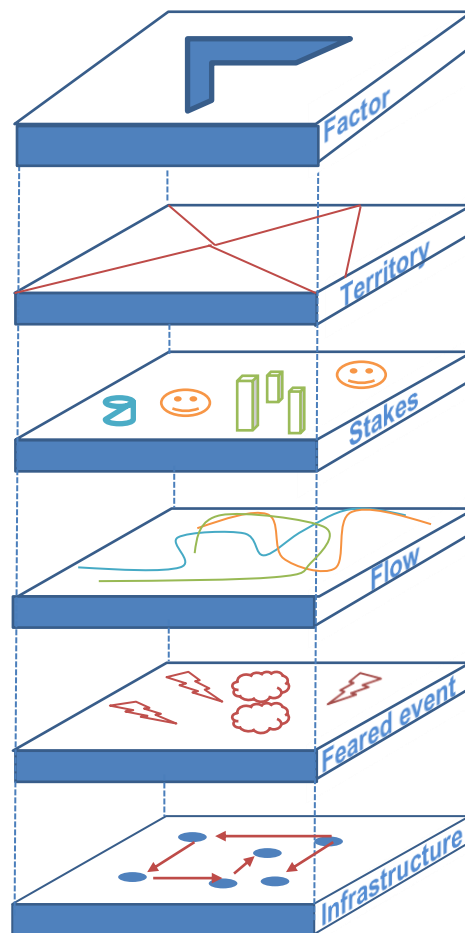


Figure II-1: Global System overview

Infrastructure network is named critical infrastructures, lifeline systems [77], systems-of-systems [77], critical infrastructure systems [78], critical system, complex system, technical infrastructure, socio-technical system, complex system, vital infrastructure, large-scale system, system of systems [23], super-system, technological networks [79] etc.

Whatever the term used, their failure analysis involves many other entities which can be seen as interconnected systems or system of systems. We face then a systemic organization described by [80] as constituted of three sub-systems: operation system, information system, and control system. This subdivision is a low level one. In a high level, the global system is constituted of 5 sub-systems: Territory including

aggravation and mitigation factors, Stake, Flow, the Environment which is mostly made up by Feared Event and the Infrastructure network itself. These systems are presented in the Figure II-1. In the context of this thesis, these systems are divided into four views: structural, functional, organizational, and external. Each view contains some elements of the global system. They are broken down as following:

- Organisation: Territory, Stake;
- Function: Flow;
- Exterior: Feared event, Environment;
- Structure: Infrastructure network.

Consequently, in this thesis, a system will be defined as a set of interconnected entities facilitating flow circulation, in order to fulfil specified functions. The interaction between the subsystems shown in Figure II-1 will induce a certain vulnerability whose scope may be greater or less. Any analysis should then go through a modelling of all entities involved.

The term critical system is used in the literature to refer to a set of interrelated elements integrating management and control processes [17]. A system criticality depends on its geographic, political-economic, and administrative context. Then criticality is justified from a societal perspective by the system in large size and high complexity [81]. We can conclude then that complexity is one of the criticality sources. Little (2003) defined critical systems as entities whose failure or destruction can have debilitating impact on defense or nation's economic security [82].

Unlike system, infrastructure connotes civil engineering, reminiscent structures and buildings [17]. Societies proper functioning relies on infrastructure services. Without water, electricity, gas or roads a modern city could not survive. Infrastructure has several meanings. The definition provided by [83] is adopted in this thesis.

***Definition II-2: Infrastructure is a network of independent, mostly privately-owned, man-made systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services [83].***

This definition underlines the fact that the term infrastructure is related to the flows functioning between components.

*In that way, network such as power grid, telecommunications and gas system can be viewed as Infrastructure.*

This view is enhanced by [84] who define infrastructure systems as “a collection of nodes and arcs with material flowing from node to node along paths in the network.

Some infrastructure might be more critical than other. An infrastructure becomes critical when it provides some service without which society or the economy cannot engage in normal operations [79]. Critical

infrastructure are defined as those that provides life-essential services such as : shelter, food, water, sanitation, evacuation and transportation and access to financial resources [19].

They must be considered – to different degrees – as complex interconnected systems embedded in a rapidly changing environment.

As a consequence, the systems may be operating closer to their limits [79]. Another definition is provided by [84]. The authors define critical infrastructure as “infrastructure that are so vital that their incapacitation or destruction would have a debilitating impact on defense or economic security” [84]. From this point of view, every system might be critical. Indeed, because of the interdependence, each system failure can impact on the economic security if any action is taken. The fact that no society can live without these infrastructures justifies the term critical related to their designation. Theses definitions seem too general in our sense. That is why we provide the following definition:

***Definition II-3: A critical system is a system whose disruption leads to unacceptable risk for territories and stakes under consideration.***

*From this point of view, networks, such as power grid, water, telecommunication, gas systems, and roads can be considered as critical system.*

Critical systems are composed of elements considered as individual entities called components [72]. Definitions of these elements are given bellow.

### II.1.2.2 COMPONENTS OF A CRITICAL INFRASTRUCTURE SYSTEM

Many terms are used to make reference to infrastructure network. Numerous concepts are difficult to differentiate. In this section we provide an accurate view on the components of a critical infrastructure system.

#### ✓ *Territory*

Vulnerability analysis is performed by local authority related to a geographic area named the territory. The territory is a portion of geographical space that coincides with the spatial extension of a government’s jurisdiction [85]. It is the component that will mitigate or aggravate the feared event effect on the population.

*City like Paris or Conakry will be considered as territory.*

We have chosen to distinguish the territory from the population insomuch as there are some populations that have no stable territory<sup>1</sup>. It structures space as the localization of actions; a short of spatial framework of

<sup>1</sup> This is true of some nomadic peoples. Otherwise territory can be uninhabited

every activity [86]. From these points of view, we define territory as a geographic zone administratively independent, supporting infrastructure networks. It might be a municipality, a city, a country etc.

Many territories might be provided by a single network. Moreover one territory generally hosts many networks. Furthermore decisions taken by one of them might be different even contradictory to others. For this reason, they are separated from each other. Every territory is integrated in the system model. Territory is characterized by its limits, decision makers, set of actions, feared events and stretch. The stretch is the surface area.

Infrastructure network provides flows to some entities whose preservation is essential for the territory. Such entity named stake is presented in the next section.

### ✓ **Stakes**

---

The stake is a material or immaterial entities consuming flow and providing a function whose deterioration is damageable or prejudicial for the society. It is assimilated to Societal Critical Function in [87].

*For instance the stake can be a firm, a habitation, a government institution etc.*

The population is the group of people living in a given territory or likely to be affected by a feared event. It is the central element of our model and is divided into three dependent factors: psychological (stress, fear); physiological (age, sex, health), economical (healthiness or poverty).

Feared event, factor, and flow are susceptible to affect stakes in their stench. The action is on one of stake attributes.

*For instance an earthquake could change the mean time to the repair of one stake.*

Another possibility would be that stake resistance is superior to the feared event amplitude. It will then resist to the feared event. Affected stakes might lead to many consequences: Human, national security, environment, economy, cultural heritage, legislation, politics, education, comfort.

Energy, matter, and information travel in the network through flow presented in the next section.

### ✓ **Flow**

---

Flow represents matter, energy and information circulating from sources to target nodes. Its circulation aptitude in network is a vulnerability indicator [88]. In this thesis flow is separated from the infrastructure itself and supposed to be discrete. This distinction is made because of that feared event might affect one without the others. It circulates at a nominal speed according to a circulation law. In this model the flow may fail and recover its good working state after a mean time to recover.

The failure of a flow may affect other components (factor, stake, feared event, etc.).

15 types of flow have been identified in this thesis: Human, Electricity, Drinking water, Sewage, Information, Good, Gas, Car, Truck, Boat, Train, Hydro carbide, Waste, Plane and Money.

Every type is endowed with some particular parameters. For example for the drinking water physic-chemical parameters are taken into account. Flow has also a resistance against feared events and factors.

Network functioning is governed by the external environment presented in the next section.

### ✓ *External environment*

---

So far only the component effects on each other have been considered; nevertheless, the functioning of a component can also be altered by the operating environment. Environment effect is taken into account through component weight. The weight might be geodesic distance between nodes, or any relevant criteria for the analysis (cost, time). For the weight assessment, analyst determines the study context including:

- Method: Detection Systems, Software;
- Material: Emergency devices;
- Methods: Maintenance process, norms and regulations;
- Environment: Temperature, electromagnetic pulse, soil and subsoil;
- Workforce: Operators, analysts, decision makers;
- Moment: season, time.

We argue that weights are time-dependent functions. For instance, in French power grid distribution, the cost depends on the period (less expensive in the nights) and the weather conditions (rain, snow, sun...). Edges weight obtained by environment parameters aggregation is out of the scope of this thesis. Edge weight determines the flows circulation. Because of that, environment affects the resulting robustness and reliance. Above systems are affected by feared event. Feared occurrence processes are presented in the next section.

### ✓ *Feared event*

---

Vulnerability analysis is performed against specified feared events. The analysis assumes the presence of anthropic or natural phenomena which is not under control. In the literature feared event is called Incident, Hazard [89], [21], disturbance, threat [78], elementary event, initiating events, perturbation [14], strain, danger, accident, uncertainty [43].

- Accident is a disruptive element that can change a system state [17] or chain of unintentional and fortuitous events causing damage. Incident is an event , which directly can result in considerable reduction or interruptions in the serviceability of a link/route/road network [21];
- According to the French Institute of Cyndinique, danger is the system tendency to generate one or

more accidents;

- Hazard is defined as “a generic class grouping a set of potential causes as well as causes’ generators” [90]. It is a natural or anthropic phenomenon, harmful to the human being, whose consequences appear because of the fact that safety measures have been exceeded [15]. Hazard is normally used for strains on a system stemming from non-man-made sources such as earthquakes, severe weather conditions or tsunami [19]. But in this thesis the concept is generalized to the others feared events;

The term feared event will be adopted in this thesis. The adopted definition is given in the following.

***Definition II-4 : Feared event is a natural or anthropic phenomenon for which it’s not possible to predict together the occurrence and the intensity, and susceptible to affect stake [91].***

*Thus, a feared event may be natural, climatic, technical, human, an act of sabotage, terrorism or war [14]. In the nature, there are mainly seven types of natural feared event that may affect the networks: earthquakes, earthquakes, volcanoes, tsunamis, fires, cyclones, and storms.*

Feared event is characterized by the fact that it has a negative influence on the network functioning [89]. They are dependent. An earthquake can cause a tsunami or fire. In our model, feared event occurs with a frequency and amplitude. Its occurrence point is situated on the territory. From its occurrence time, the feared event will spread out on its stench according to a speed and a propagation mode. It will last for a given time. Component for which the resistance to the feared event type is below the amplitude will break down. The specificity of Feared event is that we cannot predict its occurrence date and its intensity at the same time. From this perspective, a predicted snowstorm with a determined intensity could not be considered as a Feared Event. On the other hand, if for some reason, this intensity cannot be approximated with an acceptable leeway, the snowstorm becomes in this case a feared event.

It should be noted that a phenomenon which does not affect any stake could not be considered as a feared event. For instance, an earthquake in an inhabited area without infrastructure will not be a feared event whatever its frequency and its intensity are. Other parameters than frequencies and intensities are to be taken into account in the feared event analysis like failure mode, number and detectability of heralds signs. In this thesis feared events are represented by natural disasters, system elements failure (node, edge, flow, and factor).

When affected by the feared event, the component will change state. According to [19], a vulnerable system goes from a planned state to an unwanted state. The authors show that for a system of  $n$  components having  $k$  faulty elements, the number of possible state of the system is a combination of these  $n$  elements taken  $k$  by  $k$ :  $C_n^k$ .

*For a network with a size of 800 with three faulty components, the number of states is nearly 85 million.*

A system is then characterized by several states. System state is a particular combination of its component states [73]. Considering different states of the system represents one of the difficulties in vulnerability analysis which is the exploration of these states for consequence estimation.

There are many approaches to assess the system state. Stochastic models like Markov or Poisson processes can be used to predict the behaviour of system in uncertain environment. But these methods lack the capability to completely capture the underlying structure of the system and the ability to adapt to failures of subsystems when strong interdependencies exist [23]. In this thesis, to predict system behaviour, a simulation is performed to obtain the system final state. One element could fail in various ways. Any flow will pass through a failing element. In the following, the element failure modes are presented.

- *Failure by unreliability:* One component characterized by reliability different from 1 could fail during the simulation. The component will recover its working state after its mean time to repair;
- *Failure by flow:* Another failure mode is given by flow congestion. A component will break down if its capacity in one flow overpasses flow quantity. Electricity overload well describes such situation. In particular, flow consuming component will fail if its consumption is more than the available flows;
- *Failure by influence:* At least, a component will break down if it is linked to another failing component by an influence.
- *Failure by feared event, factor or flow effect:* At the feared event occurrence, it will affect all components in its stench. Those for whom the resistance is under the feared event amplitude would fail. Otherwise factor can aggravate or mitigate feared event effects. In this thesis a feared event is characterized mainly by its occurrence probability and its amplitude. Three principal ways are presented by [14] to assess a feared occurrence probability: Statistical analysis of empirical disturbance (accident) data, Mathematical modelling combined with empirical component data, Expert judgments. We preconize to use vulnerability maps instead of expert judgement. In most cases, territories have vulnerability maps. On these maps feared event likelihood is distinguished by a colour. In such situation, each colour corresponds to a probability and amplitude. These elements could be used in the vulnerability analysis. The analysis will consist in this case to take into account high probability area and to make analysis for these areas.

The main element of our model is the infrastructure network itself. Its modelling is presented in the next.



**I.4: NETWORK MODELLING**

**II.1.3 NETWORK DEFINITION**

Societies' well-functioning relies on many aspects. Political stability and good finance seem obvious. On a technical aspect, the infrastructure provides citizen with goods and services. Among these infrastructures, networks such as power grid, telecommunication and gas systems occupy a prominent place. The definition provided by the American Critical Foundation [22] underlines that infrastructure is a set of interconnected components providing goods and services for society's well-functioning. Infrastructure is the physical support for flow circulation. It is the main element in the system of systems overview. Its failure could lead to stake, territory or flow vulnerabilities.

		<i>Flow</i>		
		Mater	Energy	Information
Structure	Artificial	Motorway network, Railway network, Drinking water system, Waste water system	Power grid, Gas network,	Computer network
	Hybrid	Aviation system, Shipping		Telecommunication system

*Table II-1: Network classification*

The main issue in most territorial vulnerability analysis is the infrastructure network identification. Indeed, critical system for one stake is not necessarily critical for another one. In a report from the American Critical Foundation, it listed nine critical infrastructures: Transportation; Oil and Gas Production and Storage; Water; Emergency Services; Government Services; Banking and Finance; Electrical Power; and Telecommunications [22]. In a comprehensive way, we have classified infrastructure network according to the flow circulation and the physical structure. The structure is either artificial or hybrid. Artificial ones are totally man made. On the contrary, hybrid structure includes natural entity like shipping. Fully natural structures are not considered in our point of view as infrastructure network.

According to Figure II-1, infrastructure networks can be classified into the following classes:

- Material artificial network;
- Material hybrid network;
- Energy network;

- Information artificial network;
- Information hybrid network;
- Second level network: Second level network is the other network based on the previous. In this category figure Hydro Carbide, Hospital, Nuclear Biological Chemical (NBC), Food, Audio Visual, Post, Bank and Finance. These networks rely on and use the previous ones.

*For instance a hospital network will use road and air for transportation, drinking water and sewage.*

The above list shows that infrastructure is mostly man made, but can be natural in some situation (air and shipping). Conducting an analysis for all systems is not feasible in real situations, because of budget and time reasons. The first difficulty faced by decision makers will then be the identification of the appropriate systems for the analysis. Due to the high relationship with other networks, power grid appears to be the most critical system [92]. But, others systems such as water, telecommunication, transport can be added [17],[92].

Another alternative in network identification consists in relying on current regulations. Recommendations are done by some institutions like the International Risk Governance Council (IRGC) which recognizes five strategic networks (electricity, gas, water, rail transport, and internet). For the European Union, a critical infrastructure is defined as “those assets or parts thereof which are essential for the maintenance of critical societal functions, including the supply chain, health, safety, security, economic or social well-being of people”. Based on this definition, it classifies infrastructure by sector shown Table II-2.

<b>Sector</b>	<b>Sub-sector</b>	
Energy	Electricity	Infrastructure and facilities for the production and transmission, with respect to electricity supply
	Petrol	Oil production, refining, processing, storage and distribution by pipelines
	Gas	Gas production, refining, processing, storage and distribution by pipeline LNG terminals
Transport	Road	
	Rail	
	Air	
	Inland navigation	
	Deep sea and short sea shipping and ports	

*Table II-2: Critical networks according to European Union, 2004*

In the absence of explicit regulation, selection and prioritization of critical systems can be done by a multi-criteria approach. This approach might be based on decision maker’s objectives.

Infrastructure modelling is then a challenging task. To achieve this goal, the approach adopted in this thesis is presented in the next section.

## II.1.4 NETWORK REPRESENTATION FEATURES

### II.1.4.1 MODELLING RULES

Graph theory modelling is mainly chosen for infrastructure modelling. We decided to adopt this theory since it allows the representation of the majority of communication and transportation systems [79].

A finite graph  $G = (V, E)$  is defined by a finite set of nodes  $= \{V_1, V_2 \dots V_N\}$ ; ( $|V| = N$ ) and a finite set of edges  $E = \{E_1, E_2 \dots E_M\}$ ; ( $|E|=M$ ).

*For example in the railway transportation, nodes are stations and edges are rails.*

The literature review allowed us to identify some shortcomings.

As far as we are concerned we argue that:

- Graphs should be oriented and weighted. The weight may be a loss (voltage drop), cost, or any other relevant criteria for the analysis;
- There are several flows for each component. These flows can be information, service, energy, and goods. They transit from source nodes to target nodes;
- Flows dynamic is determined by a circulation law;
- Different types of nodes exist. They depend on the function performed in the network.

✓ *Edges are direction*

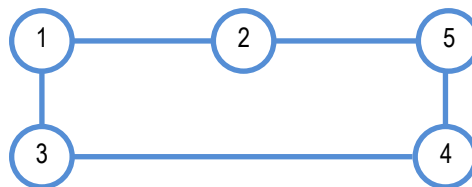


Figure II-2: Undirected network

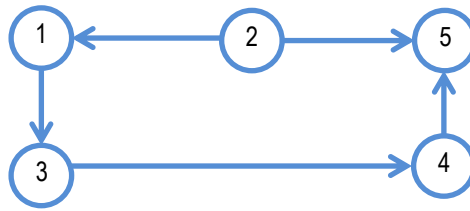


Figure II-3: Directed network

Not taking into account the edges orientation could screw the results of vulnerability analysis. In order to demonstrate that, let's consider two unweighted graphs shown in Figure II-2 and Figure II-3.

In Figure II-2, the edges are not directed; the distance between nodes (1) and (5) is 2 units. On the contrary in Figure II-3, edges are directed bringing this same distance to 3 units. Because of edge orientation, it is no longer possible to go from (1) to 5 through (2). Oriented graphs are found in many technological networks.

*This is the case of roads where highways are oriented as well as in power grid where power is transmitted from sources to targets.*

A modification of the distance has significant consequences on the network structural parameters.

#### ✓ Edge weight

Related to infrastructure networks, edges are often weighted. The weight could be a length, cost, impedance etc. To show the importance of weight, let us consider the Figure II-2. As in the previous example, the distance between vertices (1) and (5) through (2) is two units. And the distance between these same two nodes through (3) and (4) is three units. If we assign weights to the edges as in the Figure II-4, these distances become 11 and 7 respectively. The second path is then the shortest. The shortest path between two vertices is closely related to the weight of the edges and not taking it into account can affect the structural parameters of vulnerability. In our point of view, the weight must reflect at least the geodesic distance, time and cost.

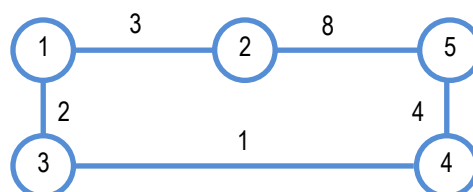


Figure II-4: Weighted graph

---

 ✓ *The node type*


---

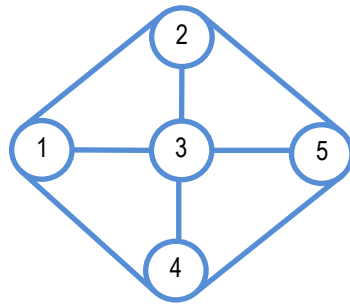


Figure II-5: Network of same type of node

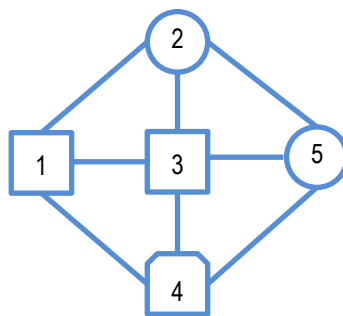


Figure II-6: Network with different types of node

Network is composed of edges and nodes considered as its elementary entity [73]. In the modelling techniques, there are several types of components. [24] pointed out in-feed nodes, supply nodes, and source nodes. For [14] they are called generation, delivery systems and users.

By analysing the above two networks (Figure II-6 and Figure II-5), one can say about the graph shown in Figure II-5, that node (3) is the most important in term of flow circulation because of its central position. On the contrary in the Figure II-6, node (3) is used as a transporting node; nodes (2) and (5) are the destination nodes, and (4) is a production node. This differentiation is performed through their shapes in Figure II-6. In this configuration node (4) will be the most important. By removing it in the network, flow will not circulate unlike in the first case. The network structure is less affected by removing (4) than (3), but the function is much more dependent on (4) than (3).

To tackle this problem and those cited above, we argue that nodes must represent a Source, a Treatment, a Target, or a Relay. This classification is based on the flow dynamic. The component type is determined for every flow. So a component might be source for one flow and treatment for another.

- *Source*: A source component produces flow. For such component, the flow output quantity is superior to the same nature of input quantity.

*For example a nuclear power plant is a source for electricity flow.*

- *Treatment*: A Component treats a flow, whether by internal processes, it changes the qualitative attributes of this one.

*For example, a sewage treatment station is a treatment component in sewage network.*

- *Target*: A component is a target for a flow if for this one its output quantity is inferior to its input quantity. These nodes are those supply flows to relevant stakes.

*For instance they may be the last switching station or a water tower.*

- *Relay*: A node relays a flow if this one is only passing it. In such a situation, there is no production, no treatment, and no consumption. This is the case of subway stations. If it comes to edges, this function means transport.

Considering the assumptions presented in this paragraph, any infrastructure can be modelled by a set of these four nodes and weighted edges. Network components are characterized by their reliability, the mean time to repair, a resistance against feared events, flows, and factors. There are other parameters like the testability not relevant in the context of this thesis. A component can carry many types of flow. According to its type, it would be endowed with a treatment coefficient for a flow. These parameters come from specialized database or from network manager. Reliability might include many local parameters: corrosion, sub component qualities etc.

Interdependence might exist inside infrastructures. Cascading failure could result from interdependence occurrence. In the next section, we present interdependence modelling technique compatible with the graph theory.

#### II.1.4.2 RELATIONSHIP TYPOLOGY

Relationship is also called interdependence, dependency, dependence, interdependency [87], interconnectedness [87]. Those terms refer to relationship between two components of same or different networks. Because of interdependence, one network failure may affect other networks. For instance in July 2012, a blackout in India affected over 620 million people. Activity of most affected areas where paralyzed.

Interdependence science are relatively immature [93]. It is defined as a bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other [94]. However, this definition does not take into account interdependence related to flow circulation. For this reason we define relationship as a process through which a component is provided in flow or affected by another component malfunction. Interdependence could be functional or representative of a constraint.

They are the main cause of performance drop [95] and feared event propagation [17]. Because of them, the analyst might be placed in a radical uncertainty or ignorance situation [96]. The main difficulty in networks

modelling is therefore to take interdependence into account. The types of interdependence uncouncted in the literature are presented in the next section. In the literature, interdependence study could be classified according to their type, their level and their visualization.

[93] describes four types of relationship: functional (or physical), geographical, cybernetic and logical.

- Physical relationship is due to flow exchange between components. For example, water system needs electricity to run properly;
- Geographic relationship is related to component proximity. It occurs when two components are geographically close, and when the failure of one may cause the failure of the other. (E.g. explosion of a gas line damaging power lines nearby);
- Cybernetic relationship comes from information transfer. This relationship can be found for instance between power grid control and monitoring systems and computer networks. Indeed, information required for monitoring must go through computer networks.
- Finally, logical relationship is related to contextual, economic, social and / or political realities [17]. It is through this mechanism that, for instance the war in Libya increased fuel prices in European countries.

In order to model relations, [84] have identified five types of relationship:

- Input: In this relationship, the output of the first system is the input of the second;
- Mutual dependence is related to two or more systems. In such relationship the output of each system is an input of the other system;
- The Co-located relationship exists for systems positioned in the same geographic area.
- Shared refers to components that have a common section of the infrastructure system;
- Exclusive-or is associated to infrastructure system sections that support only one service at a time.

Interdependence is categorized by [87] by level. The authors distinguish between direct (first order) and indirect (second order) interdependence. If, for example infrastructure  $i$  depends on infrastructure  $j$ , and infrastructure  $j$  depends on infrastructure  $k$ , there is a second order (indirect) dependency between  $i$  and  $k$ .

Another approach is presented by [78]. The authors defined a graph as  $G = \langle V, E, A \rangle$ . Where  $V$  is the set of nodes and  $E$  is the set of edges.  $A$  represents the adjacent matrix of the graph with  $a_{ij}$  equal to 1 if there is an edge joining node  $i$  to the node  $j$  and 0 otherwise. Interdependence node are then seen by the authors as weighted and this weight depends on the loads of the two nodes. To visualize and communicate interdependences to the stakeholders, “cascade diagram” is introduced by [87].

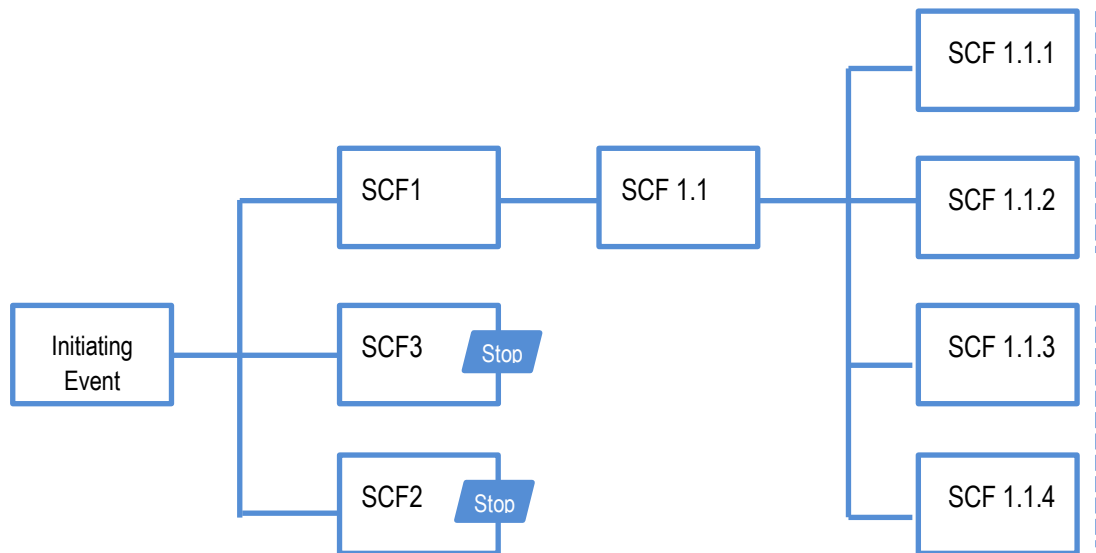


Figure II-7: Example of cascading diagram by [87]

#### ✓ Lack of interdependence modelling

Interdependences presented in the three previous sections have some shortcomings discussed in the present section. By considering [93] modelling the main lake is the confusion between logical and geographical dependence. These two relationships are similar. In both relationships, there is a state of one component that might lead to the other component malfunction.

In another word, the model presented by [84] does not consider flow direction, nor component states. Indeed a component *A* might be dependent on a component *B* without *B* being dependent on *A*. Mutual dependence seems to be two relationships Input. It is also very similar to Share relationship. Indeed, only flows direction and component number varies. Moreover two components co-located in the same geographic area, might not be interdependent. Geographic proximity does not mean absolute colocation. Shared and Exclusive-or are similar. They represent logical dependence described by [93]. In addition, [84] do not differentiate types of *Input*. Indeed, depending on the flow nature many types of the relationship *Input* might exist. In the authors' point of view, *Input* might include components of the same network. On the contrary relationships may exist only between network components carrying different flows. The model proposed by the authors does not take into account directed relationship, neither and the fact that in many realistic situations, one node can handle many flows.

Finally, diagrams proposed by [87] allow interdependence representation but not their modelling for risk or vulnerability assessment. To overcome these shortcomings, our method is presented in the next section.

#### ✓ Relationship classification

For interdependence modelling, we argue that physical, functional, and cybernetic dependences might be grouped under the name of *Dependence*. Indeed only the nature of the flows is different in these cases.



In addition, for reasons of etymology, geographic dependence is called *Influence*. In case of dependence or influence in both directions, it will be talked about interdependence or interinfluence. Dependence and Influence are specialization of *Relationship*.

From this point of view, dependence is functional and influence is dysfunctional. Relationship might exist between components of same or different subsystem.

Relationships exist between networks. These relationships are represented in the following table.

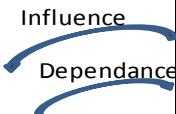
	Artificial network							Hybrid network			Second level network						
	Water flow				Energy flow		Information flow	Material Flow		Information							
	Motonway	Railway	Drinking Water	Sewage	Power grid	Gas	Computer	Aviation	Shipping	Telecommunication	Hydro Carbide	Hospital	Waste, NBC	Food	Audio-visual	Post	Bank and Finance
Motonway	Black	Orange			Orange										Orange		Orange
Railway	Red	Black			Red		Red	Orange		Orange							Orange
Drinking Water	Orange		Black	Red					Orange								
Sewage	Red		Red	Black					Orange								
Power grid	Orange				Black	Orange	Red		Red	Red	Red						Orange
Gas		Orange			Red	Black	Red			Orange	Red						Orange
Computer					Red		Black			Red							Orange
Aviation		Orange			Red	Orange	Red	Black		Red							Orange
Shipping	Orange				Orange				Black		Red						Orange
Telecommunication					Red		Red			Black							
Hydro Carbide	Red	Red			Orange		Orange		Red	Orange	Black						Orange
Hospital	Red		Orange	Red	Orange	Orange						Black					
Waste, NBC	Red	Orange	Red	Red					Red				Black		Orange		
Food	Red	Orange		Orange	Red	Orange		Orange	Orange					Black			Orange
Audio-visual					Red		Red			Red					Black		

Table II-3 : Relationship between networks

Table II-3 shows relations between networks. Relations between similar networks are not considered. High relations are represented by red arrays and low ones by orange arrays. The intensity of the relationship is traduced by the increasing grayling of the cells. The matrix is obtained by an intuitive approach based on the literature. It shows two types of relations. These relations are presented in the section II.1.4.2. The main criterion retained is the quantity of flow consumed for de relation “dependence”.

For instance railway has a strong dependence on the power grid because of the electricity consumption. But it is considered nondependent from the sewage.

## II.1.5 NETWORK MODELLING TECHNIQUES

### II.1.5.1 RELATIONSHIP REPRESENTATION

Interdependence identification is performed by the analysis. This step is a crucial one. Indeed, data are often non-existent, protected by confidentiality, or unusable. The required data consists of data relating to territories.

#### ✓ *Dependence modeling*

Any arc between two nodes materializes dependence. In general, a component  $B$  depends on a component  $A$  whether there is a flow transiting between  $A$  and  $B$ .

Dependence is represented by outgoing arrow pointing the next node in the flow direction.



*Figure II-8: Dependence relationship*

*Dependence situation can be found in the subway where stations need rails to exist. Station without incoming or outgoing communications would not have any sense.*

#### ✓ *Influence modeling*

A component  $B$  is influenced by a component  $A$  if there is at least one failure state of  $A$  causing an unacceptable failure state of  $B$ . Therefore the influence between components exists only for some states, named *influence states*. Components involved in influences are represented by a finite number of states. Among them, are at least three states: good working condition, degraded state and failure state. At the beginning, components are generally supposed to be in working conditions state.

Influence is represented by a dotted edge. Figure II-9 represents an influence edge.



*Figure II-9: Dependence relation*

Taking into account the component states and the direction of flows, all types of links can be modelled either by dependence or by influence.

*Influence could be encountered in a situation where the explosion of a water tower floods an electricity sub-station.*

### II.1.5.2 NETWORK COMPONENT CONNEXIONS

Relationships, if they exist, are between components of networks and flow. In general, there are four natures of relationship: Node-Node, Node-Edge, Edge-Node, and Edge-Edge.

Modelling techniques of these relationships are presented in the following.

#### ✓ Relationship Node -Node

Relationships between two nodes of different types can be dependence or influence. Johansson and Hassel (2010) materialize dependence between nodes by an edge. We argue that dependence edges might be oriented like other edges. So, if a node (2) is functionally dependent on a node (1), this dependence is materialized by an oriented edge starting from (1) to arrive at (2) in Figure II-10.



Figure II-10: Dependence Node-Node

*Influence may exist between nodes of the same type (explosion of a gas tank causing damage to another gas tank), or between nodes of different types (destruction of a water tower, flooding a substation). However, dependence between nodes of the same type will be represented by normal edges.*

#### ✓ Relationship Node-Edge

Relationships do not exist only between nodes. But they also exist between a node and an edge. In order to model influences and dependences between components, virtual edges and virtual nodes are introduced. Virtual component (edge or node) can carry all flows; its reliability is assumed to be 1. Every edge involved in a relationship instantiates a virtual edge. Virtual edges and nodes are represented by dotted components in Figure II-11.



Figure II-11: Virtual components

Dependence Node-Edge is illustrated in Figure II-12. For influence, the dependence edge is replaced by an influence edge.

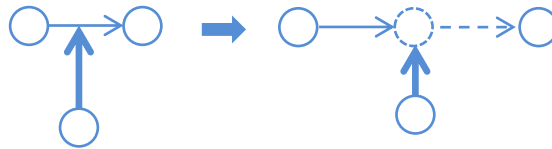


Figure II-12: Relationship Node-Edge

In some situations, a power line can be damaged by the explosion of a gas expansion station. In such situations, there is an influence from the gas station to the power line.

Relationship Node-Edge is also encountered when a node can provide flows directly to an edge.

This situation is those in sea and air transportation where tags transmit information to plane and ships.

#### ✓ Relationship Edge -Node

The relationship Edge-Node represents a direct link without an intermit node. Influence Edge-Node is represented by Figure II-13. In case of dependence, the influence node is replaced by a dependence node.

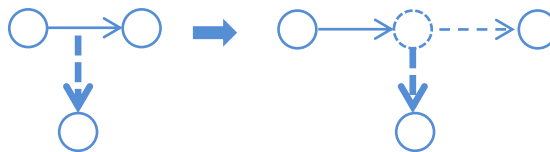


Figure II-13: Influence Node-Edge

In some real cases, a water pipeline can supply a thermal power station. In such situations, there are dependence between the pipeline and the power station.

#### ✓ Relationship Edge-Edge

The relation Edge-Edge is rare in a real situation. It represents the fact that two nodes could be linked without intermediary nodes. This kind of relationship Edge-Edge is represented in Figure II-14.

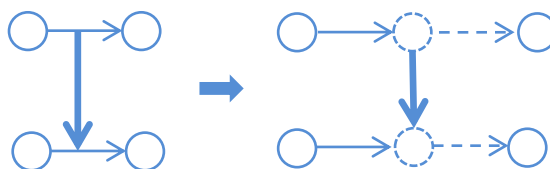


Figure II-14: Relationship Edge-Edge

Relationships between edges can be found in rail transport. Rails and electricity are closely linked to a functional point of view.

In the previous sections we have presented a modelling approach of involved entities in the networks vulnerability analysis. After determining the shortcoming of literature review on modelling by the graph theory, we presented a method including interdependences modelling. The different types of interdependence identified allow every situation modelling. Subsequently, we have determined the parameters of other systems and defined the interaction modes.

The next section presents the dynamics factors to be implemented in the system model.

### II.1.5.3 DYNAMIC FACTORS

Dynamic parameters are at the origin of the global fluctuation of the system state. Generally, all of the elements described in II.1.2.2 are dynamics due to the change in their parameters. However in terms of participation in cascading failures, flows and aggravating factors are prominent. Flow dynamic is regulated by circulation law [91]. That is why we present them in the following two sections.

#### ✓ Circulation laws

The circulation law describes the path in the physical network. We argue that each flow in network might have at least one circulation law. Law takes into account the path in the network. In the absence of explicit function, circulation law of one flow will be equitably shared among component at any time.

In the literature there are some models to determine the distribution of load of edges. [78] argues that when edge  $e_{ij}$  is damaged, the load of the broken edge will be redistributed to the neighbouring edge connecting to node  $i$  and node  $j$ . The additional load received by edge  $e_{im}$  is defined by [78]:

$$\Delta F_{im} = F_{ij} \frac{W_{im}}{\sum_{a \in \Gamma_i} W_{ia} + \sum_{b \in \Gamma_j} W_{bj}} \quad (II-1)$$

Where  $\Gamma_i$  and  $\Gamma_j$  are sets of neighbouring edges connecting to node  $i$  and node  $j$ .

$W_{ij} = (D_i \times D_j)^\theta$ ,  $\theta$  is an adjustable parameter which controls the strength of the initial load of edge.

In this thesis the circulation law is a set of ordered components:

$$LC_f = (V_1, E_1, V_2, E_2 \dots E_n, V_n) \quad (II-2)$$

$LC_f$  is the circulation law of the flow  $f$ .

#### ✓ Mitigation and aggravation factors

In the nature, some elements might mitigate or aggravate the stake consequences.

*For example a dam can mitigate vulnerability related to flood, but its failure is a source of aggravation.*

Factor is related to elements (flow, feared event, stake, network component, interdependence, another factor etc.). When a factor is activated, it will affect parameter of elements in its stench (amplitude, frequency, speed etc.).

Factors have several amplitudes related to the parameter types of elements that are susceptible to be affected. It reacts faster or slower depending on its action speed. Unlike the feared event, factor is active all the time. The action mode involves adding or subtracting factor amplitude and parameter type of the affected element.

One factor may be affected by feared event types or other factor types. For each of these elements, it can resist up to a certain threshold. For example, a dam can withstand an earthquake in a certain level. Mitigation factor can be emergency devices. Those are defined by the American Critical Foundation, as “critical infrastructure characterized by medical, police, fire, and rescue systems and personnel that are called upon when an individual or community is responding to emergencies” [22].

## **I.5: VULNERABILITY MODELLING**

There is no methodology for vulnerability analysis accepted by all. From the point of view of the American Critical Foundation, vulnerability analysis is a “Systematic examination of a critical infrastructure, the interconnected systems on which it relies, its information, or product to determine the adequacy of security measures, identify security deficiencies, evaluate security alternatives, and verify the adequacy of such measures after implementation” [22]. The methodology presented in this thesis starts by focusing on the context. It tries to answer the following questions:

- What is feared? This question is presented by some authors as "What can happen?"[18][28], [97];
- What is likely to be disrupted?
- What consequences this might have?
- What can be done?
- When can it be done?

Vulnerability analysis consists then in evaluating the system structure and function compared to a nominal state. The evaluation is made considering feared events and potential actions. The aims are to determine threats and feared events that might lead to large negative consequences.

We define the vulnerability considering three elements: The System, the Stake and the Feared Event.

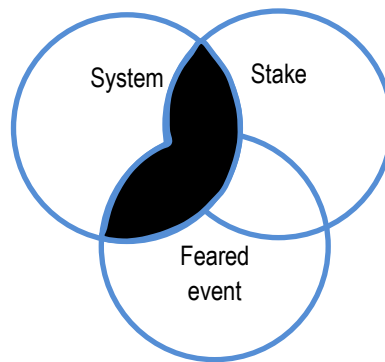


Figure II-15 Elements of vulnerability

As shown in the Figure II-15, the vulnerability is functioning of the three sets: System, Stake and Feared event.

In this thesis we are not interested in the direct effect of feared events on stakes. We will not talk about vulnerability in the case of a feared event that does not affect any stake.

### II.1.6 DIFFERENCE BETWEEN VULNERABILITY AND RISK

The concepts of vulnerability and risk are sometime confusing. The aim of this section is to explain the difference between these notions.

To distinguish concepts of vulnerability and risk, let us consider a system to be analysed (Figure II-16).

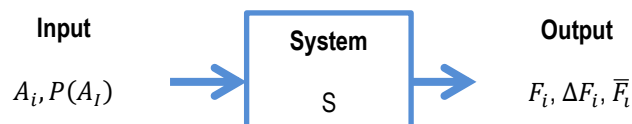


Figure II-16: Elementary system to analyse

From the two standpoints (risk and vulnerability), output may be represented by a function  $F_i$ , a difference  $\Delta F_i$ , a wrong output  $\bar{F}_i$ , or probability of one or more of these elements. The system input is described by uncertain causes ( $A_i$ ) or a probability on these causes  $P(A_i)$ .

*For instance let's consider that the analysed system is an infrastructure network like a water network. The output in such case could be the quantity of water consumed, the increase or decrease of this quantity. In other words, the difference between the provided quantity and the nominal consumption. It could be also the quality of water. The input of the system could be an earthquake or the probability of a storm.*

The risk in the point of view of [98] is an entity composed of probability ( $P(A_i)$ ) on the one hand and the consequences ( $\bar{F}_i$  or  $\Delta F_i$ ) on the other hand. [99] for its own part related probability to undesirable result

( $P(\bar{F}_i)$  or  $P(\Delta F_i)$ ). Other authors define Risk as the cumulative effects of uncertain occurrences ( $A_i$ ) adversely affecting ( $\bar{F}_i$  or  $\Delta F_i$ ) the goals ( $F_i$ ) [100], or the possibility that a fact ( $A_i$ ) having undesirable consequences ( $\bar{F}_i$ ) occurs [101]. [102] argues that Risk is defined from a set of causes ( $A_i$ ) and consequences ( $\bar{F}_i$  or  $\Delta F_i$ ) on the system [102]. [103] defines the risk as an uncertain event ( $A_i$ ) or condition ( $P(A_i)$ ) which, if it occurs, has a positive ( $F_i$ ) or negative ( $\bar{F}_i$ ) effects on a project objectives, [104]. From all these point of views, risk analysis deals with the outputs and the inputs without considering the system structure or dynamic. Only the effect of Input on Output is taken into account. The system state fluctuations are not taken into account.

*In the previous example the risk analysis will focus on the probability of having bad quality of water, or a loss of the quantity supplied. The risk could also be the effect of the earthquake on the quality or quantity of water.*

Vulnerability is also documented in many ways in the literature. As discussed in I.1.2, there are two views of vulnerability: A system-based view and the event-based view. From these two views interest is focused on the system itself (structure and function) rather than on its outputs/inputs.

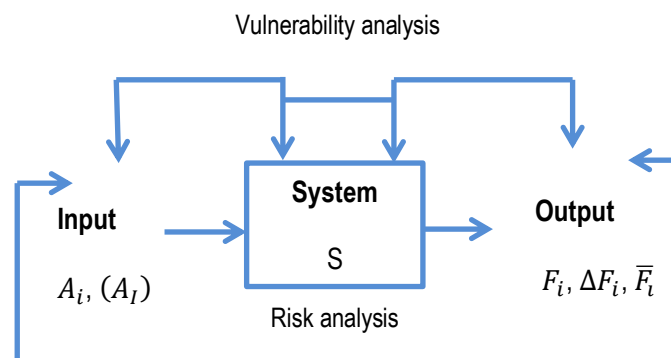


Figure II-17: Risk and vulnerability analysis

*For the water network, the vulnerability will focus on the way how the network will support the earthquake, or on how a perturbation in the network could have consequences in terms of water quality and/or quantity.*

The fundamental difference between risk and vulnerability presented by Figure II-17 is that the former focuses on the input and the output while the second concentrates on the system and its input (or on the system and its output, less frequently on the three elements). Vulnerability analysis will take into account the system state variation, contrary to the risk analysis. A framework for the vulnerability analysis is proposed in the next section.



## II.1.7 VULNERABILITY ANALYSIS FRAMEWORK

A closed loop system is proposed for vulnerability view in Figure II-18. The output is determined by decision makers and may be damage, prejudice, loses, service function (e.g. electricity consumption). Mainly, outputs are linked to stakes and might be part of the system itself, flow etc. The model input is the feared event. The system itself is broken down into network and stake. The stake is affected by feared event effects through components of infrastructure networks. The Feared event has a frequency and magnitude. It impacts on the structure and / or function of the network components. This influence is reflected by the component *S* which converts intensity and/or frequency on network parameters, (Failure rate, centrality, etc.). Through the obtained vulnerability model, damage or, a set of damage can be estimated. Likewise, network weak points can be determined and actions carried out. This task concerns decision makers which will use decision support models to inform population and define actions to be undertaken.

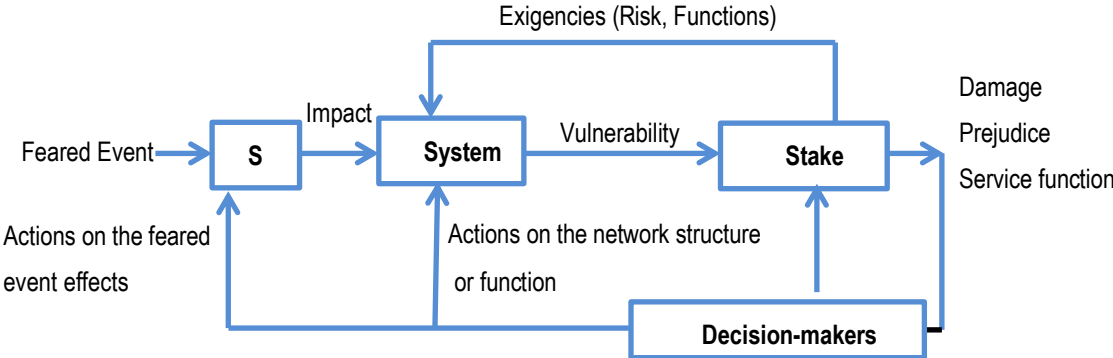


Figure II-18: Vulnerability view

The framework for vulnerability analysis is embedded in a process presented in Figure II-19. This process defines a methodology used for the developed Decision Support System. First the context identification is needed. The context is invariant of the analysis. It includes among other territories, stakes, networks, feared events, emergency devices, flows, decision levels, risk situation, decision phases, and decision makers.

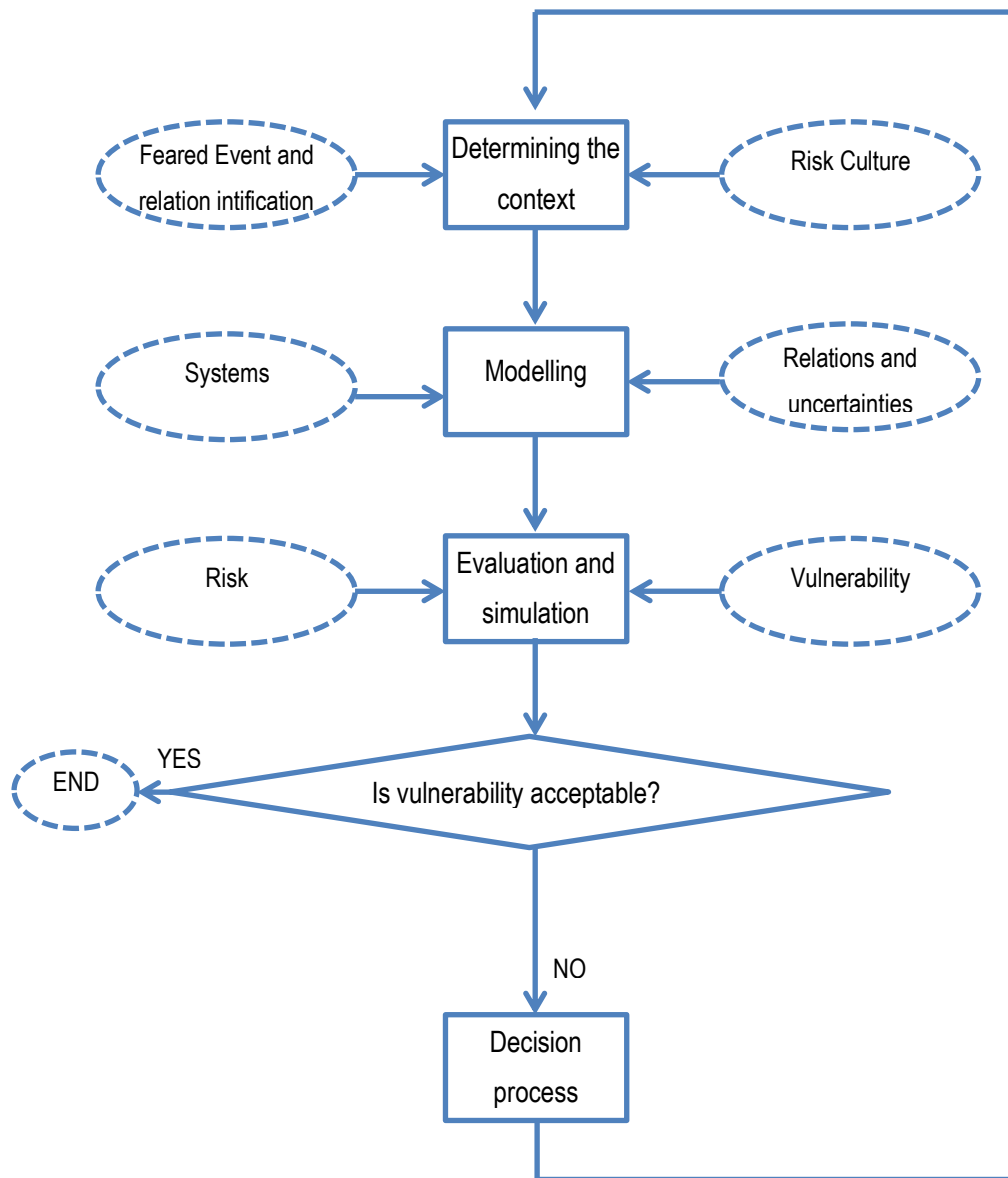


Figure II-19: Analysis framework

The parameters of the context are difficult to determine. The analyst is assumed to be an expert of the area. After modelling step, vulnerability and risk can be assessed. A decision process would be needed if vulnerability and/or risk are not acceptable. The model for vulnerability assessment is presented in the following section.

## II.1.8 VULNERABILITY ASSESSMENT

In the literature, authors agree on some vulnerability properties. We present below the ones which seem to be relevant from our points of view:

- The vulnerability is not increased by edges adding;
- Vulnerability is a function between  $[0,1]$ ;

- For different networks with the same size, the complete graph is the least vulnerable;
- The path redundancy and the presence of complementary networks that can carry the same flows reduce the vulnerability;
- The vulnerability is multi-dimensional [105]. This means that it is linked to several parameters.

To assess the vulnerability, let's consider a single system represented by Figure II-16.

*For instance the system could be an entire network like a power grid, a component like a water tower. The output in this context is the flow such as electricity (or its parameters). The input is a feared event like an earthquake.*

As soon as the output is different from its nominal value, the system will induce an *averred vulnerability*.

*For a power plant, it will induce an averred vulnerability as soon as the intensity of the electricity is different from the nominal value.*

The concept related to the averred vulnerability in the literature is the robustness. Robustness is the structural component related to the network's physical organization. The next section presents this concept.

### ✓ **Robustness**

---

Robustness is defined in various ways in the literature. The Table II-4 shows some definitions.

<b>Definition</b>	<b>Author</b>
A complex network is robust if it keeps its basic functionality even under failure of some of its components	[106]
Robustness is the extent to which, under pre-specified circumstances, a network is able to maintain the function for which it was originally designed	[107]
The degree to which a system or component can function correctly in the presence of invalid inputs or stressful environmental conditions	[108]
Ability to resist imprecision	[109]
The ability for a system to withstand a strain	[21]

*Table II-4: Robustness definitions*

From definitions in Table II-4 we deduce that robustness is the ability to withstand a constraint [24], or the ability to maintain its connectivity properties after damage of one or more of its components (nodes and edges) [36]. It means that the system will maintain its functions intact when exposed to disturbances [14]. In

the context of this thesis the function of component is to assume flow circulation. For this reason the following definition is provided.

**Definition II-5: The robustness is a system aptitude to assume flow traffic after a feared event occurrence.**

From this definition, the robustness of a component depends on its flow consumption. It is calculated only for component whose initial and final consumption are non-null.

Let us note that  $C_{np1}$  is the component  $n$  consumption in flow  $p$  before the feared event and  $C_{np2}$  is consumption after the feared event. Robustness is under the following constraints:

$$\left\{ \begin{array}{l} \text{if } C_{np2} = C_{np1} \text{ then } R_{nbp} = 1 \\ \text{if } C_{np2} = C_{np1} = 0 \text{ then } R_{nbp} = 1 \\ \text{For } C_{np2} > C_{np1} \text{ then } R_{nbp} \text{ increases if } C_{np2} \text{ increases} \\ \text{For } C_{np2} < C_{np1} \text{ then } R_{nbp} \text{ decreases if } C_{np2} \text{ increases} \end{array} \right. \quad (II-3)$$

Robustness induced by a flow  $p$  to the component  $n$  for  $C_{np2} \neq C_{np1}$  is given by:

$$R_{nbp} = 1 - \frac{|C_{np2} - C_{np1}|}{C_{np1} + C_{np2}} \quad (II-4)$$

$R_{nbp}$  is the robustness induced by the flow  $p$  to the component  $n$ . In this thesis flows are supposed to be robust. Indeed they are not supposed to consume each other. In case of many flows consumed by a component  $n$ , the resulting robustness is the product of robustness.

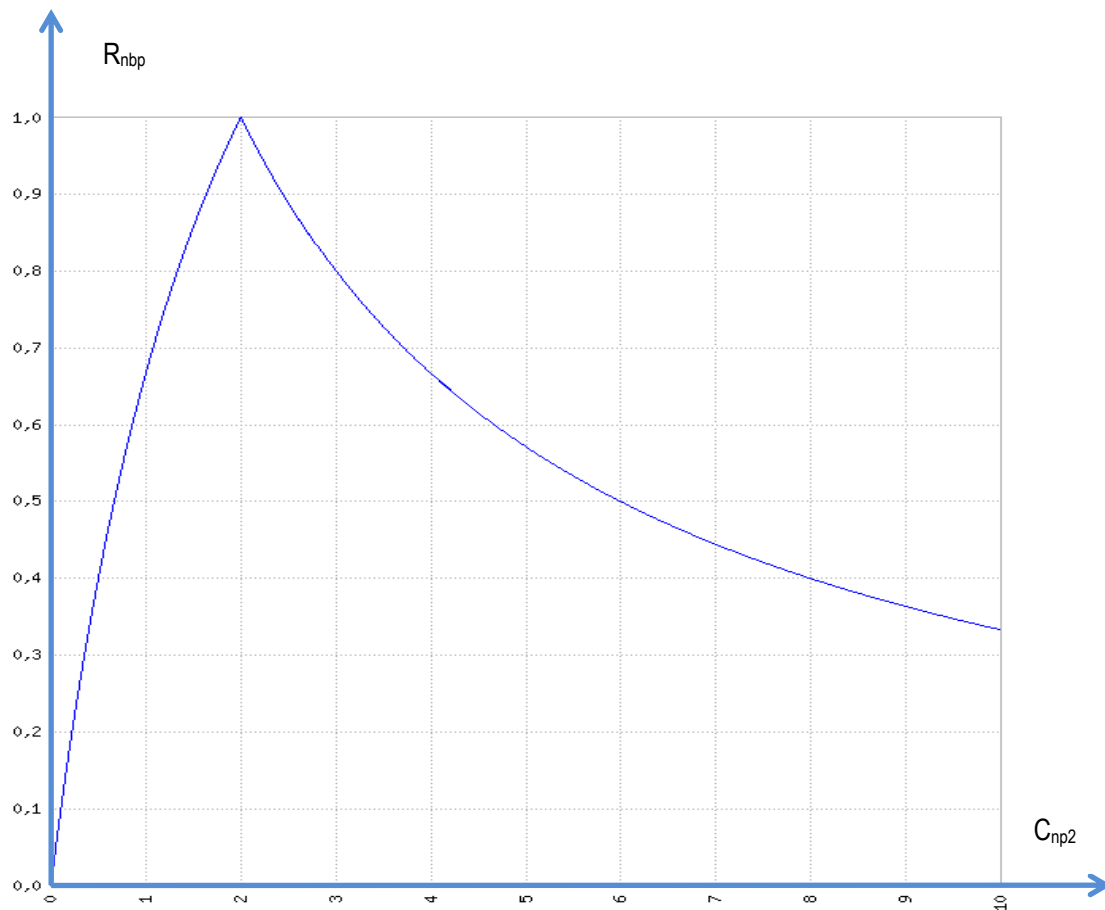


Figure II-20: Robustness evolution

The Figure II-20 presents the robustness evolution according to the final consumption (for  $C_{np1}=2$ ). It shows that the robustness will increase with the final state consumption if this one is superior to those of the initial state. Otherwise it will decrease.

If there is an averred vulnerability i.e. the robustness is different from 1, the system will induce an *Intensity of vulnerability*. This intensity is related to the resilience presented in the next section.

### ✓ Resilience

The concept of resilience is different from that of robustness. The Table II-5 shows the points of view of some authors in the literature.

<b>Definition</b>	<b>Reference</b>
Capacity to cope with unanticipated dangers after they have become manifest, learning to bounce back	[110]
The ability of a system to withstand stresses of environmental loading	[111]
The capacity to adapt existing resources and skills to new situations and operating conditions	(Comfort, 1999) quoted by [112]
The ability of social units (e.g., organizations, communities) to mitigate hazards,	[113]

contain the effects of disasters when they occur, and carry out recovery activities in ways that minimize social disruption and mitigate the effects of future earthquakes.	
The ability to bounce back from adversity and regain health.	[114]
The capacity to recover from extremes of trauma and stress is termed resilience. Resilience reflects a dynamic confluence of factors that promotes positive adaptation despite exposure to adverse life experiences.	[115]
Capacity of a system to experience disturbance and still maintain its ongoing functions and controls	[116]

Table II-5: Resilience definitions

From these definitions, the resilience implies that the system can adapt and find a new stable position close to its initial state after the occurrence of the feared event [14]. In the context of this thesis the resilience is defined as following:

**Definition II-6 : Resilience is the aptitude of a system to retrieve its nominal state functioning after a feared event occurrence.**

According to this definition, the resilience is assessed by considering the nominal state of the system to be analysed. It determines the stake's aptitude to recover this nominal state. Its assessment depends on actions efficiency and rapidity. After a simulation which leads to a new state, resilience depends on the cumulated time of the bad functioning states ( $t_2$ ), and that of the good functioning ( $t_1$ ). In our approach the resilience includes the maintenance means. Its assessment might respect some constraints presented in the following.

$$\begin{cases} \text{if } t_2 = t_1 \text{ then } R_{ns} = 0,5; \\ \text{if } t_2 \text{ decreases then } R_{ns} \text{ increases;} \\ \text{if } t_1 \text{ decreases then } R_{ns} \text{ decreases.} \end{cases} \quad (II-5)$$

From these constraints; resilience is acceded by:

$$R_{ns} = \frac{t_1}{t_1+t_2} \quad (II-6)$$

The evolution of the resilience according to the cumulative good functioning state and that of bad functioning one is given by the Figure II-21 and Figure II-22.

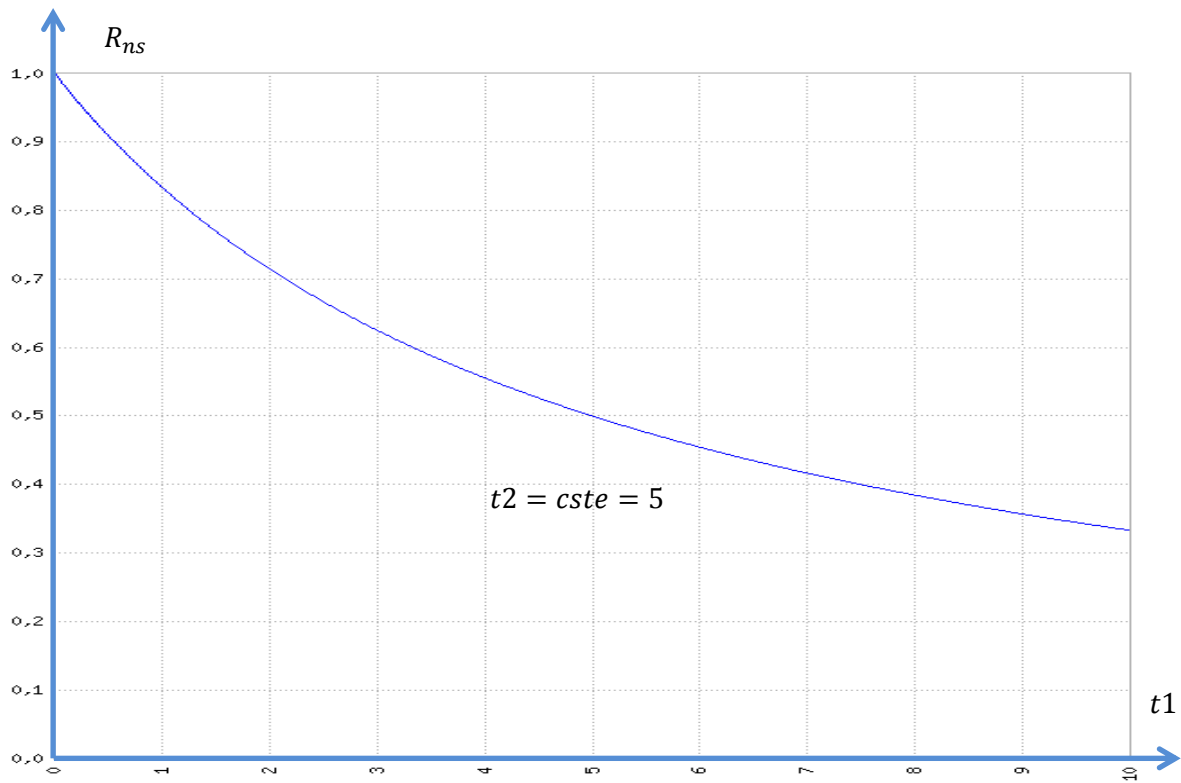


Figure II-21: Resilience for  $t_1$  equal constant

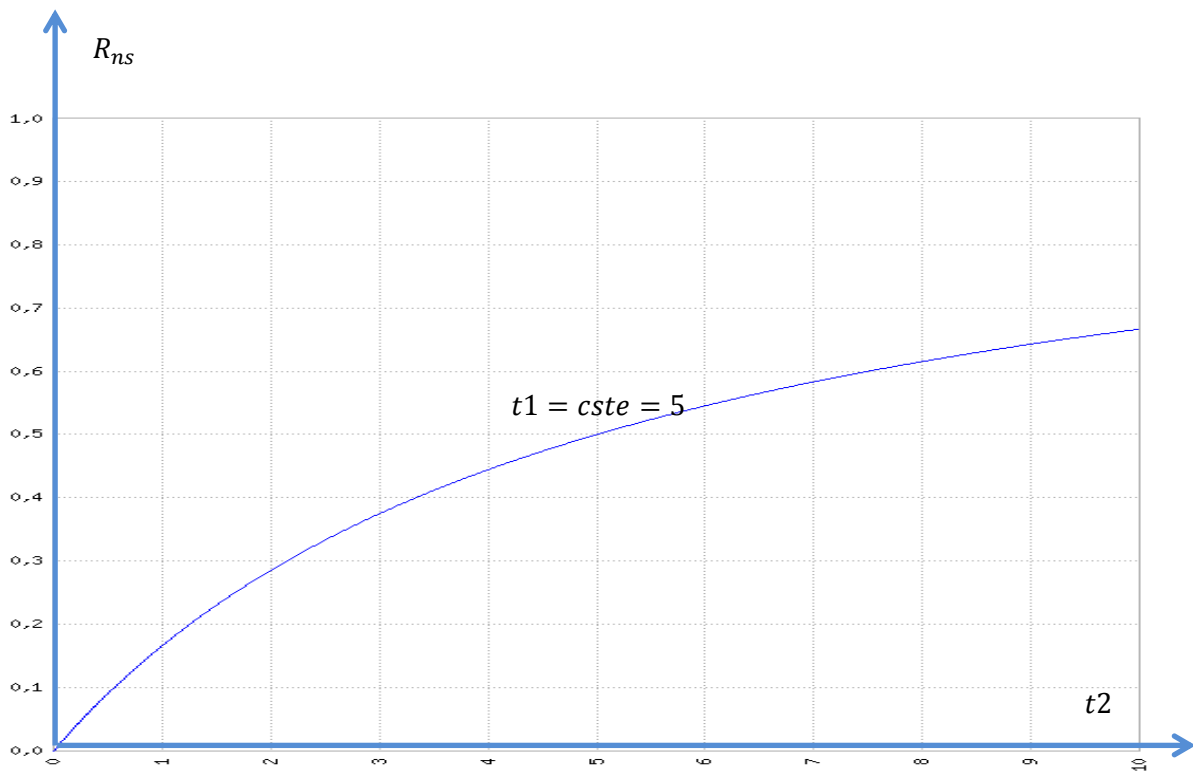


Figure II-22: Resilience for  $t_2$  equal constant

According to these figures, the resilience variation is not linear. It depends on the simulation time. Then vulnerability is also time-dependent.

## ✓ Vulnerability

The vulnerability includes two components: (Robustness); and a functional component related to its ability to recover a nominal state (Resilience). It supposes then the existence of an averred vulnerability, and has intensity. We defined the vulnerability as “the incapacity of a stake to resist to the occurrence of a feared event and to recover efficiently its nominal function during a given period of time”. A stake can be vulnerable to a feared event without being exposed to this event. The more a stake will resist to the feared event effects and will recover quickly its nominal functions, the less it will be vulnerable. The concept of vulnerability in the context of this thesis has many aspects divided into global vulnerability (for the entire network), specific vulnerability (for a component, a network or region), vulnerability induced by interdependences. These classes are named perspectives by [19]. The author pointed out three vulnerability classes: Global vulnerability, critical component and geographical vulnerability. These perspectives are not sufficient in our point of view. Indeed, many other parameters must be included in the vulnerability assessment. In this thesis, we consider the following aspects in the vulnerability analysis: Specific vulnerability for one element, network vulnerability for an entire network, territorial vulnerability and vulnerability induced by the relationships.

The Figure II-23 shows vulnerability classes. Specific vulnerability is composed of that of network component, stake, flow, and factor. In addition, vulnerability might be related to an entire network, a territory or it can be induce by an interdependence. By the fact that a territory could host many component, its vulnerability could include that of component, stake, flow or factor.

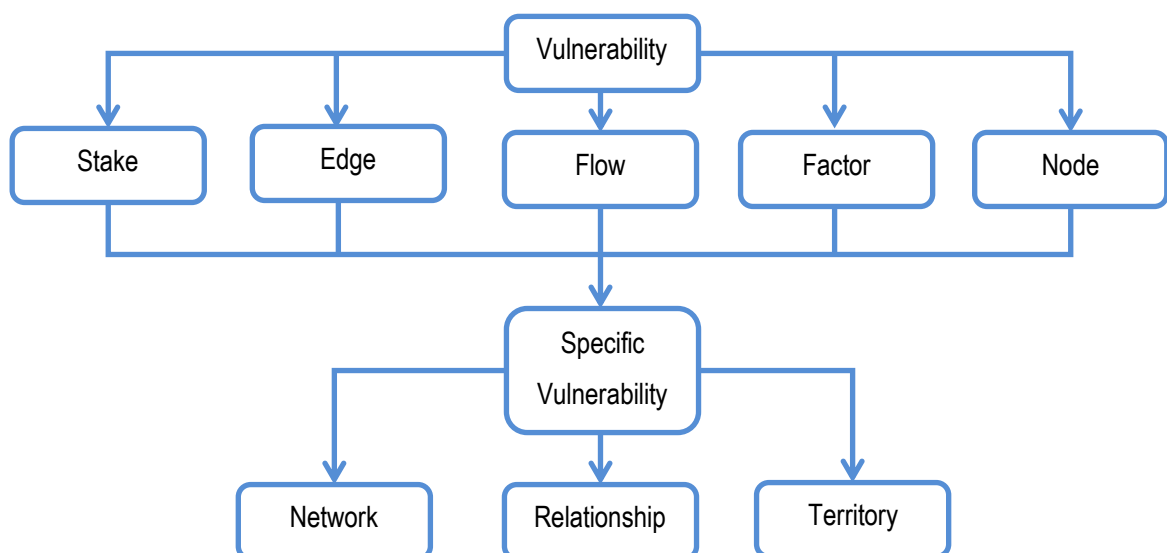


Figure II-23: Vulnerability Classes



Figure II-24 illustrated the fact that vulnerability assessment is based on the system states. At the beginning, it is in an initial state supposed to be the good functioning one. Many feared events identified in II.1.2.2 could occur at the time  $T_0$  and drop the system in another state. The element will be in a stable functioning state at  $T_1$ . According to the deployed mean and the element maintainability it will stay in this state until the tile  $T_2$ . It will get its initial state at the time  $T_3$ .

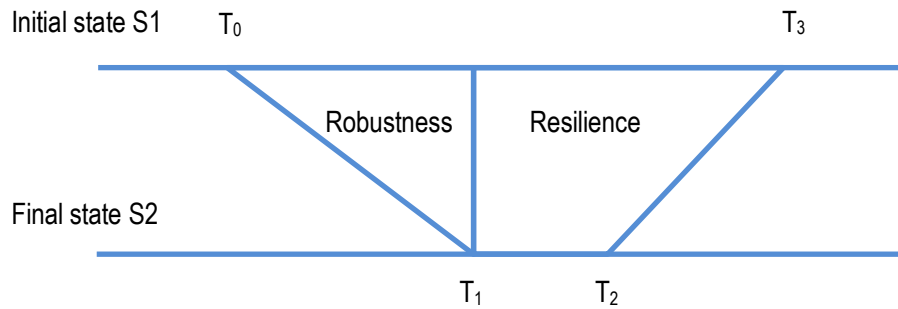


Figure II-24: Robustness and resilience

Vulnerability analysis is used for characterizing the lack of robustness or resilience [117], [9]. Robustness is the system's ability to resist its environment random evolution while resilience is its ability to recover its nominal function after feared event. Vulnerability is then composed of two elements: The robustness or resistance ( $R_{ns}$ ) and the resilience ( $R_{nb}$ ).

The specific vulnerability is the vulnerability of a single element  $n$  ( $\vartheta_n$ ). The element can be a network component, a stake, a flow or a factor. To determine the function  $\vartheta_n$ , many constraints might be satisfied.

$$\left\{ \begin{array}{l} \vartheta_n \in [0,1]; \\ \text{if } R_{ns} = 0 \text{ and } R_{nb} = 0 \text{ then } \vartheta_n = 1; \\ \text{if } R_{ns} = 1 \text{ or } R_{nb} = 1 \text{ then } \vartheta_n = 0; \\ \text{if } R_{nb} \text{ is constant then } \vartheta_n \text{ decreases with the increase of } R_{ns}; \\ \text{if } R_{ns} \text{ is constant then } \vartheta_n \text{ decreases with the increase of } R_{nb}. \end{array} \right. \quad (II-7)$$

Those constraints lead to the following truth table.

$\vartheta_n$		$R_{ns}$	
		0	1
$R_{nb}$	0	1	1
	1	1	0

Table II-6: Vulnerability truth table

From these constraints, component  $n$  specific vulnerability is given by:

$$\vartheta_n = 1 - R_{nb} \times R_{ns} \quad (II-8)$$

This equation shows that a component totally robust and resilient would be invulnerable. On the contrary to be totally vulnerable, the component must be totally unrobust and totally unresilient. For a constant resilience the Figure II-25 plots the intrinsic vulnerability function of the robustness. The graph representing the intrinsic vulnerability for a constant robustness is similar. Vulnerability variation is linear and varies between 0 and 1.

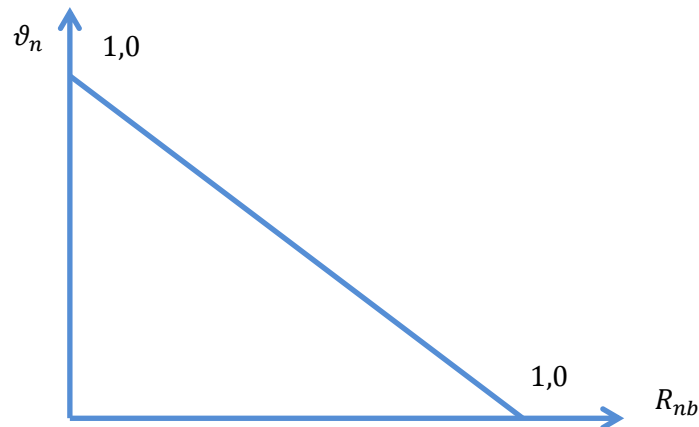


Figure II-25: vulnerability graph

Network vulnerability is that of an entire network. Network vulnerability arises from that of its components:

$$\vartheta = 1 - \prod_{n=1}^N (1 - \vartheta_n) \quad (II-9)$$

$\vartheta_n$  is the vulnerability of the component  $n$ , and  $N$  the number of component. Component includes nodes and edges.

Territorial vulnerability assessment is performed in the same way as network vulnerability. The difference is that on territory there is a flow and stake in addition to network component. The relational vulnerability is the difference between the network vulnerability with and without the considered relations. These three levels will influence the number of edges and nodes used for the simulation.

## CONCLUSION

In the above section we have presented a modelling approach of involved entities in the network vulnerability analysis. After determining literature review shortcomings on graph theory modelling, we presented a method including interdependences modelling. The types of interdependence identified allow every situation modelling. Subsequently, we have determined parameters of other systems and defined interaction modes. We have also presented a vulnerability model. It is based on network functioning simulation. From the nominal functioning, infrastructure can be disrupted either by the feared event or an internal failure. The vulnerability results from the way the system will reach the final state. We have thus seen that the vulnerability of a composed element is a function of that of its components. Once the estimation is made, it now remains to determine actions to reduce the vulnerability. This determination is based on a decision aiding process with a possibility to use a Decision Support System. The following chapter presents the process adopted for the decision aiding.

# CHAPTER III

## DECISION

### AIDING

#### **Résumé en français**

Ce chapitre présente la mise en œuvre des éléments d'aide à la décision pour la gestion d'une crise induite par la défaillance des réseaux d'infrastructure. Elle est divisée en deux parties : La première partie traite des processus d'aide à décision, la seconde présente le système que nous avons développé pour l'implémentation des modèles du Chapitre II. Nous avons commencé par définir les éléments du contexte. Ces éléments contiennent le niveau de crise, la situation de risque, le niveau de décision, l'identification des décideurs, les décisions, les décisions potentielles et les problématiques liées à la décision. La méthodologie que nous proposons inclut la structuration et l'agrégation de ces éléments. Cette démarche est implémentée dans l'outil informatique. Nous avons aussi défini les caractéristiques d'un tel outil ainsi que les risques associés à un projet de développement. L'architecture adoptée est composée d'une base de données, d'une base de modèle, et d'une Interface Homme Machine. L'outil final permet entre autre de déterminer les attributs de chaque éléments du modèle, son évolution pendant le temps de la simulation, les événements les plus redoutés, le temps de moyen de bon fonctionnement, l'effet des interdépendances, et l'interrogation de la base de données.

"You have your way. I have my way. As for the right way, the correct way, and the only way, it does not exist"

Nietzsche

## INTRODUCTION

In the previous chapter we have presented the way of estimating the vulnerability. But this estimation is not an end in itself. Vulnerability assessment must also lead to decisions to reduce and manage it. This is the objective of this chapter. It presents the implementation of decision elements in a crisis induced by infrastructure network failure. It is divided into two parts: the first part deals with the decision aiding process, the second presents the system that we have developed to implement models in Chapter II. We began by defining the elements of the context. These elements contain the crisis level, the risk situation, the decision level, the identification of decision makers, the decisions, the potential decisions and the decision problems. The methodology that we propose includes structuring and aggregation of these elements. This approach is implemented in a Decision Support System. We have also defined the characteristics of such a tool as well as the risks associated with the project development. The adopted architecture is composed of a database, a model base, and a Human Computer Interface. The final tool allows among others determining the attributes of each element of the model, its evolution during the simulation time, the most feared events, the effect of interdependences, and querying of the database.

### I.6: DECISION MAKING DIFFICULTIES

Decision is one of human being's main cognitive activities. In fact, man is a being who doubts. Through the doubt mechanism, it is in constant reflection in every decision process. This situation is further emphasized whenever more than one choice is available to him. In the network management, decisions are taken every time with or without decision process. But in some situations every action might lead to large negative consequences. In such a situation decisions might be streamlined and analysed [43].

*Natural disaster management suits these kinds of situations.*

Every decision taken in crisis situation is to be justified and explained. To overcome these difficulties and reach objectives a decision aiding process is needed.

The objective of the decision aiding is to provide a choice of actions by bringing together the different points of view of actors. The intention is not to seek optimal decisions. The process of decision support relies more in finding compromise.

Decision making process difficulties are pointed out by [118]. They consist in:

- The complexity of the problem;
- Uncertainty of the problem;
- Several different objectives;
- Different conclusions that may derive from different perspectives.

Each decision is taken in a specific context. From the natural disaster context analysis we added to the difficulties of [118] three others: the decision-makers' emotional states instability, the consequences extend, the justification needs [43]:

- **Complexity:** Complexity is one of the difficulties in a decision making process [118]. It consists among others in uncertainty associated with outdoor environments, decision makers' cognitive processes, difference and diversity of actions; decision makers' objectives. The situation of disaster affecting infrastructure network could be seen as complex because of the fact that infrastructures are different from their constitutions and behaviours. It is therefore difficult for a decision maker to understand the overall functioning or evaluate consequences. In such situations, the complexity is enhanced by the high number of components and the interdependence between them. The use of a Decision Support System could give an overview of the context to the decision maker. It could also facilitate potential actions identification by interdependence analysis;
- **Emotional state instability:** In most cases, decision-makers' emotional states are stable. But in a disaster no one can claim to be free from fear, anguish or frustration. Disaster could affect not only infrastructure, but also a decision maker and his immediate family members. When affected, decision maker's lucidity is disturbed. It seems logical and understandable that relevance of any assessment could be disrupted. Because software has no qualms, their uses can minimize judgmental errors in such a situation. In addition, they can reduce the stress and enhance the decision makers' cognitive process [25];
- **Consequences extension:** Decision consequences are often acceptable and do not require any special justification. Conversely, there are situations where consequences may be unacceptable. For some of them, even if consequences are acceptable, they require a justification [43]. Natural disasters are especially suitable to such situations. Through interdependence phenomena disaster can extend beyond a nation limits.

*The Icelandic volcano in May 2011 well illustrates this kind of situation. Several flights have been cancelled by companies in several states. It was not easy to determine aircraft path to optimize international traffic.*

Decision Support Systems in such a situation will be helpful for decision makers;

- **The need of justification:** Even insignificant actions must be justified in the context of disaster. Media pressures increase this need for justification. A Decision support system in this sense is a justification mean.

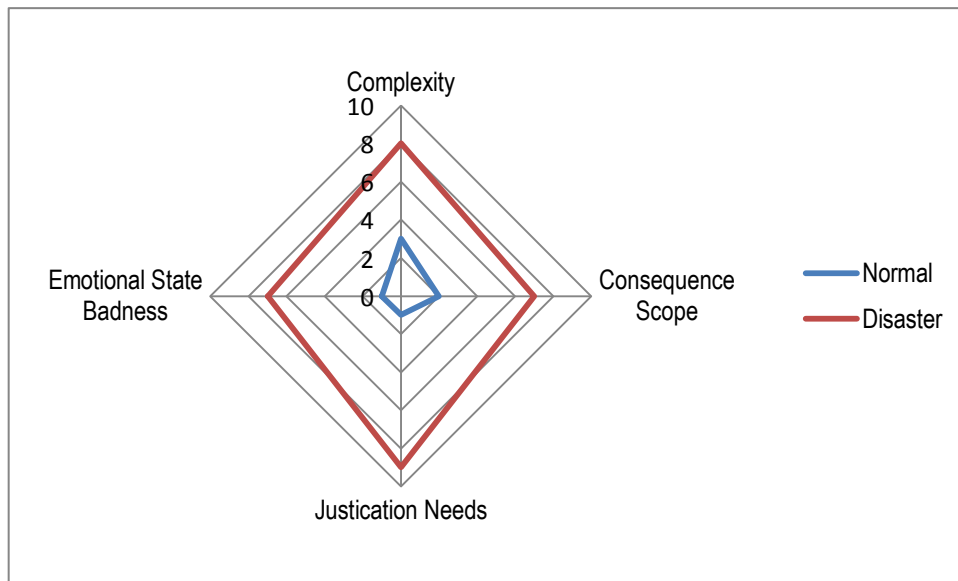


Figure III-1 : Decision context

To illustrate this situation, Figure III-1 compares a current decision situation and disaster situation one. We can see that currently everyday decisions are not complex, their consequence scope is limited, they don't need justification and the decision maker's emotional state is quite stable. On the contrary, in a crisis situation, decisions are more complex, the consequence scope is high, decisions need to be justified, and the decision makers are emotionally instable. Thus, in natural disaster situations, the need of being helped seems obvious for decision making. Using computer software (Decision Support System) is therefore valuable for the crisis management.

In decision aiding there are many methods, but there is not an affirmed one [44]. We have decided to divide our research on decision aiding into two categories as suggested by [119]: Decision theory building (decision process), and the Decision Support System application development. We begin by the decision process presented in the next section.

## I.7: DECISION PROCESS

[49] argues that decision is not an act but a process carried out to solve problems. We share this point of view which is a common reference quoted by many authors in the decision aiding. For this reason the following definition is proposed



**Definition III-1 :** *Decision aiding is an interactive process between decision makers, stakes and subsystems with the aim of finding satisfying states for every involved entity.*

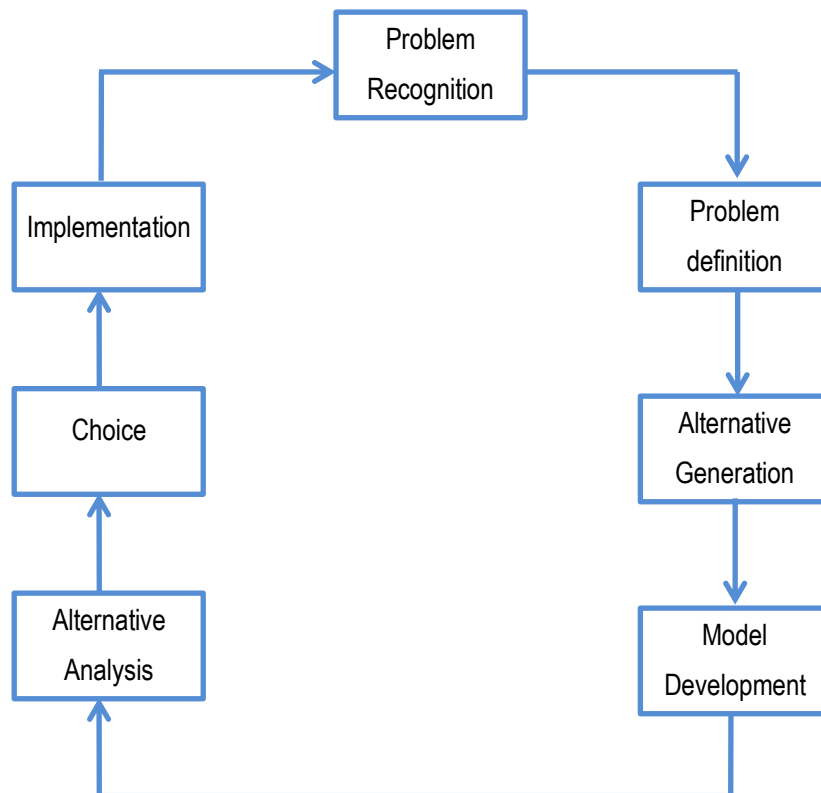


Figure III-2 : Decision-making process: source [120]

The process of Decision Aiding shown in Figure III-2 highlights the decision as being a process. It begins by the problem recognition. That will allow a better definition of the identified problem and alternative generation. Furthermore, best alternatives are to be selected among generated one after their analysis. The last step is implementation of the selected alternative.

As it can be seen, a decision process is composed of many phases. Those are also named *process progress states* [52], *criticality of the environmental context, artefact* [44], *decision mean time* [54]. From Simon's point of view decision has four main phases in the field of management: Intelligence, Design, Choice and Review. This point of view is shared by many other authors in the literature [121]. Simon's process best suits management in industrial context than that of disasters. In fact, in such context it might be more than four phases. These phases are identified and described in the Chapter III. With regard to [44], he presented four artefacts of a decision process: problem situation representation, problem formulation, evaluation model, and final recommendation.

- The problem situation representation is set of  $P = \langle A, O, S \rangle$ .  $A$  is the set of decision process participant,  $O$  is the set of stake carried by decision makers,  $S$  is set of engagement taken by decision makers about their own stake and about stake of the others decision maker.

- Problem formulation is the set of  $\Gamma = \langle A, V, \Pi \rangle$ .  $V$  is the set of viewpoints,  $\Pi$  is the decision problem.
- Evaluation model is the set of  $M = \langle A, \{D, E\}, H, U, R \rangle$ .  $D$  is the set of dimensions,  $E$  is the set of scales associated to each element of  $D$ ,  $H$  is the set of criteria,  $U$  is set of uncertainty distribution associated to  $D$  and/or to  $H$ ,  $R$  is the set of operators that allow synthetic information obtaining on elements of  $A$ .

As it can be seen in [44]'s description, each phase is composed of many elements or grain. [44]'s model is quite similar to that of [52] and has the same limitations mentioned above. In this thesis, phases are especially designed for a crisis induced by network failure. But they could be adapted to other crisis situations. The main difference with [52]'s proposition is the integration phase. Indeed, network management is a complex task which needs the use of a Decision Support System. The process is then composed of five phases: Characterization, Modelling, Structuring, Aggregation and Integration.

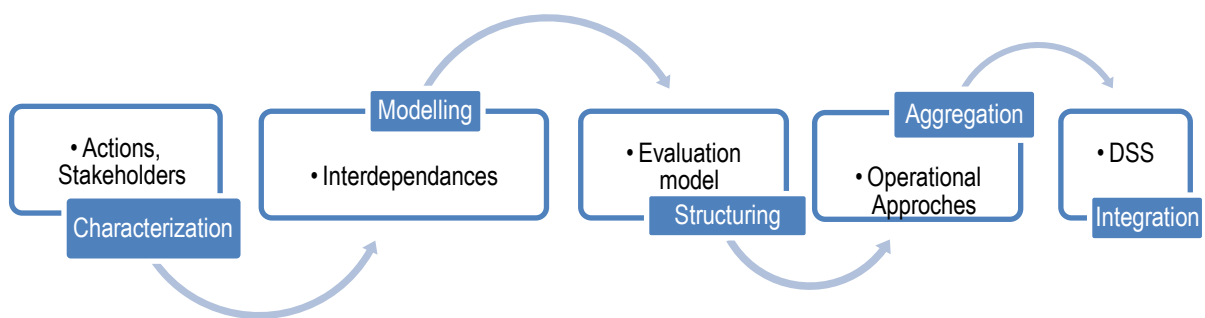


Figure III-3: Decision phases

The first step of this approach is to describe the decision context in the characterization phase. After this description, networks and interdependencies modelling would be performed in the modelling phase. The modelling approaches presented in I.4: will enable the structuring of characterized elements. This helps the selection and the integration of an operational approach for the performance aggregation.

The process is supported by a decision maker, an analyst and eventually a decision support system. Every step of the process presented in the Figure III-3 is constitutive of some elements. [122] describes decision elements as constitutive of: Input, Output, Decision Makers, Analyst, Decision Support System, and Decision process. The main limitation of [122]'s model is the non-integration of the decision level and the risk situation. To overcome this shortcoming, we provide the description presented by the Figure III-4. It describes decision as a process in a crisis level and a risk situation. It is composed of many phases. Each phase is endowed grains. According to the context, a decision method would be used to transform the inputs into outputs. The inputs can take many forms. They are identified by the analyst. The outputs are set of recommendation, and/or justifications. Notion of analyst and decision maker are presented in Chapter III.

The next section describes the first step of our approach, the decision context characterization.

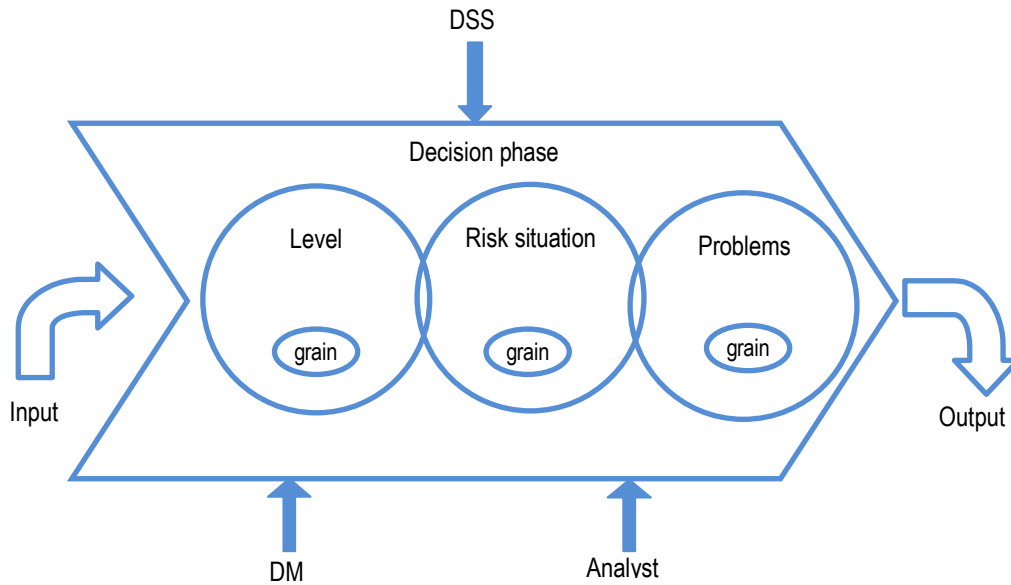


Figure III-4: Decision aiding process elements

### III.1.1 DECISION CONTEXT CHARACTERISATION

Some experiences show that the problem formulation influences decision maker's behaviour [44]. Simon quoted by [44] shows that in the decision theory it is admitted that decision makers know their problems. This hypothesis is not validated according to Simon. It is then necessary to determine the decision context in order to better understand [66]. The aim of characterization is to understand the need of the decision makers. It leads to decision characteristics. Those are called by [52] aspects of reality, or invariant. Characteristics are supposed to be sufficiently stable for every phase. Their change may put in another sub-process. Our approach considers the context as a set of six components:

$$C = \langle CL, RS, DL, DM, D, DP \rangle \quad (III-1)$$

Where CL is the crisis level, RS the risk situation, DL, decision level, DM the decision makers, D decisions, DP the decision problems. Problem formulation in our point of view may integrate crisis level, risk situation and decision level. These elements have not direct impact on the decision model, but they could change the decision maker's behaviour and indirectly the final decision. These components are presented in the following.

#### III.1.1.1 CRISIS LEVEL

Crisis level analysis is investigated by many institutions and governments. The FEMA (Federal Emergency Management Agency) pointed out four levels in a crisis management: Preparedness, Mitigation, Emergency

Response, and Recovery. [123] pointed out three levels: pre-crisis, crisis and post crisis. These phases are too simplistic especially when it is induced by natural disasters. From our point of view, crisis is composed of the following phases:

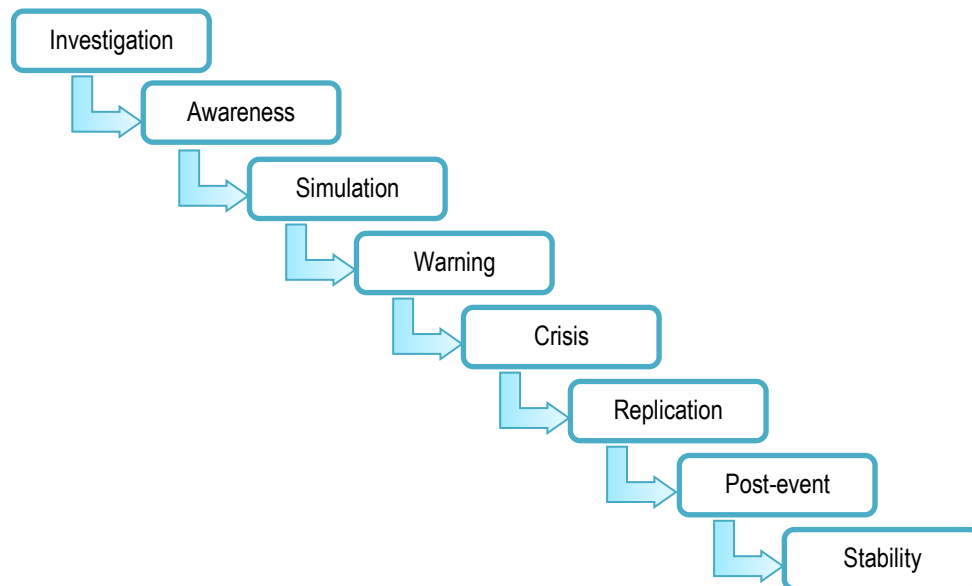


Figure III-5: Crisis level

- Investigation: To identify the feared events and the stakes: This is the phase of ignorance which aims to identify risks;
- Awareness of the situation: In this phase, the risk is known, stakes are aware of the situation which means the beginning of cognitive processes to integrate the risk culture;
- Simulation: Aims to evaluate different scenarios through models more or less elaborated;
- Warning: This is the phase where we assist to the appearance of the feared events' signs;
- Crisis: Occurrence of the feared event;
- Replication: The event is over but the risk of recurrence is high. Replicas are seen especially when it comes to earthquakes;
- Post-event: The crisis is over, but it remains to rebuild and repair damages;
- Stability: This is the last phase. Choices are evaluated and feedback formalized.

We consider that each of crisis level corresponds one or more decision phase. The Table III-1 presents decision phases for every crisis level.

<i>Crisis Level</i>	<i>Decision phase</i>
Investigation	Characterisation,
Awareness	Characterisation
Simulation	Characterisation, Modelling, Structuration, Aggregation, Integration
Warning	Characterisation
Crisis	Characterisation, Modelling, Structuration, Aggregation
Replication	Characterisation, Modelling, Structuration, Aggregation
Post-event:	Characterisation, Integration
Stability	Characterisation, Integration

Table III-1: Phases by crisis level

Table I-1 shows that the characterization phase is present at many crisis levels. In fact to be efficient, our model needs to be characterized before the disaster occurs. The next section presents the risk situation.

**III.1.1.2 RISK SITUATION**

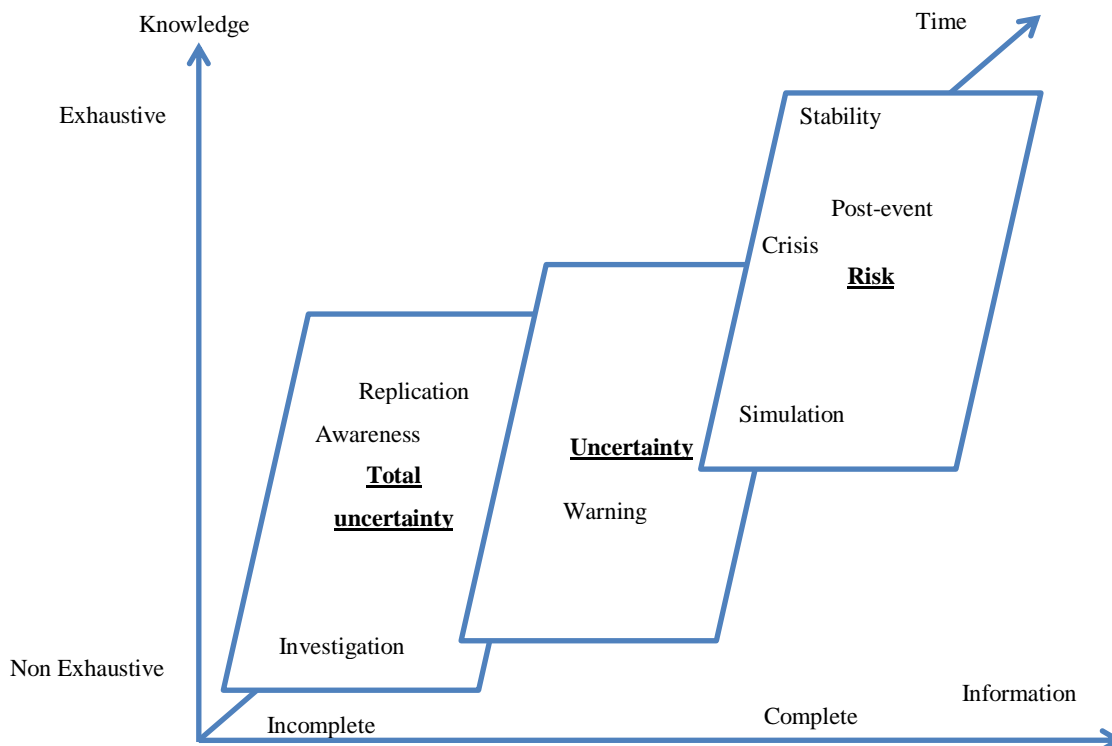


Figure III-6: Crisis situation inspired from [54]

The risk situation depends on available information and knowledge. [54] has identified three situations in risk analysis: total uncertainty (incomplete information and knowledge is not exhaustive), risk (full information, exhaustive knowledge), uncertainty (between the two situations, with subjective probabilities).

Figure III-6 draws crisis level according to the risk situation pointed out by [54]. Based on crisis level, it shows that phases of stability, post-event crisis and simulation are in a risk situation; phases of warning in an uncertain situation; phases of replication, awareness, and investigation in a total uncertain situation. Decision levels are presented in the next section.

### III.1.1.3 DECISION LEVELS

Decision level corresponds to the decision aiding process horizon. Literature presents three typical levels of decision: operational level, tactical level, and strategic level [54]. Decision levels are represented on three axes: Information (accurate-global), impact (local-national), and scientific dimension place (low-very important). To these axis might be added: problem's definition (how well it is defined); states' variables quantification; nature (technical, organizational, etc.); complexity; goal (general, local); scope (long term, short term); coherence; and data certainty.

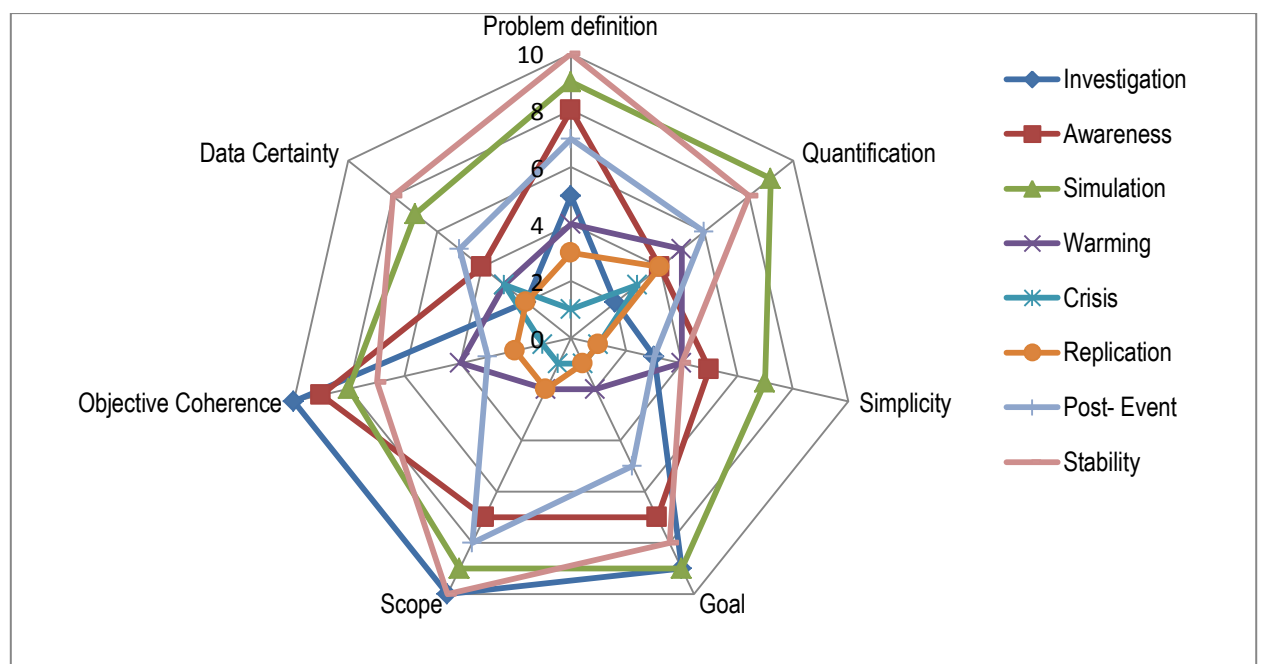


Figure III-7: Decision level

Strategic decisions contrary to managerial decisions must be made in environment with imprecise and uncertain information [124]. The authors emphasize that most strategic decisions are made in groups [124]. Level depends on analysis phase. Figure III-7 shows the situation of Lourdes on a scale from 0 to 10, plotted in a radar diagram presented in [125]. It can be noticed that phases of simulation and stability are in an

operational level, phases of investigation, post-event, and awareness in a semi-strategic level, phases of crisis, replication and warning in a strategic level.

#### III.1.1.4 DECISION MAKERS IDENTIFICATION

One of the decision process issues is to answer the question: Who is going to be helped by the decision or take decisions? Decision makers are also named actors or stakeholders. The following definition is adopted in this thesis.

**Definition III-2 : Decision maker is individual or individual group of which by their value system, whether at first degree because of their intentions or second degree by the way they involve those of others, directly or indirectly influences decision [52].**

Any decision aiding should start by their identification [126]. It follows that disaster crisis management involves several decision makers: *constituted profession*, composed of *experts*, *local authority* and rarely an *isolated individual*. Decision maker has objectives, preferences, elimination criteria, information system. Final decisions are validated through their objective's systems.

By way of illustration, Table III-2 shows Martel's identification approach by decision makers' participations and influences quoted by [54].

	<b><i>Directly involved</i></b>	<b><i>Indirectly involved</i></b>
Influence the problem	Fiduciaries	Invisibles
Affected by the problem	Concerned and active	Concerned and passive
Influence and is affected by the problem	Traditional	Behind curtains

Table III-2: Martel's decision maker identification

[127] described six types of actors for Decision Support Design: initiator, analyst, developer, validation team, user, decision maker. This identification is less applicable to disaster management. Indeed one decision maker might influence and be affected. Then, identification by implication and objective categories seems more relevant.

<b><i>Category</i></b>	<b><i>Example</i></b>
Category 1: International	World, Continental Community
Category 2: National	Country
Category 3: Regional	City

Category 4: Infrastructure manager	EDF, GDF
Category 5: Local Operator	Local operator
	Site
Category 6: Citizen	
Category 7: Emergency	Hospital
Category 8: Analyst	

Table III-3: Decision maker categories

In Table III-3 eight categories have been identified from high objective level (International) to the low objective level (component).

<b>Crisis Level</b>	<b>Decision Maker</b>
Investigation	Analyst, Local
Awareness	Analyst, Local
Simulation	Analyst, Local
Warning	Emergency, Local
Crisis	Emergency, Component, Local, National,
Replication	Emergency, Component; Local
Post-event:	Analyst, Local, National,
Stability	Analyst, Local, National, International

Table III-4: Decision maker per crisis level

Each crisis level concerns especially some categories shown in the Table III-4 which underlines the place taken by the analyst and the local decision maker. The next sections will present decisions that could be taken in a general way.

### III.1.1.5 DECISIONS

Decision makers are likely to make arrangements and take decisions to solve identified problems. Decision is also called action. It is defined as following

**Definition III-3 :** *Decision represents a possible contribution to the overall decision and likely, given the sub-process, to be independently envisaged, and to serve as a point of application through to decision aiding [52].*

Simon distinguishes two types of decision. The first is programmed and repetitive, the second is unscheduled, unusual and unstructured. From this standpoint the decision-making in a disaster context is obviously an



unscheduled decision. In networks' vulnerability analysis, all decisions are finite. Their numbers directly proportional to the number of components being high, they should be defined by a description instead of an exhaustive list. Furthermore, the environment of a natural disaster is changing. Decisions are then becoming progressive. They are also fragmented in as much as the results of the decision process involve combinations of several elements of the actions' set.

Another characteristic is the fact that actions are dynamic and depend on the phases. In addition, decision maker can act or evaluate only some of them. This evaluation is not static.

We have identified seven categories of action. The identification is made in a generic way in order to be expandable to other studies. These categories are based on a network vulnerability's model presented in [128] and [91]:

- Action on network components: Action on component may be changing some of their structural parameter; reliability etc. It can also consist in adding or removing component;

*Building new roads, airfields, increasing the reliability of a power plant are example of action on network component.*

- Action on flows: Action on flow consists in changing its speed, reliability, resistance, circulation law. Adaptation of this law can contribute to streamlining of the entire network;

*This is especially what happens on the power grid, where electricity is supplied to vital structures.*

- Action on factors: For example increasing hospital autonomy by providing generators or additional beds;
- Action on stakes: The evacuation of an area, the riser of a transformer, information;
- Action on interdependences: Interdependence might be a cause of cascading failure, when one component failure impacts on other components' failures. Acting on these interdependencies can help to significantly reduce network's vulnerability.
- Action on feared event: feared event is characterized among other by its propagation speed. Decision maker could take some measures to reduce it.

Through these categories, we consider that actions are vectors of several sub-actions. Decision problems from these actions are presented in the next section.

### III.1.1.6 DECISION PROBLEMS

Problems correspond to the manner of envisaging and formatting conclusions and decisions. Bernard Roy in [52] has identified four problems in decision aid. Choice ( $P_\alpha$ ), which takes the form of a subset selection;

sorting ( $P_\beta$ ), which corresponds to a form of assignment to predefined categories; rank ( $P_\gamma$ ) which takes the form of a ranking actions, and description ( $P_\delta$ ) for describing and structuring.  $P_\delta$  precedes other problems [66]. In natural disaster context, we pointed out two others problem: acceptance and change management, and planning problem.

#### ✓ *Problem $\omega$ acceptance and change management*

In disaster context, the four classical problems of decisions are not sufficient for describing all situations. Indeed, there's a problem of acceptance and change management. One situation might be well described but not accepted. The problem  $\omega$  is encountered in post crisis phases.

#### ✓ *Problem $\kappa$ of planning*

The problem of planning is justified by dynamism of actions and uncertainties. These problems, function on the study phase, are presented in Table III-5.

<b>Phases</b>	<b>Problem</b>	<b>Objectives</b>
Investigation	$P_\delta P_\alpha, P_\beta, P_\omega$	Identifying risk
The awareness of the situation	$P_\delta, P_\omega$	Establishment of the culture of risk
Simulation	$P_\delta, P_\omega$	Elaboration of scenarios
Warning	$P_\delta, P_\alpha$	Information et communication
Crisis	$P_\delta, P_\alpha, P_\beta, P_\gamma, P_\kappa$	Minimize the consequences for stakes
Replication	$P_\delta, P_\alpha, P_\beta, P_\gamma, P_\kappa$	Minimize the consequences for stakes
Post- Event	$P_\delta, P_\alpha, P_\beta, P_\gamma, P_\omega, P_\kappa$	Restoration of affected infrastructure, action planning
Stability	$P_\delta, P_\kappa, P_\omega$	Formalization of a feedback

Table III-5: Problem per phase

Table III-5 underlines the importance of the crisis and replication phases where all problem exists. After the context characterization, the system modelling is needed before the decision itself. The elements of the model are presented in the next section.

### III.1.2 SYSTEM MODELLING

Vulnerability analysis is related to some systems. The decision aiding process is based on models of the identified systems. The need of a model is emphasized in the decision definition in [52]. It is a simplification of the problem. Decision problem modelling is also named formalization [43]. The role of the modelling is to understand the dynamic. According to the problem, many kinds of the system modelling can be used. Mainly, there are mathematical (decision elements description by functions or values) and graphical models (decision tree, graph), and arrays. We used graphical modelling by a graph theory. The modelling approach is presented in the Chapter II. A system model consists of:

$$M = \langle FE, NT, ST, FL, FC, IN, TE, VM \rangle \quad (III-2)$$

Where FE is the Feared event, NT is the network, ST is the stake, FL is the flow, FC is the factor, IN is the interdependence, TE is the territory, VM is the vulnerability model. This model is presented in II.1.8. After the modelling the structuration will allow to apply a decision process. Decision structuration is discussed in the next section.

### III.1.3 STRUCTURATION

Structuration is called by some authors exploitation [54], evaluation model [44], It is the decision process invariants formatting for an operational approach implementation. We call "structure" set of elements resulting from the structuring process. Structuration consists in identifying potential action, decision makers' preferences systems, criteria evaluation and scenario building.

#### III.1.3.1 POTENTIAL DECISION

In decision making, decision could be classified in many classes: potential, efficient, fictitious etc. Efficient action is not dominated by another action. Real action comes from a project completely developed and can be put in execution. Fictitious action is an idealized project. Realistic action corresponds to a project that implementation can be reasonably expected [52]. Reference actions; serve to limit the categories to which potential actions are affected.

In the III.1.1.4, we have identified actions in a generic way. The aim here is to identify potential action. An action is potential if it is temporarily considered possible by at least one decision maker or presumed by the analyst [62] [54] [64], [52]. Potential actions will be evaluated according to the criteria presented in III.1.3.3. Potential actions are evaluated according to decision makers' preference system presented in the next section.

### III.1.3.2 PREFERENCES SYSTEMS

Actions cannot be compared one by one because of their generic definition. To accomplish this comparison, decision makers, or the analyst judging by their names, must develop a relational preference system. This system reflects diverse views that can be opposed, or even contradictory. Thus, the system must tolerate ambiguity, contradiction and learning wherever possible [52]. Preference systems are also called “approach and the dominant culture” [54]. They are set of beliefs, attitudes and assumptions shared by a group as a result of past experiences [54]. We have determined the preference system for decision makers in Table III-6. There are four basic preference situations: *I* (indifference), *P* (strict preference), *Q* (low preference), *R* (incomparability). The totality of a decision maker’s preference can be grouped into the fundamental relational system of preference, or in the grouped relational system of preference [52], including the outranking relation (*S*), the presumption of preference (*J*), general preference (*>*), non preference (*~*), K-preference (*K*).

<b>Phases</b>	<b>Decision maker</b>		
	Local operator	Network manager	International, National
Investigation	I,P,Q	R,P,Q,I	R,S
The awareness of the situation	I,P,Q	I,> ,	R,S
Simulation	I,P,Q	I,> ,	R,S
Warming	I,P,Q	I,>	R,S
Crisis	R, I,>	R,S	R,S
Replication	R, I,>	R,S	R,S
Post- Event	I,P,Q	R,I,S	R,S
Stability	I,P,Q	R,,I,S	R,S

Table III-6: Relational preference systems

Table III-6 illustrates systems accepting and refusing incomparability: (*I >*), (*I, Q, P*), (*I, R, >*), (*R, S*), (*R, I, S*). Decision makers of category 1 admit incomparability in critical phases. This is due to the fact that before these phases data are available at the local level. Risk for stakes allows taking time needed for the analysis. This situation is similar for the second class, except the investigation phase - where data are less available. However, in line with regulatory requirements, and facing potential communication and collaboration process, decision maker has to accept the incomparability at the international and national level.

### III.1.3.3 CONSEQUENCES

The consequence could be called indicators or impacts, damage, prejudice. They are defined as a progressive effect of system failure through time, on users [17]. The term damage alludes to materials damage, loss refers to human lives [129] and prejudice concerns peoples damages [1]. Generally, an action has several consequences [64]. We have identified 13 categories of consequences induced by infrastructure networks' failure: These criteria are presented in the Table III-7.

<b>Consequences</b>	<b>State</b>
System	Failure cost, Flux losses, flux congestion, Reparation, interruption in communication and transportation
Human	Number of deaf, number of injured, number of traumatized
Environment	Affected ecological systems, , affected species
Economy	Employment losses, insurance, cost, reconstruction
Patrimony	Branding
Legislation	Norms
Politic	Political stability
Education	
Comfort	Indoor temperature
Cognitive factors	Risk acceptance, risk knowledge, change management, population training
Cultural factors	
Organization/institutions	
Security	Increase in crimes

*Table III-7: Decision making criteria*

Table III-7 shows the wide variety of disaster consequences. Some of them can be determined by the vulnerability model presented in II.1.8. Others will be determined by experts' judgments. Potential actions will be evaluated according to some modes presented in the next section. For instance, the loss of flow, affected people can be determined by the model. On the contrary, the political effect has to be determined by expert judgment.

### III.1.3.4 EVALUATION MODE

Decision makers must evaluate potential decision according to the consequences. The evaluation can be performed by one of the following modes. These modes represent the granularity.

- Evaluating actions' scenarios after feared event scenarios;
- Evaluating actions' scenarios after the elements of feared event scenarios;
- Evaluating elements of actions' scenarios after elements of feared event scenarios.

After decision evaluation, a multicriteria aggregation will be used to determine best decisions. The aggregation methods to be used are presented in the next section.

### III.1.4 MUTICRITERIA AGGREGATION

Criteria are derived from actions' consequences [64] and allow their assessment. They represent consequences function for which one seeks to determine the maximum or the minimum [43]. In this thesis the main criterion in the decision point of view is the vulnerability function determined II.1.8. The vulnerability function could be seen as certain criterion. But there are other criteria related to consequences to be taken into account. Their assessments are out of the scope of this thesis and will be performed through expert judgment. Hence there are two main types of criteria in the context of this thesis:

- Assessed criteria: Vulnerability, resilience, robustness etc;
- None Assessed: Environment, Economy, Politic etc.

Criteria aggregation is sometimes called exploitation [54]. In the literature, several decision aiding methods for aggregation can be found. With regard on MCDA the difference resides in multicriteria aggregation procedures [54]. Methods of multicriteria decision aiding can be divided into three families, called operational approaches for aggregating performance in [47], [43]: single synthesis criterion, outranking, local interactive judgment with iterations try-error. [67] also identified three families: The classical approaches, outranking, and utility functions. [126] argues that criteria should be limited in number, complete, including goals, significant, operational, able to discriminate actions and bear comparison of all actions performance. To choose an adapted method [54] proposed seven questions:

- Stakeholders in the decision, are they numerous or not?
- How to think or what cognition procedure is used by decision makers?
- What is the problem referring to?
- What information is available?
- What level of compensation does the decision-maker seek?
- What are the basic assumptions available?
- Is there any software that takes up the principles?

Multiattribute methods allow solving programs that provide satisfactory solutions of various criteria on the basis of linear combination or nonlinear functions. Outranking methods do not follow the axiom that all

consequences are comparable. They therefore agree to the incomparability [43], [54]. For these reasons outranking methods are chosen for the aggregation.

In Figure I-5 and Figure I-6, methods of type A (ELECTRE) and Type C (PROMETHEE) suit more to the context of this thesis. The aim here is not to make a comparative study of these approaches but to justify the chosen method: ELECTRE. We have rejected PROMETHEE because of the fact that in the context of this thesis decisions are defined in a generic way so considered as infinite according to the number of components. In fact, PROMETHEE method is defined for finite actions [130]. Otherwise, the analysis performed in the III.1.1.6 shows many problems in disaster management. This is not the case for PROMETHEE which is mainly for ranking problem [130]. The reader can see Chapter I for a comprehensive comparative literature review. For the reasons cited in I.1.4.2, we have chosen the ELECTRE methods. Such methods have many variants. We use those proposed by [62] to select the appropriate method for each phase. The result of this analysis is given in the Table III-8.

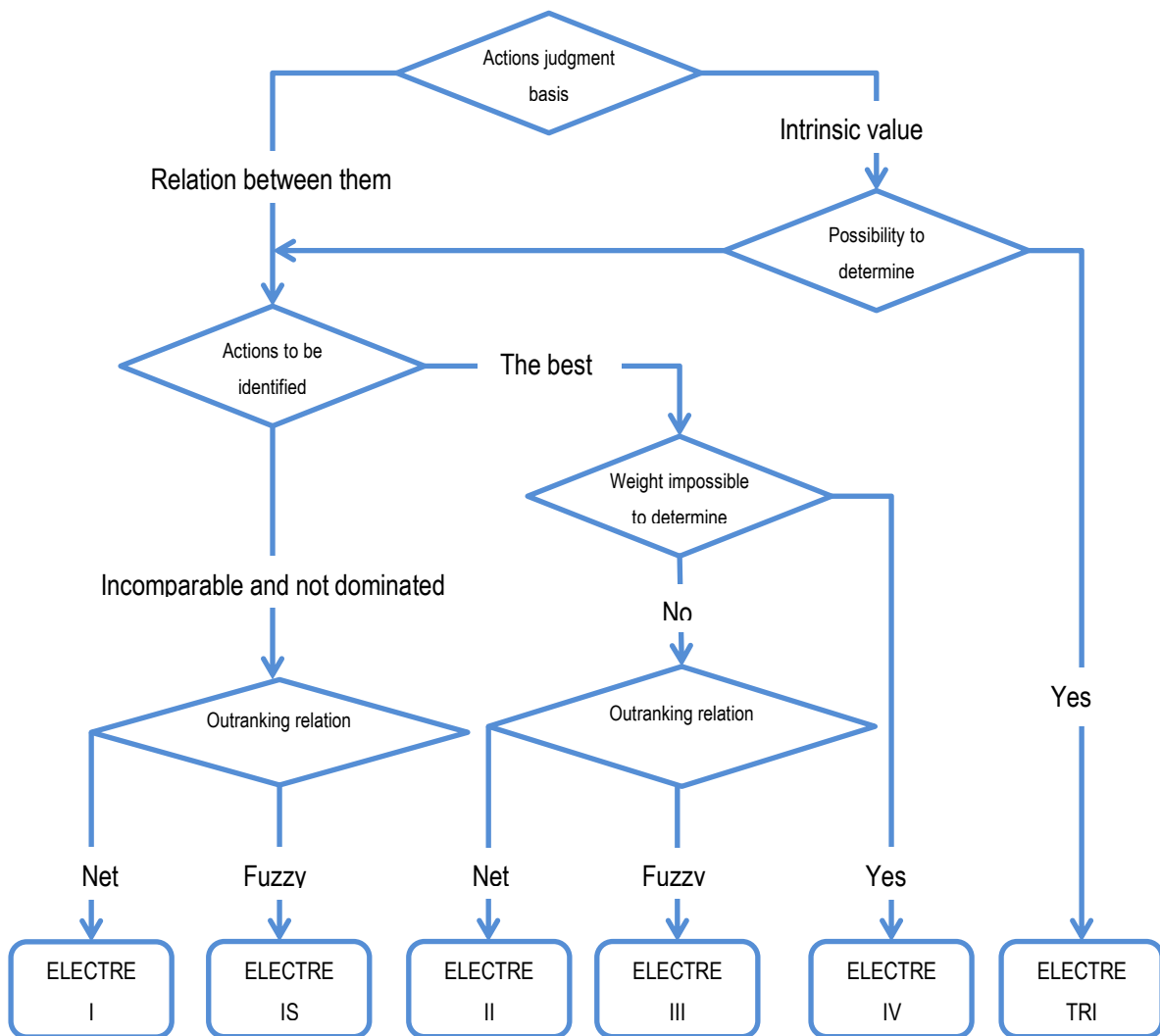


Figure III-8: ELECTRE methods by [62]

Table III-8 shows for each crisis level the dominant problem and the aggregation method.

<i>Phase</i>	<i>Problem</i>	<i>Method</i>
Investigation	Sorting	ELECTRE TRI
The awareness of the situation	Ranking	ELECTRE IV
Simulation	Ranking	ELECTRE IV
Warning	Choice	ELECTRE IS
Crisis	Choice	ELECTRE IS
Replication	Choice	ELECTRE IS
Post- Event	Ranking	ELECTRE IV
Stability	Sorting	ELECTRE TRI

*Table III-8: Aggregation methods*

Choice problem is dominant in the level of warning, crisis and replication phase. This results from the fact that in these situations the most important is to determine best decisions into the potential ones. Because of data imperfection ELECTRE IS is recommended. ELECTRE IS is a further version of ELECTRE Iv which takes into account the notion of veto threshold. This method is the current version of choice problem [69].

Sorting problem is dominant in the phases of investigation and stability. In fact, during these phases, the main objective is to categorize decisions. For this reason, ELECTRE TRI is proposed.

Ranking problem is encountered and predominates in the phases of awareness, simulation and post-event. In these phases it is more relevant for the users to rank decisions in order to select best ones later. For this reason we use ELECTRE IV. This method is the only ELECTRE method which does not make use of the relative criteria importance coefficients [69].

### III.1.5 INTEGRATION

The integration is the set of operations to speed up the process by using a decision support system. The elements of this phase are described in the next section.

## I.8: THE DECISION SUPPORT SYSTEM (DSS)

Disasters have always been societies' destabilization source since the beginning of human societies. In the past, they were attributed to divine wrath sign. Afterward, we begin to understand their manifestations. Actual knowledge allows disaster description through models more or less established. But it is still hard to eliminate causes even if those are identified. The last line of defense is prevention. Decisions applicable to complex infrastructures are then needed.



The aim of this chapter is to describe a method to develop a decision support system (DSS) for infrastructure network failure analysis in a context of natural disasters. DSS engineering is a complex problem. That complexity is related firstly to the diversity and different uncertainties related on one hand. On the other hand, we face the networks structural and functional complexity. In the actual state of knowledge, it is hardly possible to predict the occurrence date of some feared events. The best way to reduce impacts remains crisis management. This is achieved by implementing an effective process in a Decision Support System. In fact, one of the challenges in the crisis management is the decision makers' responsiveness. Indeed, every second counts, decisions must be taken quickly. Using simulation tool seems essential in such situations. The objective of this chapter is to present the Decision Support System for infrastructure network vulnerability analysis. The developed system is called VESTA. The next section presents its features.

### III.1.6 DEFINITION AND FEATURES

Nowadays, there are computer systems in almost all areas of life. Applications can be embedded in equipment from the simplest to the most complex. They exist in common device like TV, but also in large carrier aircrafts or in satellites. To this variety of embedded applications can be added software for management, forecasting, scientific computing, engineering, decision support etc. For those reasons, one of the issues in software engineering is taking into account the nature of the developing system.

Many terms are related to Decision Support System in the literature: artificial intelligence, data mining, on-line analytical processing, knowledge management [15], Group Support System (GSS), Executive Information System (EIS). In general, a Decision Support System is a computer-based system for decision support [131].

There are many definitions in the literature. We divided these points of views into three groups:

- Definitions focusing on the characteristic [131], [120];
- Definitions on the objective [25], [15];
- Definitions on the architecture [121], [119].

Table III-9 summarizes these views.

<b>Definition</b>	<b>Reference</b>
A flexible, adaptive, responsive and interactive computer based system for decision support	[131]
An integration of computer hardware and software that is designed to complement the cognitive processes of humans in their decision making	[25]
Computerized system which improves the activity of decision-makers situated on different levels in the chain of command (from supervision of different processes to leading positions in politics)	[15]
Computer technology solutions that can be used to support complex decision making and problem solving	[120]

Computer based systems, which help decision makers utilize data and models to solve unstructured problems	[121]
DSS is defined as a computer-based interactive system that supports decision-makers rather than replaces them; utilizes data and models; solves problems with varying degrees of structure: non-structured (unstructured or ill-structured) (Bonczek et al, 1981), semistructured (Bennett, 1983, Keen and Scott Morton, 1978), semistructured and unstructured tasks (Sprague and Carlson, 1982), and structured, semistructured, and unstructured (Thierauf, 1982); and focuses on the effectiveness rather than the efficiency of decision processes (facilitating decision processes)	[119]

*Table III-9: Decision Support System definitions*

In this thesis the definition proposed by [121] will be adopted.

**Definition III-4 : Decision Support System is a computer based system, which helps decision makers utilize data and models to solve unstructured problems [121].**

Thus, the main objective of the designed Decision Support System as those of many other is to focus on the use of interactive calculation in semi structured decision-making [132]. To overcome this objective, the Decision Support System must be able to do some tasks. [121] and [15] determined some of them. The authors argue that Decision Support System should:

- Provide support for decision making, but with emphasis on semi-structured and unstructured decisions;
- Provide decision making support for managers at all levels, assisting in integration between the levels whenever appropriate;
- Support decisions which are interdependent as well as those that are independent;
- Support all phases of the decision making process;
- Support a variety of decision making processes, but not be dependent on any one;
- Be easy to use.

To overcome these objectives, Decision Support System must have some features. Their features depend on the use. Those were described by Sprague and Carlson through the ROMC approach [133]: Representations, Operations, Memory Aids, Control Mechanisms. With regard to decision support systems in a disaster setting, they might be flexible, adaptive, responsive, interactive[131], progressive and controllable [25]. To these features, we have identified several others specific to natural disaster context: response time, geographical distribution, views, simplicity, portability, ergonomic, adaptability and efficiency.

- Response time: Temporality is an important concept in the functioning of computer system in general. To be efficient in crisis management, Decision Support Systems must provide the required results in desired time. The response time must be very short in a context of disaster - of the order of some seconds. Because of the fact that every second counts in a disaster, decision support system functioning must be real time. In fact a Decision Support System may go unused if the manager cannot get the information in a timely fashion[25];
- Geographic distribution: The interest of geographical distribution is to avoid complete paralysis at the occurrence of large-scale disaster. Geographical distributed software is less vulnerable than those in one place. To be distributed, the Decision Support System could be based on the client/server functioning or on Application Service Provider (ASP). Most geographically distributed applications are based on Client / Server functioning. In such situation application is often on Internet. Client sends requests that are processed by the server. The result is then transmitted to the client. A variant of the client-server process is the use of Application Service Provider (ASP). In this case, requests are sent to an agent who makes the connection between the client and the server. After the request processed by the server, results are sent directly to the client.

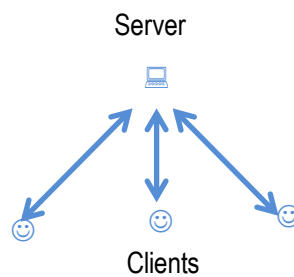


Figure III-9: Client-Server functioning

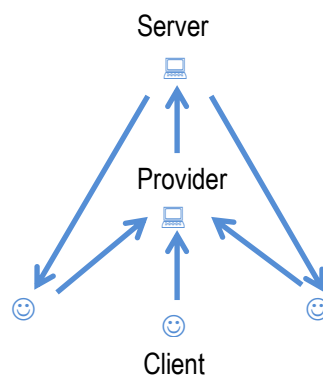


Figure III-10: Application Service Provider functioning

The architecture of the designed Support System in this thesis will be based on the client/server architecture. This one is less vulnerable in a natural disaster situation because of the fact that the Decision Support System is not located on the decision maker's computer;

- Views: The system view for a given user is his way to see functions or to access to treatment. The system must be able to manage multi-views by taking into account users' profiles. In instance, for some users, it will consist in being informed about the vulnerability of a specific region;
- Ease of use: One of the software disposal causes is the difficulty of getting started. Simplicity implies an easy, fast, intuitive and handy - especially in crisis management. Ergonomic aspect plays a significant rule in the software use frequency. Ergonomic will encourage decision makers to use the software in the simulation phase. The acquired use habit will help them to be more reactive in the crisis management. Hence, Decision Support System is designed to be evolving as the user becomes more familiar with the technology and to be interactive and controllable [25];
- Portability: Emergency devices are not immune from destruction in major disasters. Neither is the server that hosts Decision Support System. At the time of the internet and smart phones, the application must be multi support for efficiency. It must run on maximum support: laptop, touchpad, smart phone;
- Adaptability: In III.1.1.1 we have identified several phases in the crisis management. The decision support system must be deployable during all these phases. It must be designed to meet new demand [25];
- Efficiency: The cost is the primary cause of software engineering projects abandonment. Cost analysis must be performed and updated along the project.

Whatever its characteristics, Decision Support System categorization can be performed according to three views: The nature of the decisional problem, the number of users, the technology generation. From the decision problem nature point of view, according to Donovan and Madnick (1977) quoted by [15] Decision Support System is divided into two categories:

- Decision Support System for structured problem;
- Decision Support System for semi-structured problem.

From this point of view Decision Support System in the disaster management is in the category of semi-structured problem. Indeed, for the Decision Support System proper functioning crisis must be prepared in advance. But anyway, the feared event occurrence always causes decision context deconstructing. From the number of users point of view, [134] pointed out three categories of DSS:

- Single user Decision Support System;
- Group Decision Support System;

- Organizational Decision Support System.

From this point of view, we argue that Decision Support System must be an organizational one because of the fact that a crisis management involves several institutions. From the Decision Support System generation point of view, [132] pointed out Data Oriented Decision Support System and Model Oriented Decision Support System. These categories are completed by [15] and [135].

- Data oriented Decision Support System;
- User Interface oriented Decision Support System;
- Model oriented Decision Support System;
- Knowledge oriented Decision Support System;
- Communication – based Decision Support System;
- Document-driven Decision Support System;
- Web-oriented Decision Support System.

Model-Based Decision Support System is based on stages. [120] have identified three of them: Formulation, Solution, and Analysis. For these reasons, we argue that Decision Support System for infrastructure network vulnerability analysis must be data oriented and/ or Model oriented.

Above characteristics lead to some risks in the project. These risks are described in the following section.

### III.1.7 THE RISK OF THE PROJECT

Decision Support Systems can have many objectives. Some of them are designed for specific purposes. The others seek a wide audience. Many processes outside the engineering one are imbricated to meet the objectives. Software engineering is then a complicated project. It demands skills in several areas and contain numerous types of risk. Risk is located at all levels: programming, project management etc. The above identified risk management must be integrated into all phases of the project.

- Financial: Financial risk is the risk of exceeding the initial budget;
- Temporal: Time overrun risk is due largely to poor planning. Milestones and deliverables must be defined for each phase;
- Human: Major failure risk is located at the human level. For the user, we can face resistance to change. Then, the final product could not be accepted. In addition, the developer himself might misunderstand specifications or lack required competences. Managers must incorporate change management and training at the beginning of the project to manage human risk.
- Technical: Technical risk is related to software reliability and performance. It also includes coding, maintenance and quality problems.

The diversity and apprehension complexity of these risks justified the projects high level of failure. Decision Support System engineering must respect some process to minimize or eliminate these risks. The following section presents a process used to design our Decision Support System.

### III.1.8 SOFTWARE ENGINEERING PROCESS

Decision support systems are a specialisation of computer systems [15]. For this reason, Decision Support System engineering process is part of the software engineering one. The adopted development process in this thesis is based on engineering approach pointed out in [136]. The overall development process is divided into several sub-processes: development, project management, change management, update and maintenance. These processes are presented by the Figure III-11. Each process consists of non-linear multi-steps.

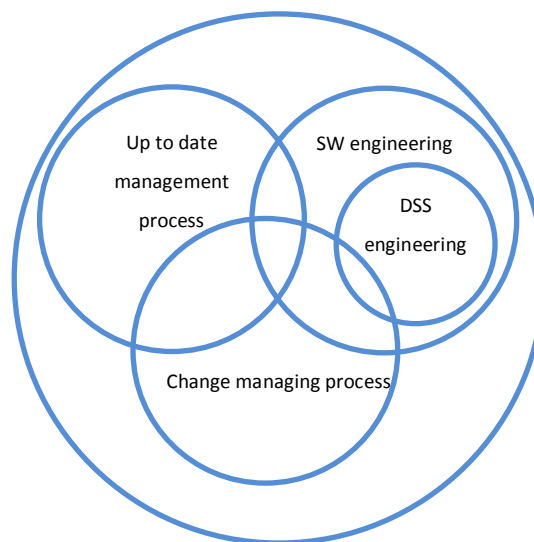


Figure III-11: Processes

- Project management: The process management process encloses other processes and specifies them. It defines the execution time and allocates budget;
- Development: Development is the coding process itself. It is the process that manages the software development;
- Change management: This process defines necessary change needed to accept the application;
- Update and Maintenance: Update process integrates the new laws, life mode changing, emergence of new technologies, new user requirements etc.

The objective of this section is to provide a process for the design of a Decision Support System for natural disaster crisis management. The resulting process is based on the literature review. In the following are presented those which inspired us: the waterfall model, the prototyping model and the spiral model.

✓ *Waterfall model*

---

The specificity of the waterfall model is the step organization. Those are organized sequentially (linear). Waterfall model is based on a continued document-driven milestone approach [137]. That means that every step takes as an input (validation criteria) from the output of another step etc. At the end of each step is provided deliverables in standardized formats: Plan, feasibility report, design document, source code, and review report. This model is particularly suitable for structures with staff high mobility.

The main problem in waterfall model is its linearity. Indeed, the output and the specifications of one step are assumed accurate and usable for another one. Furthermore, the model assumes that the specification is stable. This is not always the case.

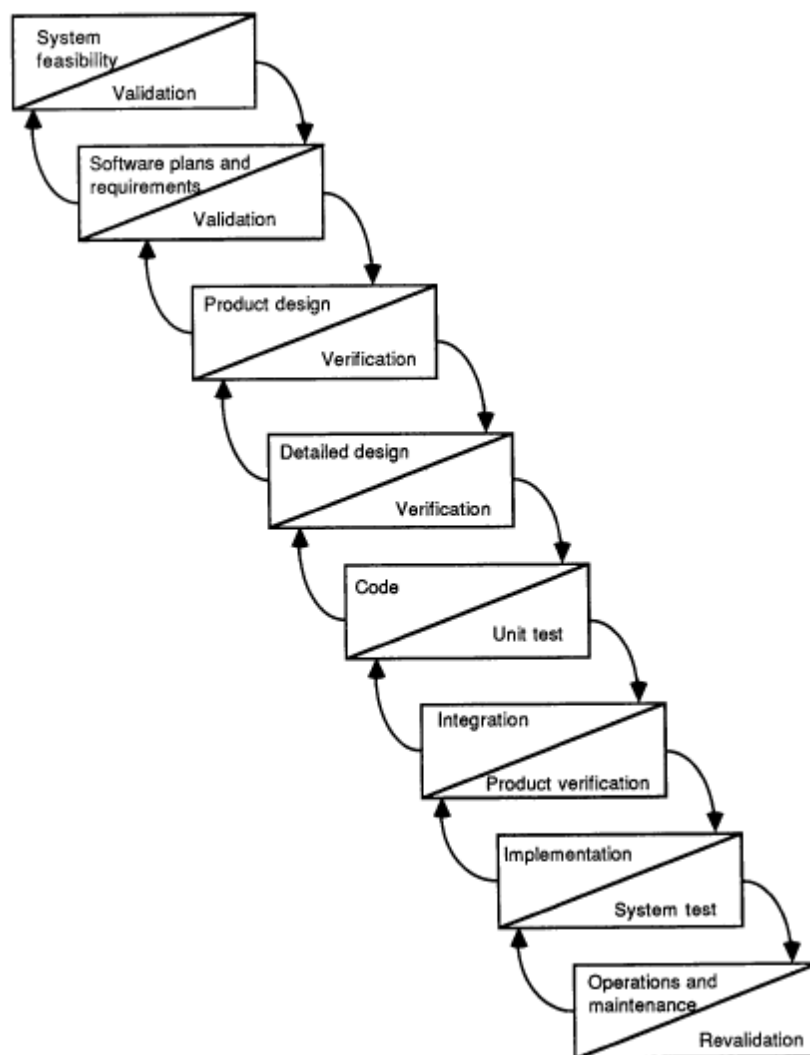


Figure III-12 : Water-fall model by [138]

Figure III-12 shows water-fall diagram proposed by [138]. It shows the linearity of the model. In such a model a mistake at one step could have high consequences on the other steps in term of error cost.

### ✓ Prototyping model

The idea of the prototyping model is to focus on the prototype development instead of the final model [136]. The prototype is then developed and presented to the customer according to the producer understanding. This method allows achieving an enhancing version through trade or by a further analysis of specifications. The prototype model requires a lot of exchanges between the parties involved. It involves a lot of iteration and versions. Those are expensive and impact on the realization time.

### ✓ Spiral Model

Spiral model implementation is operated by cycle [138].

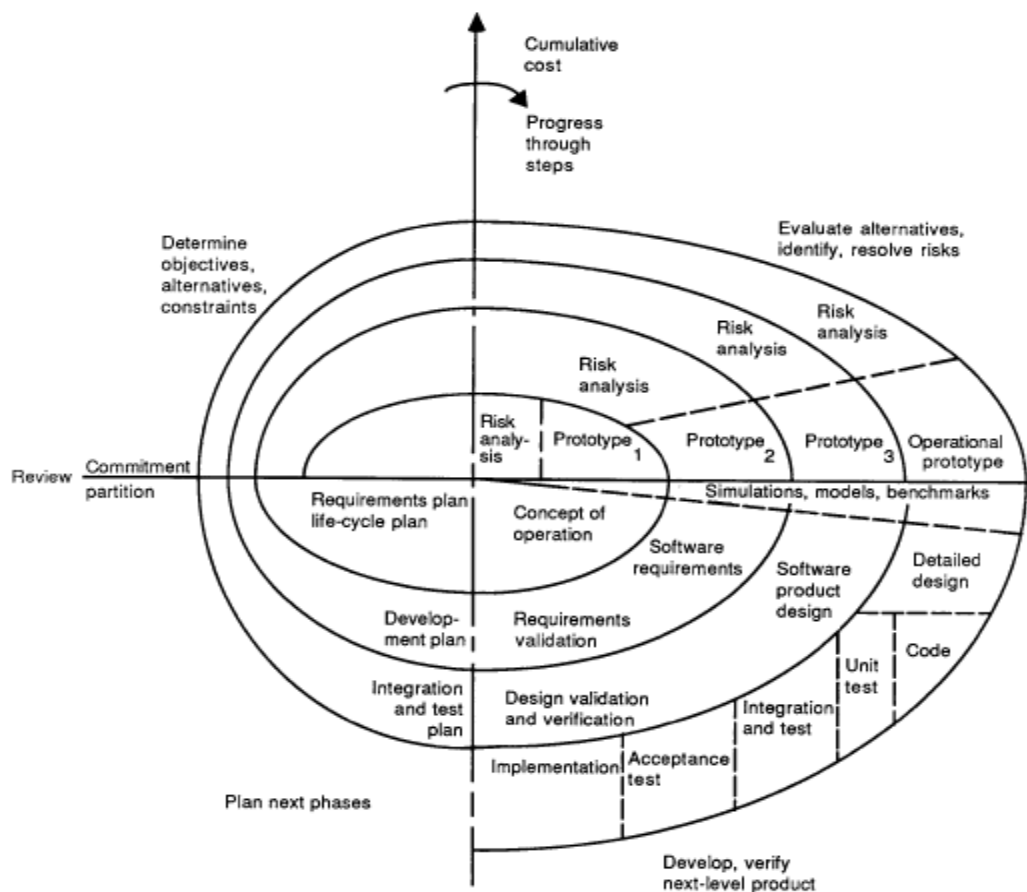


Figure III-13: Spiral model by ref [138]

In the Figure III-13 each cycle is divided into four quadrants: Determination of objectives and alternatives, assessment of alternatives and risk identification, definition of the implementation from the risks, planning the next cycle. Spiral model is a risk-based model.

There are other processes in the literature such as the cycle in V, the 2TUP etc. Given the diversity of method, we present ours for Decision Support System engineering process. It is a mix of linear and cyclic processes.



✓ *Adopted process*

From these previous processes and the engineering approach we propose a Decision Support System engineering process. Like every process, the goal is to produce required software for users. It is composed of many sub processes including analysis, design, construction, and implementation [121]. It includes many steps not necessarily disjoint. Figure III-14 presents adopted steps to design our Decision Support System.

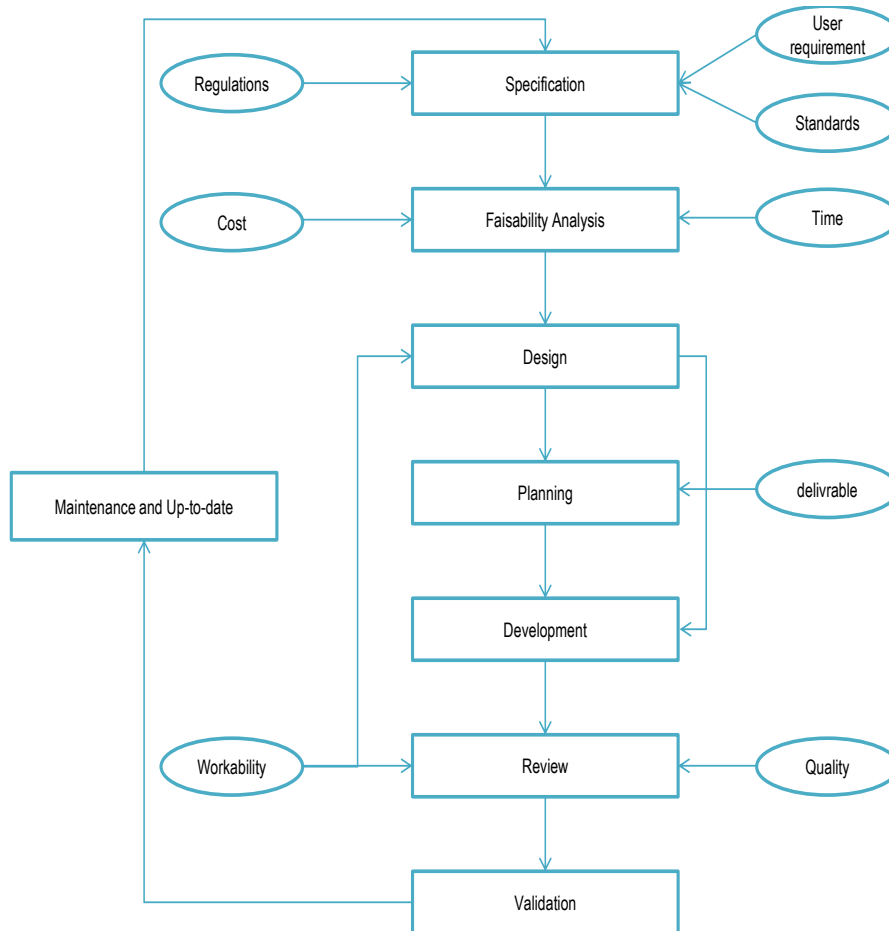


Figure III-14: The process of developing a DSS for vulnerability management

- Specification: The specification step consists in the establishment or/and interpretation of client needs. The data collection is an important action for the specification. The context is targeted in order to better define problems and objectives. Main features are deduced from rules and business constraints. The final specification document determines responsibilities, resources etc;
- Feasibility analysis: The feasibility analysis is based on elements provided in the previous step. It aims to estimate allocated resources, to determine costs, implementation time, required effort, used technology and risks. It naturally leads to identifying versions and delivery dates;
- Design: The design is the technical modelling. This step reflects implementation models. Modelling may have more or less fine granularity and depend on the field. We argue that lower-level modelling must be adopted at the expense of a high-level modelling. There are three main areas in the design

of Decision Support System: data, function, and Human Computer Interface (HCI);

- Planning: Planning aims to determine milestones in the realization of the application;
- Development: Development is the phase of application coding;
- Review: The review encloses set of testing operations, assemblage and integration. The importance of the test phase is to ensure the coherence of functions compared with the specifications;
- Validation: Before integration the model must be validated. Validation differs from the review by the fact that it is carried out jointly with the customer. At this step there are estimated tangible and intangible benefits as well as the system lifetime. [66] presents two major criteria for validation;
- Theoretical significance: the method used must be meaningful in terms of used information;
- Operational meaning in the sense that the client must be able to understand and use the model results.

Maintenance and updating: Maintenance and updating phase is continuously performed along the software life. It allows among other the integration of new features following customer's need evolution. Each of the steps is a grain of the process.

Figure III-15 presents different elements included in every step. They must be defined unambiguously and repeatable. The repeatability of a step is crucial insofar as it is not immune from errors.

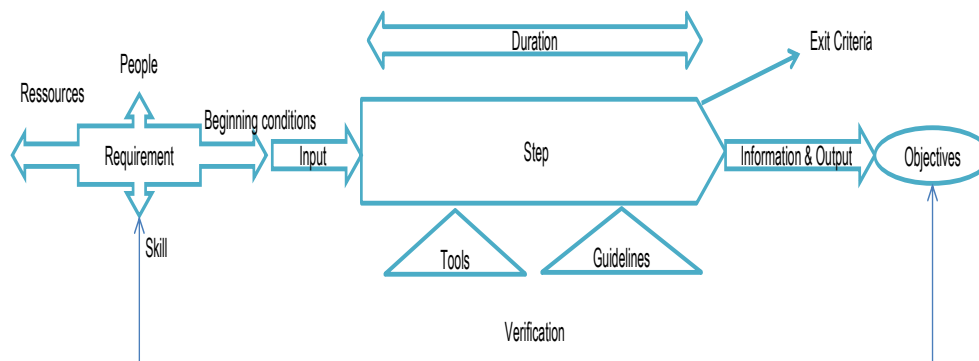


Figure III-15 : Step

Each grain has starting condition and exit criteria. It is based on identified methodologies, specifications, standards and business rules. A grain lasts a certain time and requires resources, men and skills.

In the next section we are presenting the design step shown in Figure III-14 applied to the context modelling.

### III.1.9 CONTEXT MODELLING

To design the future decision support system, the working context has to be modelled. For the modelling need, we used an object approach. There are several graphic formalisms related to object modelling: the

binary model NIAM (Natural Language Analysis Method), IDEF1X (Integration Definition for Information Modeling), UML (Unified Modeling Language). UML is designed to represent, specify, construct, and document software systems. It allows building several models of the same system. Each model highlights one aspect: organizational, functional, static and dynamic. Any system designed in UML is then composed of interacting objects. According to their behaviour, object will perform specific operations. Otherwise UML allows generating automatically a part of the code. For those reasons UML is chosen for the context modeling. Many UML tools are available: Rational Rose, MagicDraw, MEGA Designer, Modelio, Objectteering, PowerDesigner, Visual Paradigm, Win'Design, StarUML, argoUML, boUML, Together, Poseidon, Pyut, Umbrello etc. Our choice has been StarUML [139] because it is free and open source.

The methodology used in this thesis is inspired from those presented [140]. This approach included actors identification, building the static context diagram, relationships between use cases, use cases for human actors, sequence diagrams and activity diagrams. Those are presented in the next sections.

### III.1.9.1 IDENTIFICATION OF ACTORS

An actor is an external person or a process that interacts with the system. An actor gets observable result from the system while a secondary actor is asked for further information. Actors can be human or connected systems. Several kinds of actors are identified: International, National, Regional, Infrastructure Manager, Local Operator, Emergency, Citizen and the Analyst. For each of them several use cases are defined. In a general way, we defined 14 scenarios. Figure III-16 shows all the human and non-human actors. The role of every actor is defined in the following:

- International: Vulnerable area, network;
- National: Vulnerable network;
- Regional: Vulnerable area, network;
- Infrastructure Manager: Vulnerable network, area;
- Local Operator: Vulnerable component;
- Emergency: Vulnerable component, stake, area, failure time, feared event;
- Citizen: vulnerable area;
- Analyst: the analyst is the actor who can do everything.

Because of the fact that the Decision Support will be used by many persons at the same time, it is interesting to know the number of each actor connected to the system. The static context diagram in the next section will give this a view on the connected user number.

### III.1.9.2 THE STATIC CONTEXT DIAGRAM

The static context diagram is not a standardized UML diagram. It allows specifying the number of actor instance connected to a system at a given time. For example many citizens could connect to the system to know the vulnerability of their regions.

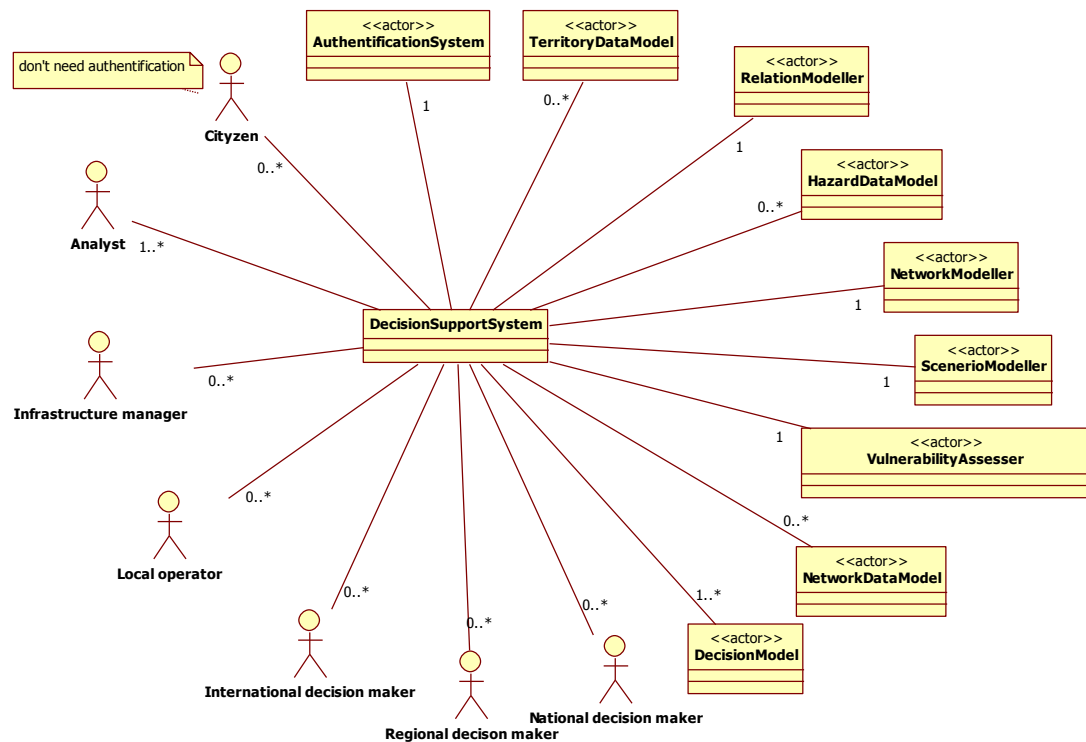


Figure III-16: Static Context Diagram

Figure III-16 shows also non-human actor like the vulnerability assessor. Those will be implemented during the coding phase. Every connected user can interact with the system through use cases. These have been identified and the relation between them is given in the next section.

### III.1.9.3 THE RELATIONSHIP BETWEEN USE CASES

A use case is a visible functionality for an actor. It represents provided service by the system, without imposing the implementation mode of this service. For a use case there are two specifications: the first is a functional view described by sequence or activity diagrams. The second is a technical view described textually.

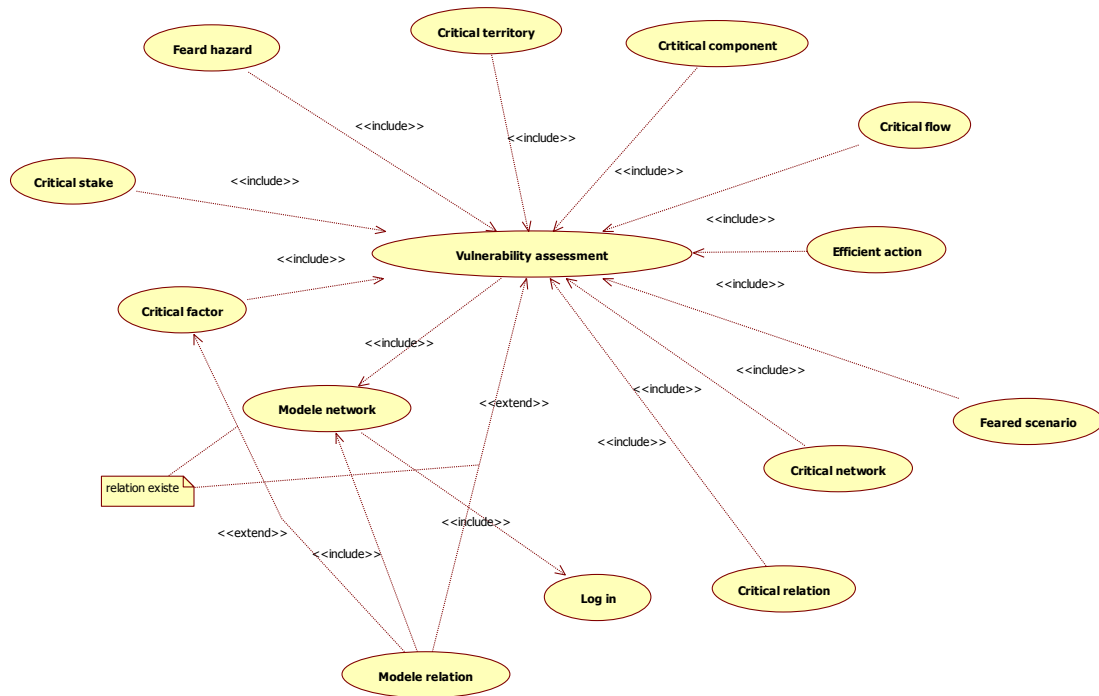


Figure III-17: Relation between use cases

Figure III-17 shows the relationships between use cases. For example the network modelling includes those of relations. The latter may be an extension of the vulnerability estimation. The next section shows the use case for human actor.

### III.1.9.4 USE CASES BY HUMAN ACTOR

The use cases by human actor specify actions to be performed. The example in Figure III-18 shows that a local actor can determine among other critical components, effective actions, feared events etc.

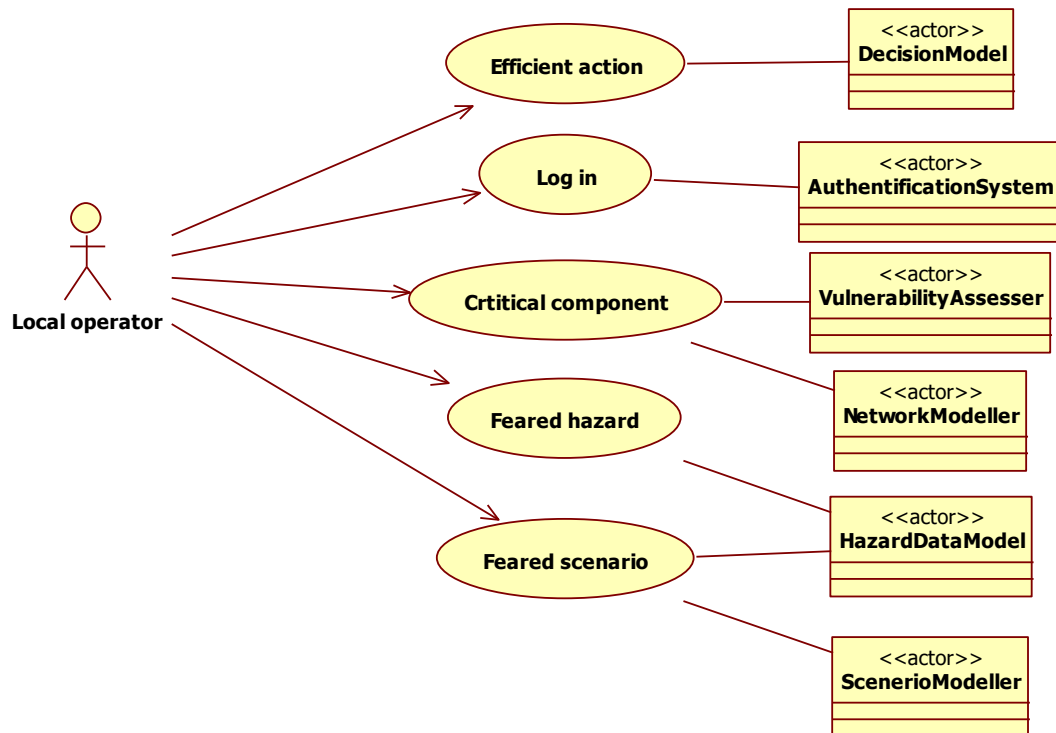


Figure III-18: Use case for local operator

The critical component determining is shown in Figure III-18. It calls upon vulnerability assessment and network modelling. For every use case, we had determined the sequence diagram presented in the next section.

### III.1.9.5 SEQUENCE DIAGRAM OF USE CASE

Sequence diagrams are used to illustrate use cases temporal aspects. Sequence diagram is usually related to the system function (i.e. a use case). For each use case, we represented a sequence diagram. Figure III-19 shows the sequence diagram in the vulnerability analysis by a human actor.

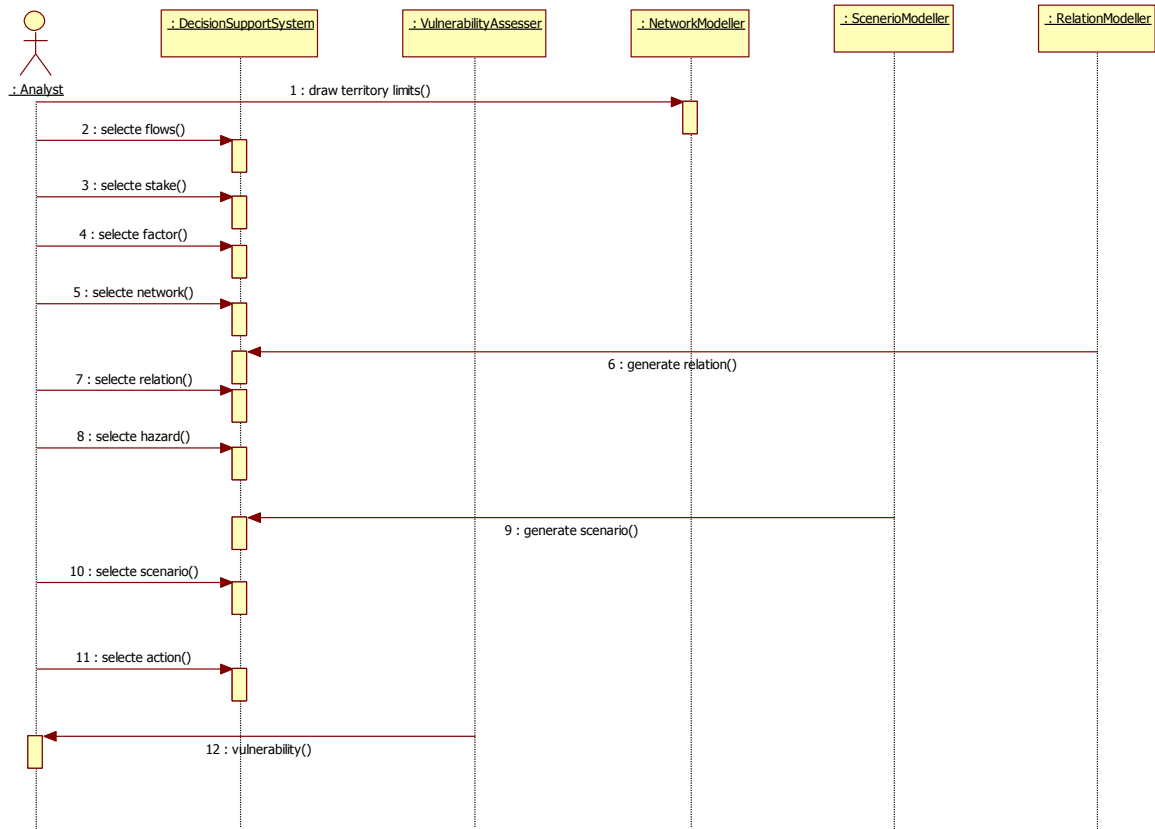


Figure III-19: Sequence diagram for vulnerability analysis

The analyst begins by drawing the network. Afterward he will select elements of the system. The DSS will generate then interdependence, feared event scenario and vulnerability.

To complete sequence diagrams, activity diagrams are used. They are presented in the next section.

### III.1.9.6 ACTIVITY DIAGRAM BY USE CASE DIAGRAM

Sequence diagrams show only the nominal use case. Functioning particularities representation could be harmful for the chart readability. That is why we used the activity diagrams in addition to sequence diagrams.

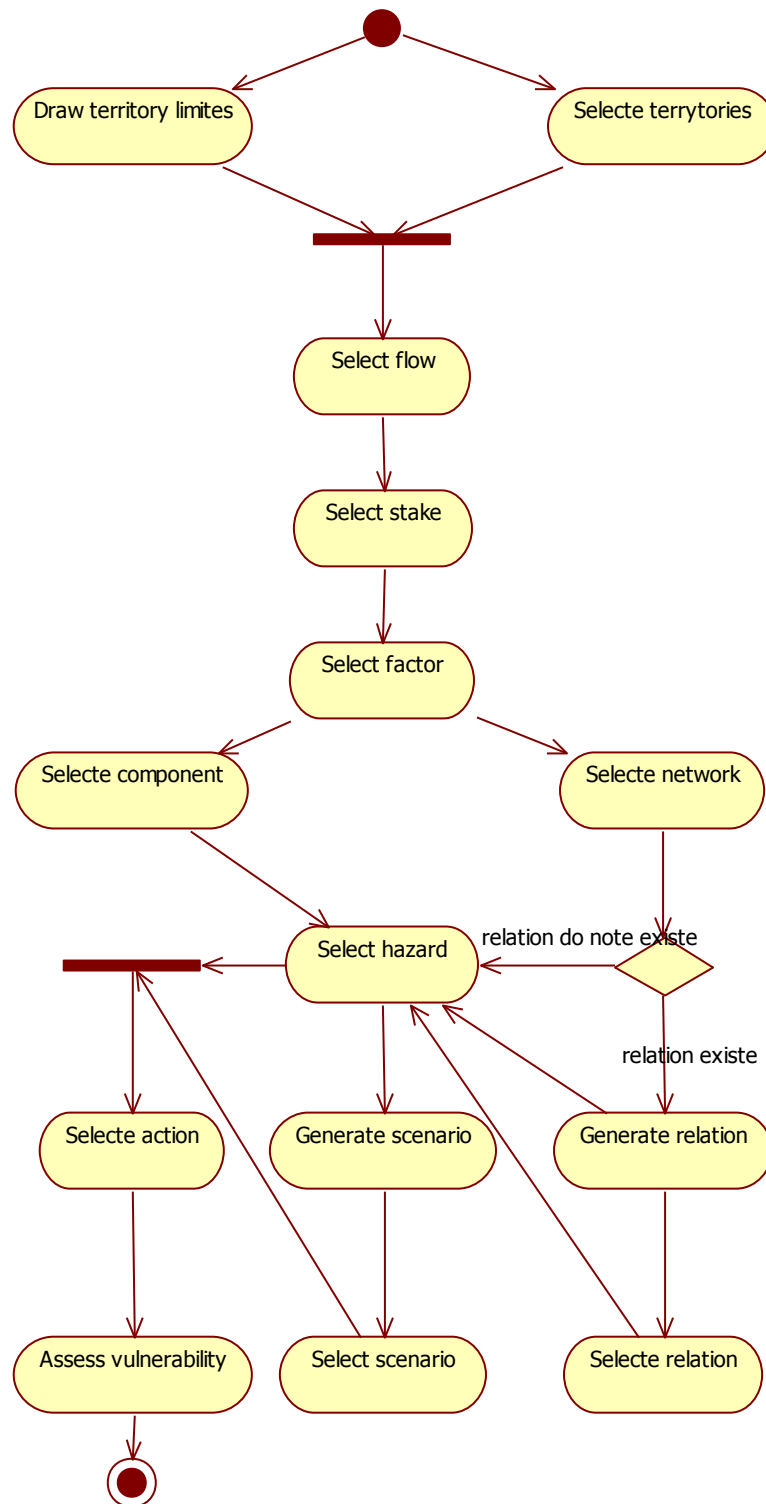


Figure III-20: Activity diagram for vulnerability analysis

Figure III-20 shows the activity diagram for the use case vulnerability analysis.



The modelling itself relies on a process. Concerning UML, there are two relating approaches: The RUP (Rational Unified Process) and the MDA (Model Driven Architecture):

- The RUP is a method for object-oriented software development. It is an implementation of the Rational Unified Process society method. It consists in set of guidelines to produce software from specification. Each directive defines who is doing what and when. The RUP is driven by use cases. These are used to analyse the project requirements. The commercial product is provided in the form of a web site reserved for Rational SoftWare customers.
- MDA is model-driven architecture. The objective of the MDA is the design of systems based on single domain modelling by ignoring technological aspects. It is a software realization process based on business models.

There are also other methods such as the Larman agile methods (Extreme programming, Dynamic software development method (DSDM), adaptive software development, Feature driven development, Crystal clear). An agile method is a method of software development which involves maximum customers. The concept was born of a manifesto signed by 17 personalities, methods creators and company executive.

None of this model was applied in this project. These processes suit better long term projects involving many people and/or organizations.

The architecture of the system is determined after the modelling. Adopted architecture for the designed Decision Support System is presented in the next section.

### III.1.10 ARCHITECTURE

The architecture adopted in this thesis for the Decision Support System design is those proposed by [121]. This architecture is composed of three parts: Human Computer Interface, Data base, and Model Base. [25] added to these parts a data analysis capability. In our approach this module is managed by the database management system. In some situations, a spatial Decision Support System can be endowed with prominent spatial components [26].

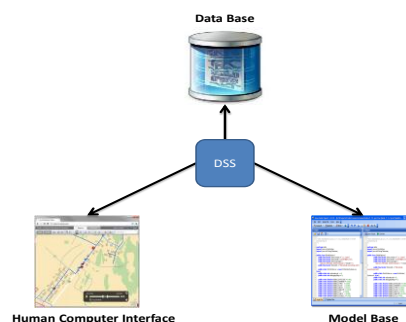


Figure III-21: Decision Support System structure by [121]

Figure III-21 represents the architecture proposed by [121]. Database is endowed with data analysis capability performed by a data base management system (DBMS). The Model Base is related to a normative model implemented in a Model Based Management System (MDBS): It allows giving unobtrusive solutions and evaluating tradeoffs between actions, and possibly providing those to be implemented. The Human Computer interface is related to a Dialogue Management System.

The next three sections describe the architecture elements of the designed Decision Support System.

### III.1.10.1 THE HUMAN COMPUTER INTERFACE

The Human Computer Interface represents all windows accessible to users. It allows interaction between decision makers and the other components. Three steps have been followed for the design of the Human Computer Interface: The prototyping, the design and the management.

- Prototyping: There are several tools for Human Computer Interface prototyping: UI Stencils, Dot Grid Book, KeynoteKungFu, Balsamiq, Axure RP, Mockinbird, MockFlow, FlairBuilder, MasterPages, Fireworks, DaftBoard, Notable, ConceptShare, DraftBoard. Among these tools Axure seems to be the most complete and professional. We used Balsamiq because it is easy to use [141]. The Figure III-22 presents the prototype of the feared event panel.

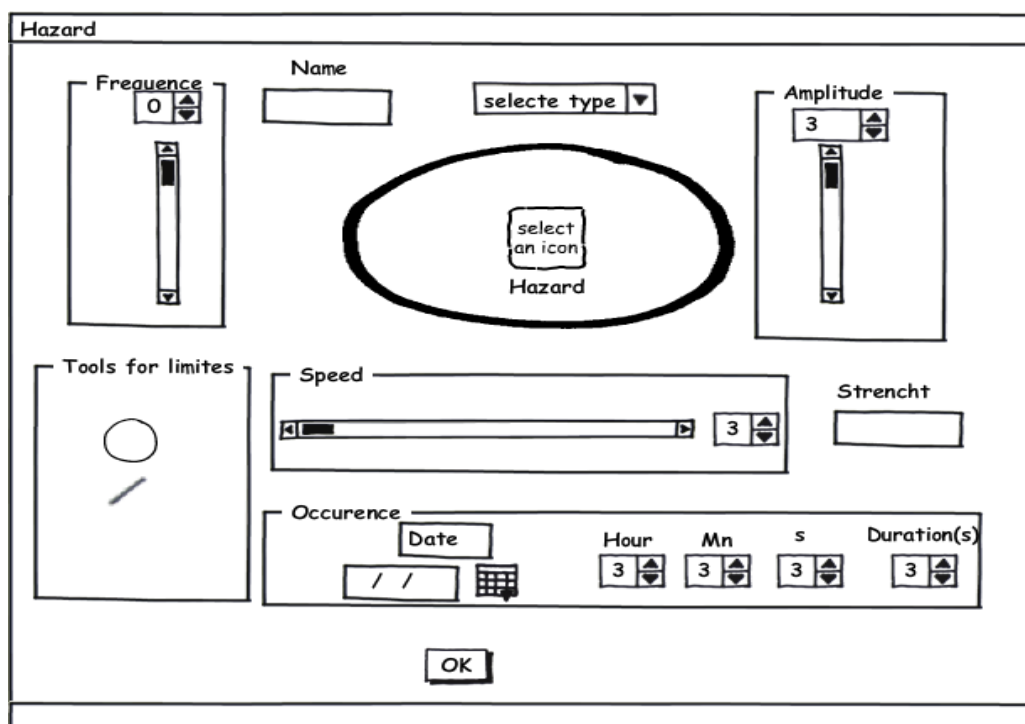


Figure III-22: Human Computer Interface with Balsamiq

- Designing the Interface: The next step was to build the Graphical User Interface by using

WindowsBuilder - an Eclipse IDE plug [142]. The choice of WindowBuilder was also motivated by its simplicity and the fact that we have chosen Java as a development language.

- The dialogue management system related to the Human Computer Interface is implemented through Java Classes.

The Decision Support System developed is composed of nine panels:

### ✓ *Connexion*

---

The identified actors might log in via the log in panel shown by Figure III-23. Every type of actor can perform specified manipulation in the Decision Support System. Those are defined in the modelling phase by the use case for human actors. This page gives the access to the other functionalities of the application. There are 8 user's profiles (International, National, Regional, Infrastructure manager, Local operator, Citizen, Emergency, and Analyst). Profiles are created by the analyst. A usual user can only create a citizen profile which has narrow access to the application's functionalities.

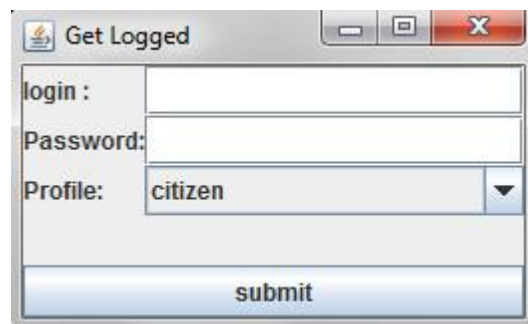


Figure III-23: Log in Panel

### ✓ *Import*

---

The software enables the user to import a map as a picture or to select an area from a real map (using Google maps for example). Then, specify the boundaries of the geographic area to work on. If the user doesn't find a map, the software offers the possibility to draw the territory and represent it by its boundaries on the zone. Territories are resizable (zoom, changing the boundaries, extension...).

### ✓ *Drawing*

---

If data are not available in the specified format, the analyst might draw needed element on the drawing panel shown by Figure II-24. He/she can draw networks, place feared events, factors, flows etc;

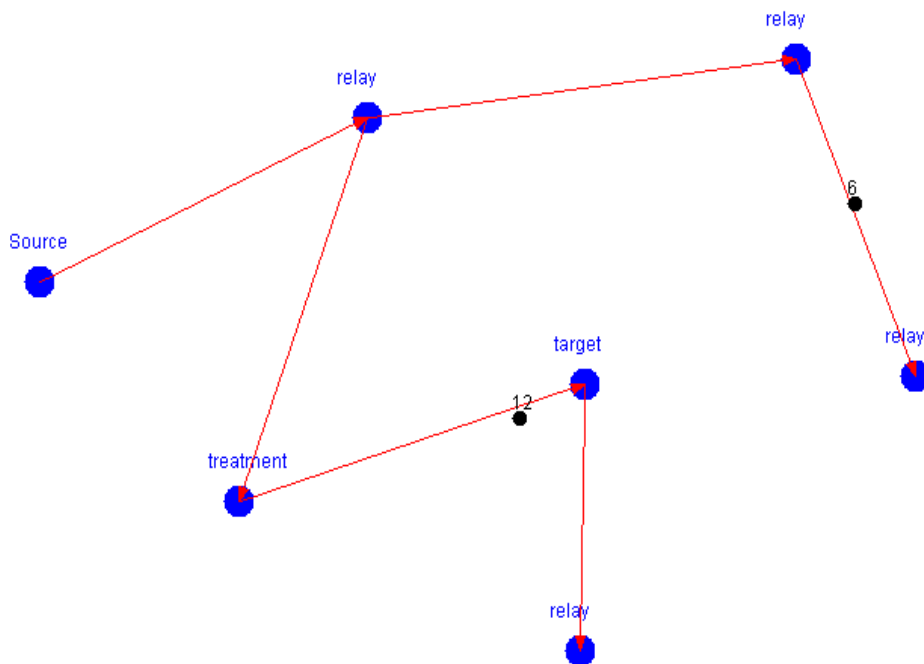


Figure III-24: Network drawing

#### ✓ Parameter filling in

Component attribute are available via this panel (Figure III-25). The user can change every parameter if needed according to his right. The user can specify the settings for each item in a separate window.

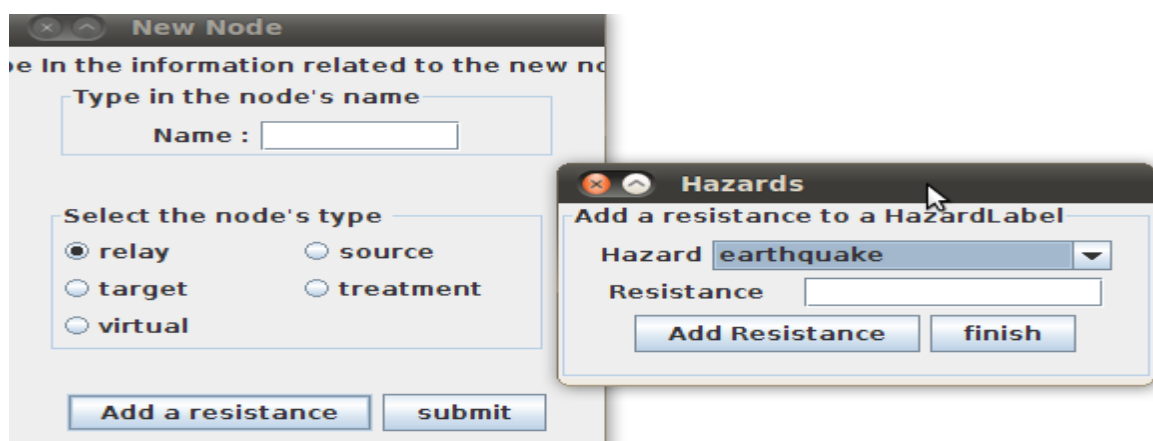


Figure III-25: Node Parameter

✓ *Simulation*

---

The simulation panel allows the user to specify simulation parameters like the time, the step. The simulation panel displays the behaviour of the system during the simulation. The user can stop the simulation at any time.

✓ *Calculation*

---

After the simulation, the calculation result is displayed in this panel. The user can visualize his need by selecting the format of the result. This format could be a graph or a table.

✓ *Decision*

---

According to the result, the user can take some actions to change one or more elements.

✓ *Final Recommendation*

---

The final recommendations come from the decision process and are displayed on the recommendation panel.

✓ *Data base*

---

In the database panel; the user can request much information about the database.

Information provided by the user will be stored in the database presented in the next section.

### III.1.10.2 THE DATABASE

Decisions emerge from the processing performed on data located in a database. For this reason, Decision Support System performance is correlated to those of the database. Data may take various and varied forms (digital, paper etc). Its description is therefore essential before the system engineering. Database management and manipulation is usually performed through a database management system (DBMS). A data manipulation language can be superimposed to the system to facilitate consultation, update, and delete operations. Database Management System is generally related to a description model.

The most adapted to the context of this thesis seem to be the relational model and the object model. The next two sections present these models before justifying the chosen approach.

### ✓ *The entity relationship model*

---

Entity relationship model is based on the real world description from concepts of entity and relationship. The entity represents a real world object. Entities have properties used to describe them. These are called attributes. Relationship is a link between entities.

Entity relationship model was proposed in 1970 by E. Codd to resolve hierarchical and network models limitations. It is based on set theory and relations and is adapted to a functional point of view. We are then interested in what is made by the system at the expense of how it makes it. Data treatment is not described by this model. It ensures data independence compared to the program. It is part of the MERISE method that is a more generalized method. There are three main levels in the model entity relationship model:

- The conceptual level: The conceptual level describes entities of the domain, and the relationships between these entities. The conceptual level gives rise to the entity relationship diagram which presents the system from the data point of view;
- The logic level: The logic model reflects the conceptual model in suitable implementation formalism. It leads to the relational model;
- The physical level: The physical model translates the concrete way of how the model is implemented into the selected Data Base Management System.

### ✓ *The object model*

---

An object is an identifiable entity in real word. It is the equivalent of a class in the entity-relationship model. Any object has a set of attributes, its structure and a set of methods, i.e. its behavior.

In this thesis we used an object approach to model the database. This choice is motivated by the fact that the object approach allows to represent treatments performed on data in addition. The UML class diagram has been then used to model software data. The discovery of objects in the system can be done either by use case diagrams breakdown or by data-driven decomposition. The data driven decomposition is used in this thesis. This approach was used because of the fact that we were the analyst and the client of the study.



Figure III-26: Class diagram with StarUML

The database has been modelled by 29 classes. The Figure III-26 presents an extract from StarUML. We can distinguish the feared event, the stake, and the flow. They represented the fact that flows are consumed by stakes. At the occurrence of the feared event, flows or stake could be affected. The overall model is presented in the annexe.

Several tools for database management exist: DB2 (IBM), Visual FoxPro (VFP), Access (Microsoft), Oracle (Oracle Corporation), MySQL (open-source).

### III.1.10.3 MODEL BASE

The model base is composed of the vulnerability model presented in Chapter II. The reader is invited to see that chapter for more information.

### III.1.11 CODING

Based on the infrastructures, the Decision Support System started in the DOS and UNIX environments around the late 1970s and then moved to windows in the early 1990s [120]. The development of the application can be done using several approaches: programming 'in line', event-driven programming, procedural programming, object programming. The object approach requires modelling the context before designing. This solution was chosen because it is compatible with the context modelling and the database design.

We have chosen Java as language development because of its portability. In addition, Java is free and can run on different computers such as PC, MAC without any change. It was fully implemented by using swing as an API for graphics and JUNG to represent the network [143].

### III.1.12 DSS FUNCTIONALITIES

In the literature there are several Decision Support System for disasters management. Their applications are related to many disciplines: pollution control, water resource management, flood, forecasting, prevention of epidemic etc [15].

Table III-10 gives a recapitulative given by [118] completed by those of [15].

<i>Name</i>	<i>Author</i>	<i>Environment</i>	<i>Complements</i>
NIMPRO (Network Interdiction Mitigation and Protection)	[26]	VB 6	MapObjets 2.4 ILOG CPLEX 10.0 GIGASOFT ProEssentials 5
TELEFLEUR (TELEmatics-assisted handling of FLOOD Emergencies in URban areas)	NATIONAL OBSERVATORY OF ATHENS		
L-THIA (Long-Term Hydrologic Impact Assessment)	Purdue University, United States of America		BDD Oracle Web Technology, Code PERL
The proDEX (complex environment pollution issues)	University of Ljubljana, Slovenia.	Pyhton	GIS Architecture, Distributed relational database



TELEFLEUR (TELEmatics-assisted handling of Flood Emergencies in URban areas)	NATIONAL OBSERVATORY OF ATHENS		
L-THIA (Long-Term Hydrologic Impact Assessment)	Purdue University, United States of America,		
The proDEX system (nvironmental protection, air and soil pollution control)	University of Ljubljana, Slovenia	Pyhton	

Table III-10: Decision Support System in the literature

None of these systems take into account the vulnerability calculation in a generic way. The Decision Support System for Interdependent Network Vulnerability Analysis realized in this thesis is different from existing systems. It contains an ergonomic graphical user interface which allows the user to choose different possibilities depending on his rights. The main functionality of the VESTA are summarized by the Figure III-27.

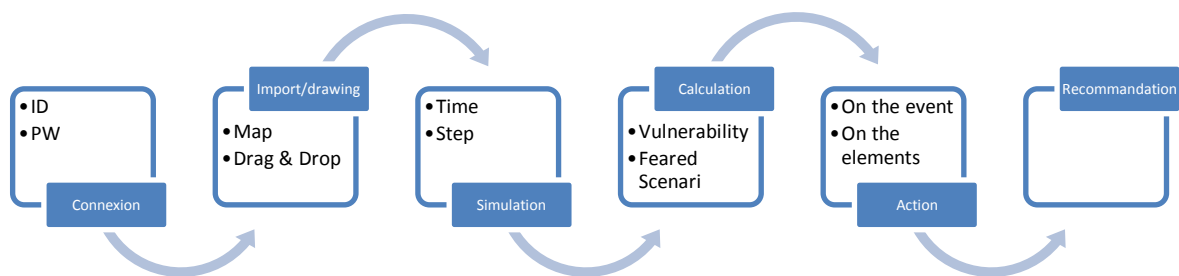


Figure III-27: Functionalities of VESTA

The simulation time is given by the analyst. He/She can rely on the feared event characteristics to assess this time. The DSS is adapted to phases before the crisis. The connection, import, simulation and drawing have been presented in the III.1.10.1. The next section presents the system possibility related to vulnerability assessment.

### III.1.12.1 PARAMETER CALCULATION

VESTA is able to calculate vulnerability parameters of one element. The parameter could be the intrinsic vulnerability, the resilience, the robustness etc. The concerning element could be a network component, flow or stake. The result is displayed in form of histogram.

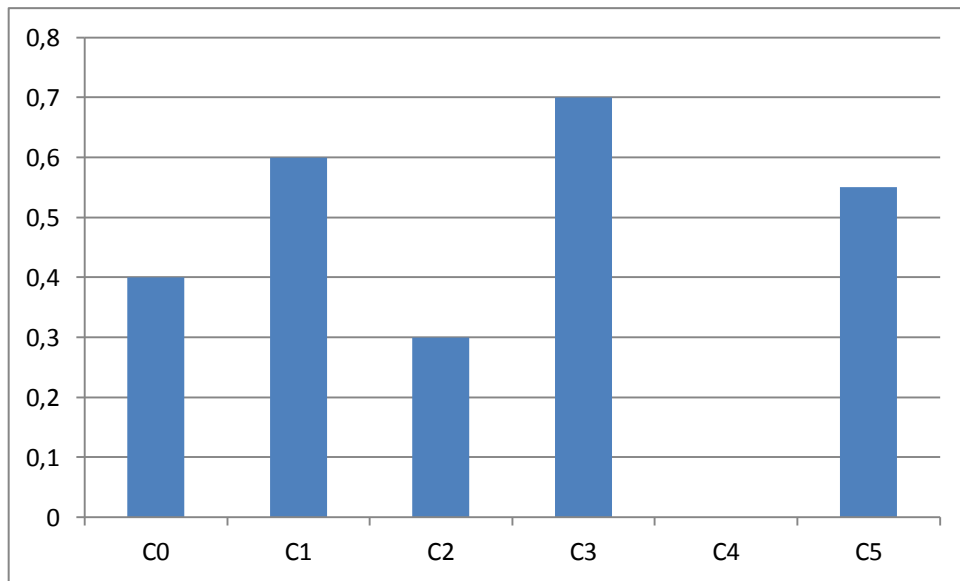


Figure III-28: Parameter calculation

The Figure III-28 represents the vulnerabilities of six components. The user could also select more or less components. The displayed parameter could be different from the vulnerability and could be resilience for example. It shows that the component C4 is less vulnerable for the feared event. Otherwise C3 is the most vulnerable.

### III.1.12.2 EVOLUTION OF THE PARAMETER

The Figure III-28 shows that the component C3 is the most vulnerable one. The user can visualize the evolution of this parameter in the simulation time.

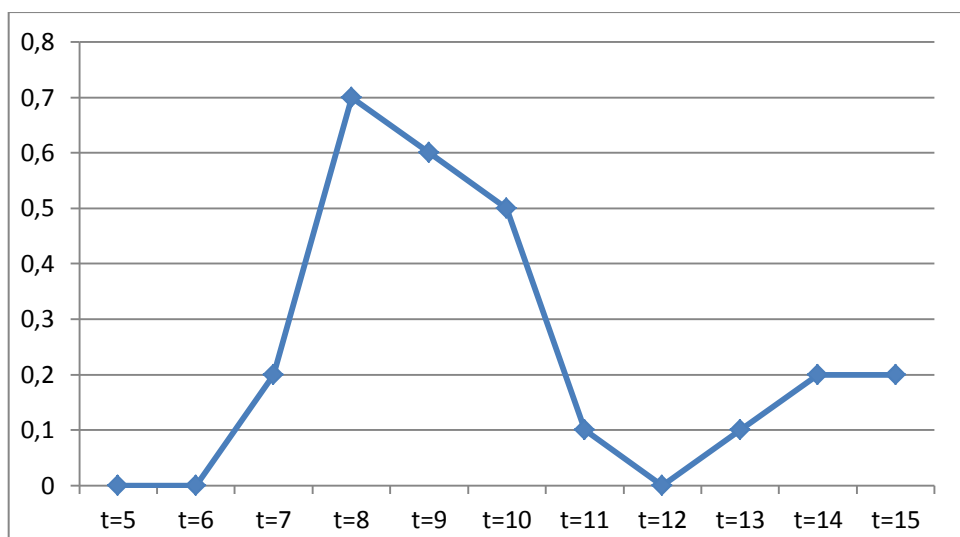


Figure III-29: Evolution of a parameter

Figure III-29 shows the evolution of the vulnerability of the component C3 from the instant 5 to the instant 15. We can then analyse what states lead to the maximum vulnerability.

### III.1.12.3 FEARED EVENT OR SCENARIO

One of the aims of vulnerability analysis is to determine feared events and scenarios. The DSS is able to build a histogram of scenario about one parameter of selected component.

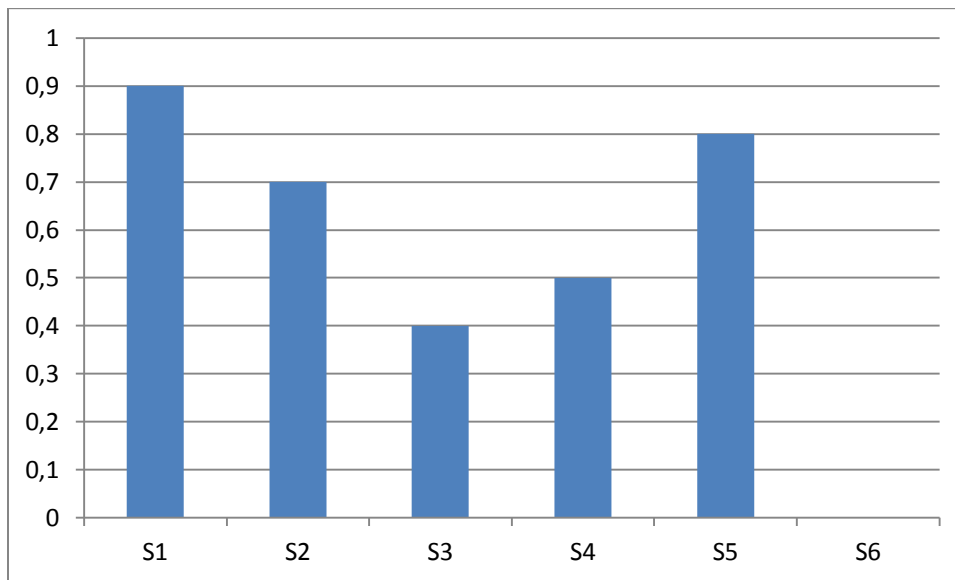


Figure III-30: Feared event or scenario

Figure III-30 presents the resilience of the component C3 for six scenarios. It shows that S6 is the worst scenario in term of resilience for this component. Indeed for this component, the resilience is zero. On the contrary, this component is very resilient to the first scenario.

### III.1.12.4 THE FEARED EVENT OCCURRENCE POINT

The consequences of feared event often depend on the societal position of the occurrence place [117]. The vulnerability and other parameters depend on the occurrence point of the feared event. VESTA can for one component specified parameter show on the map corresponding values.

Figure III-31 shows for the component C3 the vulnerability according to the occurrence point. The first vulnerability was calculated for the occurrence point P5. But as we can see when the same feared event occurs at another point, the vulnerability is quite different. The worst occurrence point is in this case the point P1.

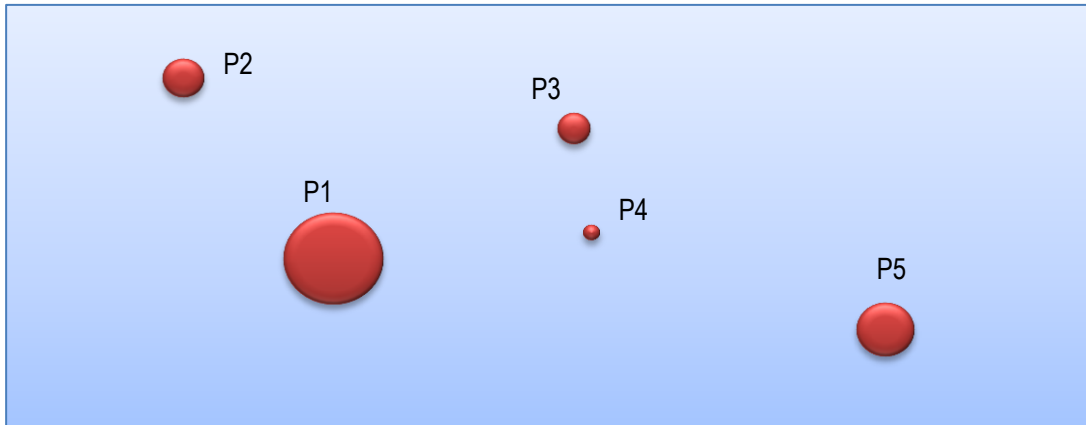


Figure III-31: Feared event occurrence point

### III.1.12.5 TIME TO BREAK DOWN

In the II.1.2.2 we have seen that one component could fail in several ways. VESTA could show for selected scenario the breakdown time relative to the simulation time.

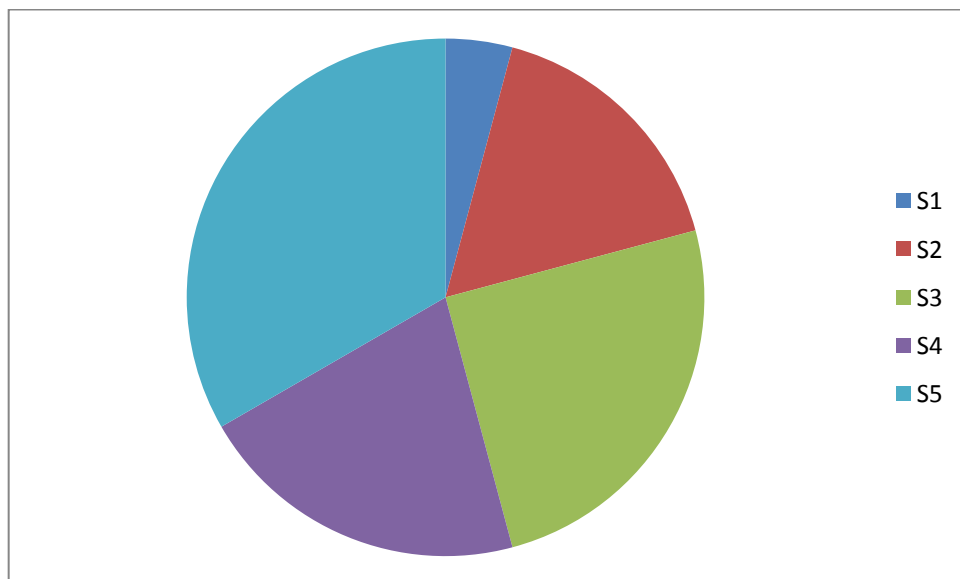


Figure III-32: Time to break down

Figure III-32 presents for six scenarios the breakdown time of the component C2. The user can click on a scenario to see that the realization condition S5 is the worst one with a ratio of 33%.

### III.1.12.6 MINIMUM VALUE OF ONE PARAMETER

Every component has many parameters. Decision consists also in changing one or more of these parameters. It is then valuable for the user to know the threshold of a parameter for one or more feared events. The component will break down if the considered parameter is above or below the threshold. VESTA allows such representation.

	<b>Scenario</b>				
	S1	S2	S3	S4	S5
Mean time to recover	23	33	9	12	7

Table III-11: Minimum value of one parameter

Table III-11 shows the minimum mean time to recover the component C2 which might have to stay functional. It shows that the scenario S5 is the best in terms of Mean Time to recover for this component.

### III.1.12.7 EFFECT OF INTERDEPENDENCE

Interdependence when activated could change the behaviour of the system. The user can select a parameter of a component and see the effect of one or more interdependence on it.

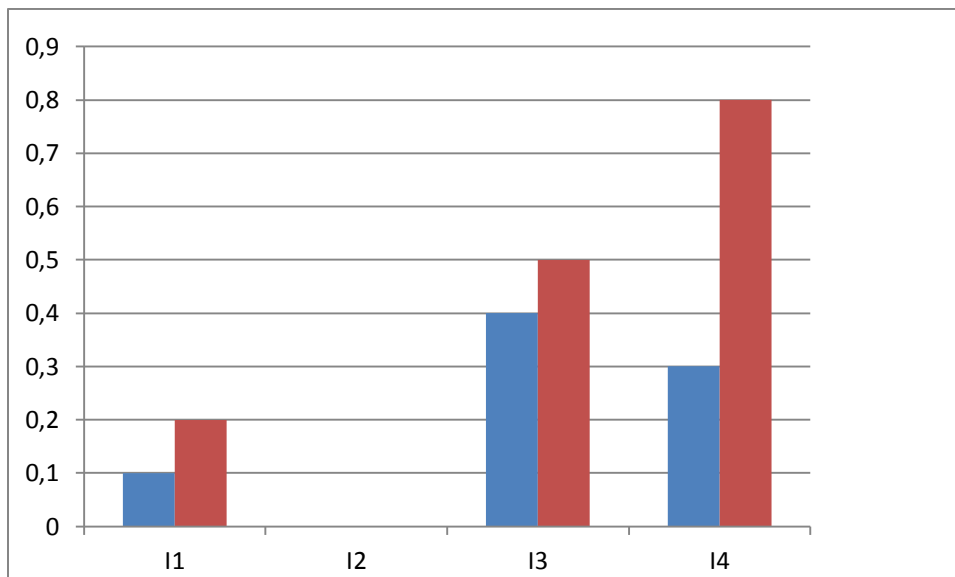


Figure III-33: Effect of interdependence

The Figure III-33 shows the vulnerability of the component C4. Each situation is plotted with regard to four interdependences (without interdependence in blue and with four interdependences in red). It shows that the interdependence I4 has more effect on this component.

### III.1.12.8 REQUEST ON DATABASE

VESTA allows the user to request the database. For example the user might wish to know:

- Who are the decision makers for one territory?
- What is the reliability of a specific component?

The main contribution of this system is to allow users to draw a network in an easy way, adding or deleting nodes and edges. It allows to analyse system dynamicity.

Another contribution of this system is to simulate a feared event and simulate what will be the results of the event. This system offers to the users a double way to simulate a feared event: network drawing and simulation.

## CONCLUSION

Natural disasters affecting infrastructure networks are destabilizing events for the society. In such crisis management the use of computer systems is required. Decision Support System for crisis management should be effective and efficient.

The objective of this chapter was to present a vulnerability model-based Decision aiding. Every component of the architecture is described. The proposed decision process is particularly suitable for infrastructure network failure management. It includes all the steps of the crisis management. It allows an estimation of infrastructure network vulnerability taking into account interdependences. Thus it is possible to deduce among other vulnerable areas, critical components and the most threatened stakes. As future work, we hope to deploy this application on the internet and on mobile devices (smartphone, tablet). To validate our study, we applied it on two case studies presented in the next section.

# CHAPTER IV

## CASES STUDY

### **Résumé en français**

Ce chapitre présente les cas d'études. Nous avons dans un premier temps généré un cas d'étude avec suffisamment de possibilités pour tester les modèles décrits dans les deux précédents chapitres. Nous avons pris soin de les rendre les plus réalistes possible. Dans un premier temps nous avons procédé à une simulation manuelle sur des cas simplistes. Puis nous avons utilisé des programmes pour des cas complexes pour finir avec l'outil développé. Nous avons poursuivi notre démarche de validation en appliquant le modèle à un cas réel. La ville de Lourdes a été choisie pour les enjeux qu'elle représente en termes d'image de la nation. En effet, Lourdes est une ville de pèlerinage située dans une zone à haute sismicité. Conscient de cette situation, les autorités ont entrepris une démarche de réduction de la vulnérabilité de la ville. L'application de notre modèle à la ville a permis de faire des propositions d'actions préventives.



"I decided that it was not wisdom that enabled poets to write their poetry, but a kind of instinct or inspiration, such as you find in seers and prophets who deliver all their sublime messages without knowing in the least what they mean"

Socrates

"In theory, there is no difference between theory and practice. But, in practice, there is"

Jan van de Sneptscheut

## INTRODUCTION

Once the models have been defined, the validation is a crucial step. One way to validate is to perform a case study which is the objective of this chapter. It presents two case studies. The first one is an example with sufficient elements to test the models described in the two previous chapters. We took care to make them the most realistic possible. At first, we carried out a manual simulation on simplistic cases. Then we used programs for complex cases to finish eventually with the developed tool. We continued our validation approach in applying the model to a real case. The city of Lourdes was chosen because of its geographical situation which makes it particularly vulnerable to earthquakes. Indeed, Lourdes is in a high seismicity area. Aware of this situation, the authorities have undertaken a process of reducing the city vulnerability. The application of our model to the city aimed at making proposals of preventive actions.

### I.9: GENERATED CASE STUDY

In this chapter the case study is a generic network presented in Figure IV-1. The aim here is to validate the model shown in Chapter II. The network is hosted by two territories T1 and T2.

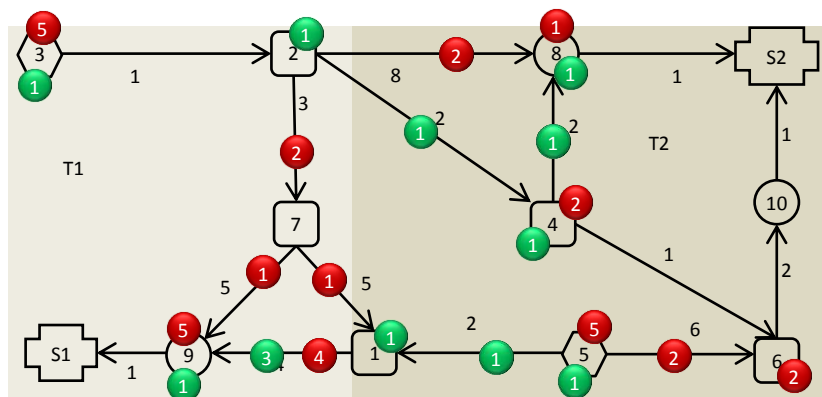


Figure IV-1: Case study

Two generic flows circulate in the networks: Flow A (red) and flow B (green). Flows are supposed to be discrete. The network is composed of two source nodes (3) and (5); five relay nodes (1), (2), (4), (6), (7) and three target nodes (8), (9) and (10). Source nodes produce flows. Target nodes are flow destinations. The number on each flow corresponds to its quantity. For instance there are 2 types of flow A (red) in the relay node (6). The network provides two stakes: a firm (S1) and a human stake (S2). Each of them consumes 5 flows A per second and 1 flow B per second. All components of the network (nodes and edges) can resist over 5 degrees earthquake on Richter scale. Their storage capability is 5 flows A and 5 flows B. For source nodes, production capacities are 5 flows A per second and 1 flow B per second. The node (7) is positioned under sea level. Water is retained by a barrier.

### IV.1.1 CONTEXT

Because of edge weight depends on the environment, the methodology begins then by its identification. In many realistic situations, infrastructure networks provide many territories. Territory might be a city or a country. As a rule, territories are administratively independent. For this reason its specificities are determined. Flows circulate in network according to many rules. Otherwise many of their characteristics influence network vulnerability. These characteristics and parameters are analysed.

Robustness and resilience analysis are performed for one or many feared events. According to its frequency and amplitude, damage is more or less important. So, feared event assessment is described. Feared event might encounter some factors that can mitigate or aggravate them. For example, a dam or a barrier prevents territory from flood but if it comes to rupture the consequences can be worse than the impact of the flood itself. The way of taking them into account is indicated.

From these elements, network good functioning is determined by a nominal state. Feared event will affect the system and drop it in a new state. From these states, the vulnerability assessment through robustness and resilience is investigated. Next sections present how to integrate all these parameters and their attributes in the models. Parameters consist in environment, Territory, Flow, Mitigation and aggravation factors and feared events.

The following section discusses how the working environment influences the network model.

#### ✓ *Environment*

---

Figure IV-1 shows weighted edges. Edge weight is indicated by a number. For example the weight of the edge (7)-(1) is 5. The notation (7)-(1) stands for the edge between node (7) and node (1). Weight might be geodesic distance between nodes, or any relevant criteria for the analysis (cost, time). For instance, in French power grid distribution, the cost depends on the period (less expensive in the night) and the weather conditions (rain, snow, sun...). Edges weight obtained by environment parameters aggregation is out of the scope of this thesis. Edge weight determines the flow circulation. Because of this fact, environment affects the resulting robustness and reliability. Network might be hosted by many territories administratively independent. Territory attributes influencing the model are presented in the next section.

#### ✓ *Territory*

---

Territory is the geographic area gathering the other elements. Many territories might be provided by a single network. Territories are administratively independent. Decisions taken by one of them might be different or even contradictory to others. Hence the need to separate them is crucial. Territory is characterized by its limits, decision makers, set of actions, feared event and a stretch. The stretch of one element is its influence area. In this case study, territories stretches are respectively 10,000,000 m<sup>2</sup>, and 5,000,000 m<sup>2</sup>. They are threatened by an earthquake.

Territory networks are supported by flows circulation. Their parameters are presented in the next section.

### ✓ Flow

In the case study, the speed of flow A is 3 units per second. The speed of flow B is 1 unit per second. The circulation flow is described as following:

- Path of flow B produced in (3) is: (3)→(2)→(4)→(8)→(S2);
- Path of flow B produced in (5) is: (5)→(1)→(9)→(S1);
- The 5 flows A produced in (3) are distributed in five different paths:
  - (3)→(2)→(7)→(9)→(S1);
  - (3)→(2)→(7)→(1)→(9)→(S1);
  - (3)→(2)→(8)→(S2);
  - (3)→(2)→(4)→(8)→(S2);
  - (3)→(2)→(4)→(6)→(10)→(S2).
- The 5 flow A produced in (5) are distributed in two paths:
  - Two flows follow the path (5)→(6)→(10)→(S2);
  - Three flows follow (5)→(1)→(9)→(S1).

Networks and flows are affected by events such as natural disasters. Modelling of these feared events is discussed in the next section.

### ✓ Feared events

Feared event is characterized by some parameters: Amplitude, frequency, propagation speed, surface, duration, and occurrence point. One earthquake is considered in the case study. Its parameters are shown in Table IV-1.

<b>Earthquake</b>	Amplitude	4
	Frequency	0,128
	extent	5000000 m <sup>2</sup>
	Speed	1000 m/s
	Duration	1000 ms

Table IV-1: Feared event parameters

From its occurrence point, feared event is situated at 1,000 meters from node (7), 3,000 meters from nodes (4) - (1); 2,500 meters from edge (2)-(7); 2,800 meters from edge (2)-(4).

From its occurrence point to the network, hazard might encounter aggravation or mitigation factors. Attributes of these factors to be integrated in the model are presented in the following section.

### ✓ *Mitigation or aggravations factors*

---

In the case study, the barrier nearby node (7) is an aggravation factor (A). Parameters of this factor are given in Table IV-2. This aggravation factor would increase the feared event amplitude of 2 points (+2) in a radius of 10 meters. From its position only node (7) is in its area.

A	Amplitude	2
	extent	10 m
	Type	Feared event amplitude

*Table IV-2: Aggravation factor parameters*

From the initial state, a simulation is performed. The final state obtained is presented in next section.

## IV.1.2 SYSTEM FINAL STATE

Final state is obtained after feared event occurrence. In the case study, when the feared event is initiated it will affect only node (7) in one second. Node (7) could resist the feared event amplitude. But because of the aggravation factor, the amplitude is rolled up to 6 to the feared event amplitude is added the aggravation factor amplitude (4+2). Node (7) will then break down after 1 second simulation.

At time  $t=2s$  the edge (2)-(7) will be over its maximum capacity in flow and will break down. Extra flows  $A$  are redistributed on the edges (2)-(8) and (2)-(4). A new full blast obtained after 6s simulation is shown in Figure IV-2.

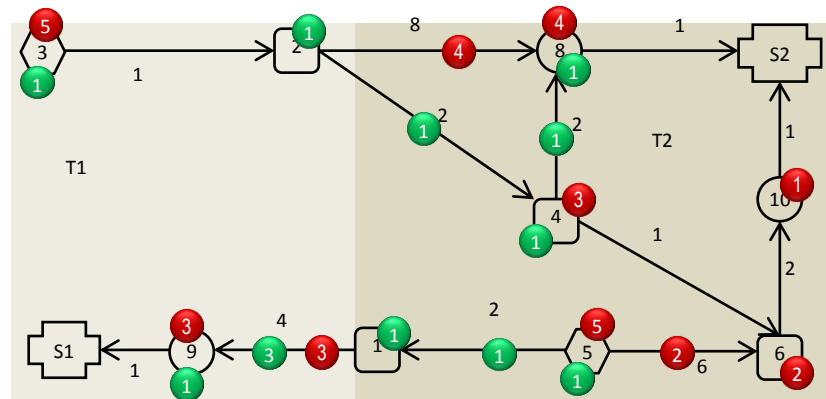


Figure IV-2: Network after feared event occurrence

It can be observed that the network structure has changed as well as repartition, and stake consumption. Initially, the consumption of the stake  $S_1$  and  $S_2$  were 5 flows A and 1 flow B. After the feared event occurrence, this consumption is now:

- For Stake  $S_1$ : 3 flows A and 1 flow B;
- For Stake  $S_2$ : 7 flows A and 1 flow B.

From the initial state and the final state, the vulnerability assessment is given in the next section.

### IV.1.3 RESULTS

Table IV-3 shows simulation results for the case study. These numbers are obtained from Figure IV-1 (State  $E_1$ ) and Figure IV-2 (State  $E_2$ ) on formula given in II.1.8.

Component	$E_1$		$E_2$		RbA	RbB	Rb	t1	t2	Rs	vul
	A	B	A	B							
Nodes 1		1		1	1	1	1	6	0	1	0
Nodes 2		1		1	1	1	1	6	0	1	0
Nodes 3	5	1	5	1	1	1	1	6	0	1	0
Nodes 4	2	1	3	1	0,8	1	0,8	6	0	1	0,2
Nodes 5	5	1	5	1	1	1	1	6	0	1	0
Nodes 6	2		2		1	1	1	6	0	1	0
Nodes 7					1	1	1	1	5	0,166	0,83
Nodes 8	1	1	4	1	0,4	1	0,4	6	0	1	0,6
Nodes 9	5	1	3	1	0,75	1	0,75	6	0	1	0,25
Nodes 10			1		0	1	0	6	0	1	1

Edge (3)-(2)					1	1	1	6	0	1	0
Edge (2)-(7)	2				0	1	0	2	4	0,33	1
Edge (7)-(9)	1				0	1	0	1	5	0,16	1
Edge (7)-(1)	1				0	1	0	1	5	0,16	1
Edge (1)-(9)	4	3	3	3	0,85	1	0,86	6	0	1	0,14
Edge (9)-(S1)					1	1	1	6	0	1	0
Edge (2)-(8)	2		4		0,66	1	0,67	6	0	1	0,33
Edge (8)-(S2)					1	1	1	6	0	1	0
Edge (2)-(4)		1		1	1	1	1	6		1	0
Edge (4)-(8)		1		1	1	1	1	6	0	1	0
Edge (4)-(6)					1	1	1	6	0	1	0
Edge (6)-(10)					1	1	1	6	0	1	0
Edge (10)-(S2)					1	1	1	6	0	1	0
Edge (5)-(6)	2		2		1	1	1	6	0	1	0
Edge (5)-(1)		1		1	1	1	1	6	0	1	0
S1	5	1	3	1	0,75	1	0,75	6	0	1	0,25
S2	5	1	7	1	0,83	1	0,83	6	0	1	0,17

Table IV-3: Results

From the Table IV-3 many observations could be made:

- A robust and resilient component will be non-vulnerable. This is the case of many components: node (1), node (2), node (3);
- If a component is non-robust or non-resilient then it is vulnerable: Nodes (4), (7), (8) and (9) for instance;
- Stakes are supposed to resist to feared events, then their robustness might be different from 1 because of the flow circulation. For stake S<sub>1</sub>, the consumption in flow A is dropped from 5 to 3. Consumption of stake 2 for the same flow has increased from 5 to 7. For both of them the difference between initial and final flow is 2. But the result shows that S<sub>1</sub> is more vulnerable than S<sub>2</sub>. Indeed lack of flux induces more vulnerability than a flow surplus. That demonstrates that extra flow in a component is a vulnerability source.
- Flows determine network dynamic. So flow dynamic robustness will have some sense. For this reason, they are supposed to be dynamically robust.

## I.10: LOURDES CASE STUDY

This chapter is an application of the model to a real case. The selected city is Lourdes, in the “Hautes-Pyrénées” (France). Indeed, the Hautes-Pyrénées lies in the highest seismic area in the French metropolitan country. The Midi-Pyrénées region and more particularly the Pyrenees departments are concerned by a possible occurrence of an earthquake. An earthquake of magnitude 6, could generate significant damage. Such disaster is reasonably foreseeable in the department without being able to situate it in time and space. Because it is not possible to predict the location and date of earthquakes, the only answer seems to be the prevention in terms of making the considered system more tolerant to the occurrence of such an event. Earthquake plan priorities are people information, control of compliance with earthquake-resistant construction rules, training of health care structures and emergency plan preparation. It was launched at the national level and declined on the chain of the Pyrenees. The Hautes-Pyrénées were selected to be pilot of this implementation. Unfortunately the only prevention is not sufficient to eliminate the risk of large-scale disaster. Without wanting to compare with the tragic events in Haiti who are in a very different context from that considered in this thesis, a parallel can be made with the recent earthquake that occurred in Italy (6.3 on the Richter scale). The occurrence of such a catastrophe in the Pyrenean is not at all unthinkable.

This section aims to estimate the vulnerability of Lourdes city situated in a high seismic area. Lourdes is a pilgrimage city since 1858 which may amplify the dramatic character of the consequences in case of the occurrence of a seism. As an illustration the city hosted during the 150th anniversary of the Virgin apparition nearby 70,000 pilgrims per day. Among the different topics of concern, the city wishes to analyse the vulnerability of the sewage network.

### IV.1.4 DATA COLLECTION

Data structure collected in this case study is those presented in the previous chapter. It was realised with the help of the city of Lourdes and specialised databases. Data includes decision makers, the recorded feared event, mitigation and aggravation factors, infrastructure, flow, stake and the external environment. Part of these elements is presented in the followings sections.

#### ✓ *Decision makers' identification*

The section III.1.1.4 underlined the importance of decision maker identification. In the case of the city of Lourdes, there are many entities involved in the decision making process. The aim here is not to list all individual and authorities that might influence decision in crisis situation. We only investigated the specific area of decision induced by infrastructure network failure in the context of natural disaster. In this case there are two decision makers:

- The analyst: we played the role of the analyst. But very often, the city appeals external competence



such as specialized institution. For instance, the National Institute of industrial Environment and Risks realized the analysis after a flood in June 2013;

- The Departmental Direction of Equipment: This direction is in charge of equipment administration in the department. It deals with the realisation of many studies related to risk and vulnerability analysis. Thanks to them we were provided with seismic maps of the city, and put in contact with the network managers;

It can be said about these identified decision makers that they are mostly involved in the analytic part of the decision. Decision maker who really takes decision in crisis situation are sometimes not clearly identified. This leads us to the first problem of crisis management.

### ***Problem 1 :Who is able to take the right decision in a crisis situation?***

- The city of Lourdes: In this case study, the city of Lourdes is in charge of the application of every decision whether at regional or national levels. Some institutions such as the ministry of Ecology could be also involved in the crisis management.

#### ***✓ The feared event***

---

Feared event determination is at the heart of vulnerability analysis. Most of them aim to determine effect of events on stakes. The case of Lourdes is quite similar to this situation. In fact the city is situated in a high seismic area. Figure IV-3 shows a seismic zoning of the Lourdes regions. This zoning is determined by the French office on Geological and Mineral Research (BRGM). It is based among other on the geological structure. We can see that Lourdes is situated in the high seismic zone (4 on a scale of 5). This card has been validated by the French Ministry of Ecology and Sustainable Development. (art. D. 563-8-1 of the environment code 01/05/2011).

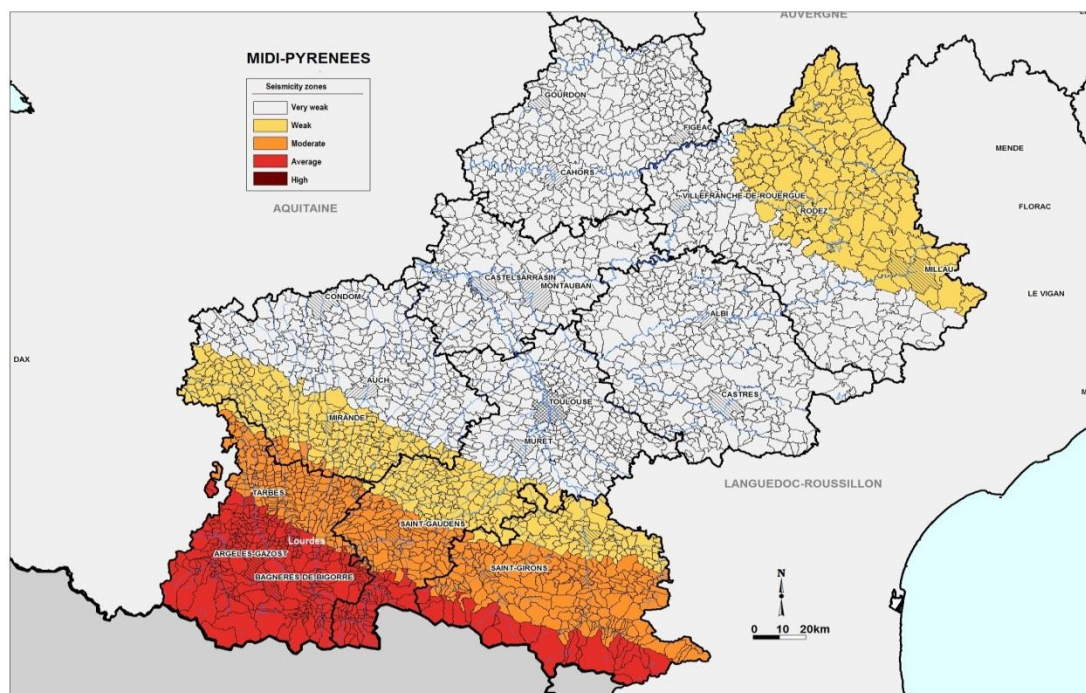


Figure IV-3: Midi-Pyrénées Seismic zoning

The city has been in the seat of many seismic events these recent years. Flood and weak amplitude seism are the main events. Table IV-4 shows some earthquakes that happened in Lourdes these past years.

<b>Date</b>	<b>Hour</b>	<b>Epicentre localisation</b>	<b>Epicentre Intensity</b>	<b>Intensity in Lourdes</b>
11/15/2007	13h47 min 35 sec	BIGORRE (E. ARGELES-GAZOST)	5	4
11/17/2006	18 h 19 min 50 sec	BIGORRE (GAZOST)	6	6
01/21/2003	18 h 1 min 1 sec	OSSAU (LOUVIE-JUZON)	5	3
12/11/2002	20 h 9 min 53 sec	OSSAU (ARUDY)	5	2
09/05/2002	20 h 42 min 16 sec	OSSAU (ARUDY)	5	3

Table IV-4: Earthquakes in Lourdes Region

There are many approaches to determine feared events to be taken into account. But for this study, the city of Lourdes wishes to analyse the city vulnerability against earthquake. The choice is suggested. But in many cases, it is not. The analysis may find out the appropriate feared event. One will have to determine if feared events including or excluding the system internal failure.

**Problem 2: In the context of the analysis, what are the events to be included, how to identify them?**

For the city of Lourdes, we suggested an analysis for an earthquake of 8 on Richter scale. That corresponds to the maximum amplitude recorded since 1660. This earthquake occurred in Bigorre (Juncalas) the

03/24/1750 at 22h. The location and the propagation speed would be hazardous in the simulation. From its position on the Figure IV-3 Lourdes is situated in a middle seismic area. For such area the period of an earthquake of 8 is between 75 to 250 years. We have chosen the minimal period of 75 years. The simulation will be performed for 100 years. We supposed that the worst case will correspond to a double occurrence of the earthquake. When it occurs it will affect components within a circular perimeter of 12 kilometres across, with a speed of 6 meters per second.

### ✓ *Mitigation and aggravation factors*

---

On the territory of the city, we did not identify any relevant factors. In fact, Lourdes is a small city of 36.4 square kilometres. Because of this small size it does not host infrastructure that could be considered as aggravation facture.

### ✓ *Territory*

---

The only territory considered is the city of Lourdes itself. They are no interest to divide it. But in the context of interdependent network, we faced the following problem:

#### ***Problem 3: What is the limit of the territory to be included in the analysis?***

### ✓ *Infrastructure*

---

This analysis is about sewage network. The Autocad map of this network was provided by the city of Lourdes. The sewage network is represented in red; the green is the rain network. The network in magenta is a secondary network for both sewage and rain.

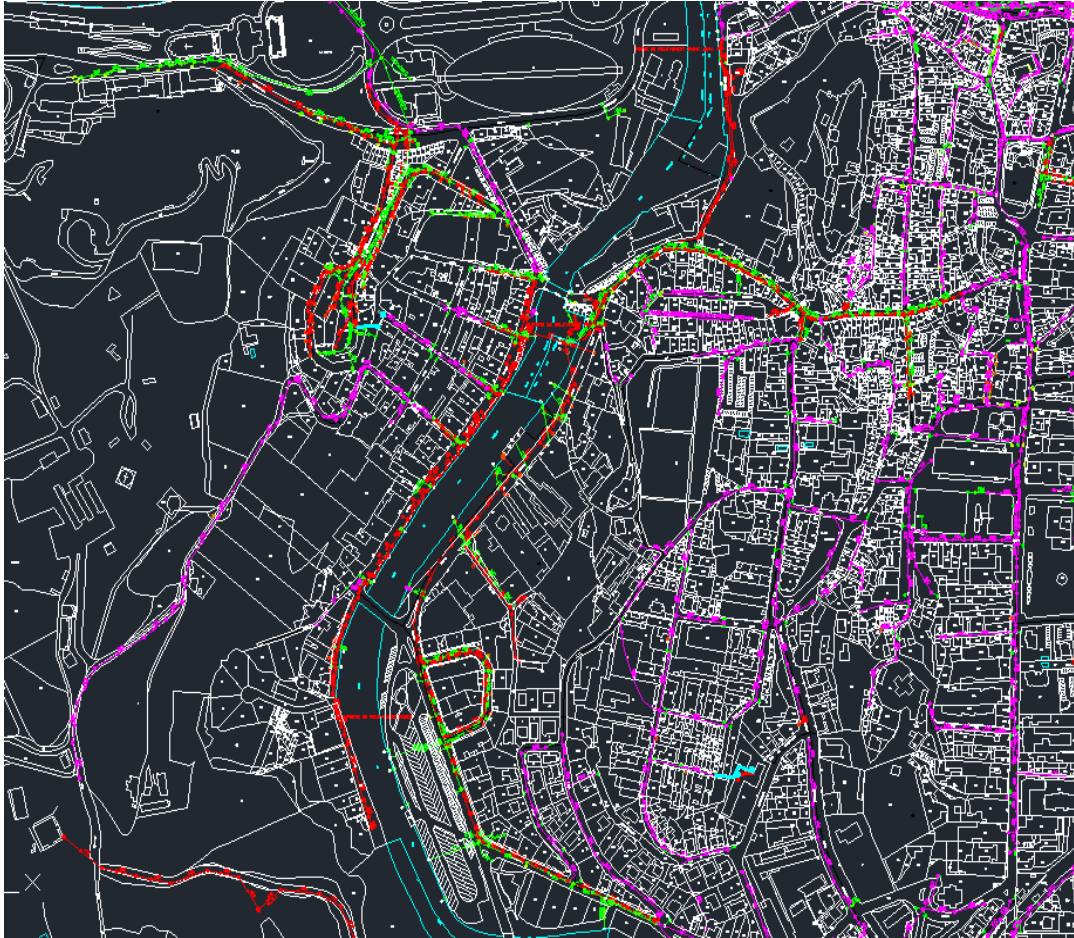


Figure IV-4 : Lourdes networks

The network in Figure IV-4 consists in outlet pipes, pumping stations, water treatment plants, and manholes. Reliability of these components was not provided by the owner of the network. We supposed that the reliability of these components is 0.9 for the simulation time, their mean time to repair 24 hours and they could resist over 7 amplitude earthquake on Richter scale. These values are fictive. That leads to the following problem.

**Problem 4: What influence date relevancy could have on the result?**

✓ **Flow**

Flow considered in this analysis is sewage. The circulation direction is imposed by the network structure. The unit is the cubic metre. The city consumed approximately 3 millions of cubic metre of water every year. The capacity of pumping stations, water treatment plants is 7, 000 cubic metre (700 cubic metre per hour). The speed is supposed to be 3 meter per second.

### ✓ Stake

---

After some interviews with the authorities of Lourdes city, we decided to focus on the human stake. This decision was taken because pilgrims represent a wide population. The city is full of 16,000 people. But it hosts every year nearly 6 million of pilgrims or tourists for which approximately 60,000 are sick or invalids. This reason justified the choice of population as the main stake in our model.

### ✓ External Environment

---

We did not include the external environment. The environment consists among others of the effect of weather on the infrastructure and flow circulation. Its influence is not that considerable. Another reason was the time constraint. We did not have enough time for modelling this influence. This analysis leads to the following problem.

**Problem 5: From the vulnerability model to its implementation in a case study how to estimate the project duration? How many resources must be allocated?**

Results of the simulation are presented now.

## IV.1.5 RESULTS

We have modelled part of the network in a software called VESTA. First, we imported a map edited by Google map and drawn the network on this image (Figure IV-5).

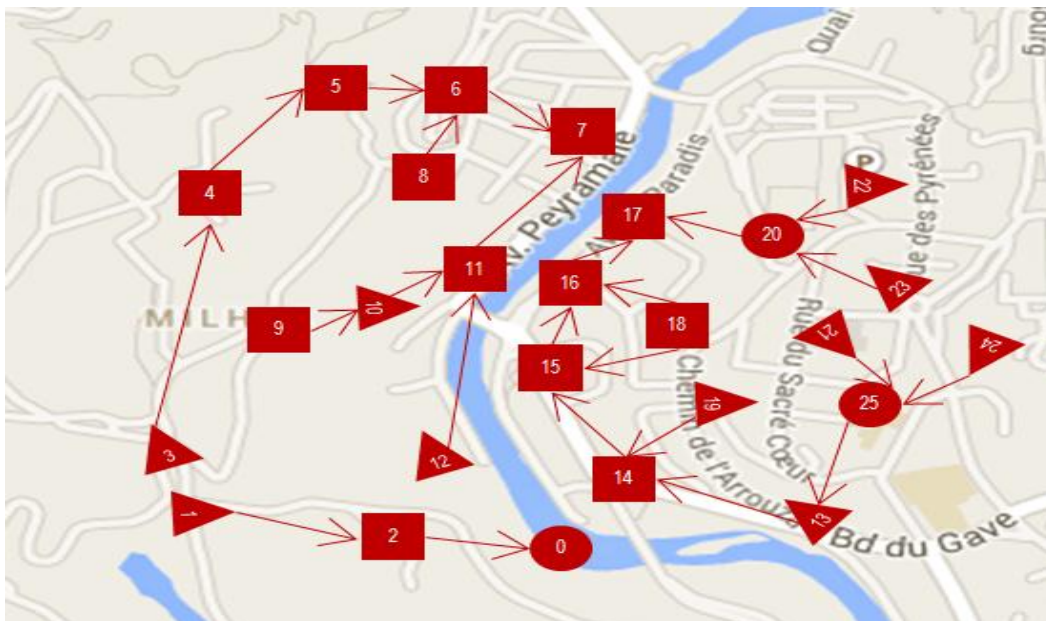


Figure IV-5: Lourdes network modelling

After a simulation, the results are shown in the following table.

<b>Component</b>	<b>S1</b>	<b>S2</b>	<b>t1</b>	<b>t2</b>	<b>Rb</b>	<b>Rs</b>	<b>v</b>
Nodes 1	700	700	98	2	1	0,98	0,02
Nodes 2	700	500	70	30	0,83	0,7	0,42
Nodes 3	300	400	100	0	0,85	1	0,14
Nodes 4	300	300	45	55	1	0,45	0,55
Nodes 5	300	300	99	1	1	0,99	0,01
Nodes 6	500	600	100	0	0,90	1	0,09
Nodes 7	700	700	68	32	1	0,68	0,32
Nodes 8	200	300	23	77	0,80	0,23	0,82
Nodes 9	100	0	56	44	0	0,56	1
Nodes 10	100	0	94	6	0	0,94	1
Nodes 11	200	100	71	29	0,66	0,71	0,53
Nodes 12	100	100	98	2	1	0,98	0,02
Nodes 13	200	200	81	19	1	0,81	0,19
Nodes 14	400	500	97	3	0,88	0,97	0,14
Nodes 15	500	500	45	55	1	0,45	0,55
Nodes 16	600	600	78	22	1	0,78	0,22
Nodes 17	700	600	22	78	0,92	0,22	0,8
Nodes 18	200	100	59	41	0,66	0,59	0,61
Nodes 19	200	300	89	11	0,8	0,89	0,29
Nodes 20	100	100	44	56	1	0,44	0,56
Nodes 21	100	200	94	6	0,66	0,94	0,37
Nodes 22	50	100	27	73	0,66	0,27	0,82
Nodes 23	50	0	78	22	0	0,78	1
Nodes 24	100	0	89	11	0	0,89	1
Nodes 25	200	200	32	68	1	0,32	0,68
Edge(1)-(2)	700	600	55	45	0,92	0,55	0,49
Edge(2)-(0)	700	500	70	30	0,83	0,7	0,42
Edge(3)-(4)	300	400	30	70	0,85	0,3	0,74
Edge(4)-(5)	300	300	90	10	1	0,9	0,1
Edge(5)-(6)	300	300	97	3	1	0,97	0,03
Edge(6)-(7)	500	600	92	8	0,90	0,92	0,16
Edge(8)-(6)	200	300	84	16	0,8	0,84	0,33

Edge(9)-(10)	100	0	81	19	0	0,81	1
Edge(10)-(11)	100	0	21	79	0	0,21	1
Edge(11)-(7)	200	100	99	1	0,66	0,99	0,34
Edge(12)-(11)	100	100	98	2	1	0,98	0,02
Edge(13)-(14)	200	200	92	8	1	0,92	0,08
Edge(14)-(15)	400	500	93	7	0,88	0,93	0,17
Edge(15)-(16)	500	500	68	32	1	0,68	0,32
Edge(16)-(17)	600	500	17	83	0,90	0,17	0,85
Edge(18)-(15)	100	0	9	91	0	0,09	1
Edge(18)-(16)	0	100	29	71	0	0,29	1
Edge(19)-(14)	200	300	46	54	0,80	0,46	0,63
Edge(25)-(13)	200	200	99	1	1	0,99	0,01
Edge(21)-(25)	100	200	99	1	0,66	0,99	0,34
Edge(24)-(25)	100	200	96	4	0,66	0,96	0,36
Edge(23)-(20)	50	0	2	98	0	0,02	1
Edge(22)-(20)	50	100	86	14	0,66	0,86	0,43
Edge(20)-(17)	100	100	79	21	1	0,79	0,21
Stake	2000	2200	100	0	0,95	1	0,05

Figure IV-6: Results of the Lourdes case study

Results in this table confirmed those of the generated study. With the initial parameters, components 9, 10, 23, 24, (9)-(10), (10)-(11), (18)-(15), (18)-(16), (23)-(20) are the most vulnerable. This is because at the end of the simulation any flow passes through these components. However, for (23)-(20) is fully vulnerable because of the fact that it has any flow at the beginning of the simulation. The less vulnerable components are 1, 5 and (25)-(13). This is because of the feared event occurrence point. In fact, these components are far away from the occurrence point. These results could be displayed in one of the forms presented in the III.1.12. The following figure shows the vulnerability per component.

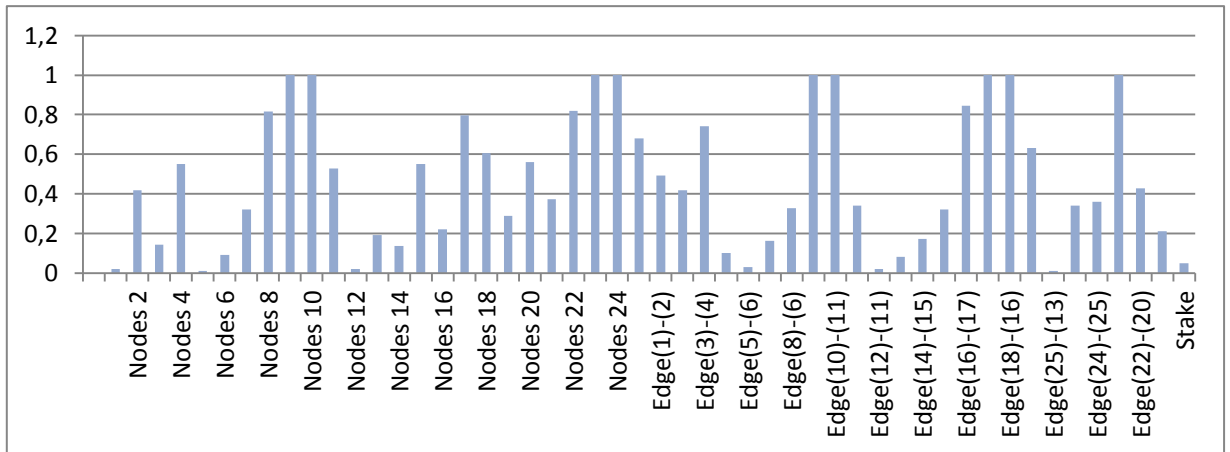


Figure IV-7: Vulnerability of Lourdes network components

These results despite their none-realism are quite satisfying. They could be more relevant with real data.



### CONCLUSION

The aim of this chapter was to illustrate the application of the models introduced in the previous chapters. First, we generated a case study taking into account all the parameters of the model. Second, we applied the model to a real case: the city of Lourdes. This second phase was the most difficult. Difficulties are related mainly to the data acquisition. In fact for the selected network, this latter is the property of “Veolia eau”. Veolia did not want to provide us with data about its network for public thesis. The alternative was to generate the missing ones. We then researched in public database on internet. The selected values are much closed to the reality. The main problem is the similarity of component parameters. We selected the same value for similar component. These values could be very different in reality. The implementation of the model in these case study revealed some problems summarized below:

- Decision maker identification;
- Feared event selection;
- Territory limitation;
- Data relevancy;
- Environment effect assessment.

These problems highlight the limits of our models. In spite of this, this chapter showed the importance of flows circulation and the interdependences of dynamic factors.

"In all things the end is the essential" Aristotle

## General conclusion

These days, natural disasters are becoming more and more frequent and devastating. A deficit of scientific work has been highlighted to manage a crisis situation linked to the occurrence of disasters disrupting infrastructure networks. For instance, following a serious earthquake, it has been estimated at approximately 5 days the time limit for the emergency response to save human lives. The organization at this level is crucial. Every organization is strongly disturbed by network disruption that may be affected or rendered unusable after the feared event. In this exceptional situation, decisions must be taken quickly. The efficiency of these decisions depends on the models used. The objective of this thesis was to determine a vulnerability model allowing a crisis management in the context on infrastructure networks affected by natural disasters. The scientific problem dealt with:

- The modeling of interdependent critical infrastructure;
- The analysis of structural and functional vulnerability;
- The correlation between the feared event intensity and damages to the stakes;
- The establishment of a decision aiding methodology;
- The prototyping of a Decision Support System.

### ✓ *Contribution*

---

The contribution in this thesis can be summarized as follows:

- Literature review on vulnerability and decision aiding;
- Identification of component influencing the vulnerability analysis;
- Definition and modelling of interdependences;
- Vulnerability modelling;
- Determination of crisis management components;
- Elaboration of a decision aiding process;
- Characterisation of Decision Support System for disaster management;
- Building a prototype of a Decision Support System;
- Identification of implementation problem from the model to a real case;

We began by a literature review according the two points of views pointed out in the introduction, that is: A vulnerability model especially designed for decision aiding in the situation of a crisis management. We analysed and differentiated the analysis of vulnerability and the analysis of risk. This literature review allowed us to identify the elements to be integrated in our future model. The objective was to answer the question: what are the interacting elements which could make a stake vulnerable or not vulnerable? Two kinds of components, one considered as static, the other as dynamic, aroused from the analysis: Dynamic factors are responsible of interdependences inside the global system. We then investigated the interdependence notion. We pointed out in particular a functional part representing the dependence relationship and a dysfunctional part standing for the influence connexion. The challenge was to integrate these concepts in the network modelling by using graph theory. The proposed modelling approach takes into account every possible configuration of the network. Then, we proposed a vulnerability assessment model. With this model, it is possible to determine the vulnerability of a component, or that of an entire network. This model confirms the point of view of many authors, which consider that vulnerability is composed of robustness and resilience. Vulnerability assessment is not an end in itself. It must lead to a decision. Consequently every component of a decision in a crisis context has been identified and described. The suggested process can be used in various identified crisis situation. This process includes the multicriteria aggregation method to be used. With the objective to provide the decider with a computer-aided tool, we characterized a Decision Support System and built a prototype. This prototype does not implement all the functionalities, but is under progress. The last contribution in this thesis was to point out all problems that occurred while implementing the model in a real case. With our contributions decision makers could find some answer element to the following questions:

- What is to be feared?: event, scenario, system configuration;
- What is vulnerable?: single component, network, stake, territory;
- What can be done?: action on one or many element(s) of the global system;
- How it could be done?: Decision process, aggregation approach;

These results lead to some perspectives in the next section.

### ✓ *Perspectives*

---

Results pointed out in this thesis are quite satisfying. But they could be enhanced through some elements of perspective summarized in the following:

- Using Multi Agent System for a wide simulation;
- Deployment of the software on internet and mobile devices;
- Using collaboration between Decision Makers;
- Integration of direct impact of feared event on stakes;
- Integration of the component failure mode after the occurrence of the feared event.

The use of Multi Agent System approach seems to be indicated to more than one title. In the context of this thesis, an agent could be seen as an autonomous computer module which is able to take decisions in an uncertain environment. From this point of view, different elements of the model could be considered as interacting agents. This will promote the emergence of new structure in the network. These structures are not directly accessible to human analysis. On another hand, the use of Multi Agent System offers the possibility of determining actions while Decision Makers are themselves affected by the feared event. This situation is unfortunately very common in natural disaster. Another point to mention is that the Multi-Agent approach is suitable for simulating Complex Systems and a vulnerability model could be seen as a Complex System.

We have already highlighted the importance of the software distribution. By distribution, we mean geographical one. Software located at different places seems to be less vulnerable than when it is located in a single place. Moreover, its use and survivability will be greater when deployed on tablet and mobile devices. At this level, the software can be built in a collaborative way. For instance the users can determine the exact localisation of aggravation factor, the affected component etc.

In this thesis we were interested only on indirect effect of feared events. Our model could be enhanced by taking into account the direct impact on stakes. In real situation direct impact are often those which are investigated. Moreover, component failure is not binary. Feared event effect is related to component failure mode. An affected component will resist or not according to its structure. We plan to incorporate in our model parameters such as testability, detectability, Integrated Logistics Support etc.

## Conclusion générale

De nos jours, les catastrophes naturelles sont de plus en plus nombreuses, fréquentes et dévastatrices. Le déficit du travail scientifique pour gérer une situation de crise liée à la l'occurrence de catastrophes perturbant les réseaux d'infrastructures a été mis en évidence. Il est prouvé que suite à un grand tremblement de terre, il y a environ 5 jours de délai pour l'intervention d'urgence afin de sauver des vies humaines. L'organisation à ce niveau est cruciale. Chaque institution peut être perturbée par une défaillance réseau due à la catastrophe. Dans cette situation exceptionnelle, les décisions doivent être prises rapidement. L'efficacité de ces décisions dépend des modèles utilisés pour déterminer les vulnérabilités. L'objectif de cette thèse était de déterminer un tel modèle de vulnérabilité afin de favoriser une gestion de crise dans un contexte de catastrophes naturelles affectant les réseaux d'infrastructures. Nous avons traité les problématiques scientifiques suivantes :

- Modélisation des infrastructures critiques interdépendants ;
- Modélisation des interdépendances ;
- Analyse de la vulnérabilité structurelle et fonctionnelle ;
- Corrélation entre un évènement redouté et les dommages-causés aux enjeux ;
- Mise en place d'un processus de décision pour le management de la vulnérabilité ;
- Prototypage d'un Système Interactif d'Aide à la Décision.

### ✓ *Contribution*

---

La contribution dans cette thèse peut être résumée comme suit :

- État de l'art de la vulnérabilité et de l'aide à la décision ;
- Identification des composants qui influencent l'analyse de la vulnérabilité ;
- Définition et modélisation des interdépendances ;
- Proposition d'un modèle de la vulnérabilité ;
- Détermination des composantes de la gestion des crises ;
- Élaboration d'un processus de décision facilitant la gestion de la crise ;
- Caractérisation du Système Interactif d'Aide à la Décision ;
- Construction d'un prototype du système d'aide à la décision ;
- Identification des problèmes lors du passage du modèle au cas réel ;

Nous avons commencé par une revue de la littérature selon deux points de vue, comme indiqué dans l'introduction - à savoir : Modèle de vulnérabilité pour aider à la prise de décision suite à une crise de catastrophe. Nous avons analysé la vulnérabilité et l'avons différenciée du risque. Cet état de l'art a permis d'identifier les éléments à intégrer dans notre futur modèle. L'objectif était de répondre à la question : Quels sont les éléments qui interagissent et qui pourraient rendre un élément vulnérable ou non vulnérables ? Deux types de composantes ont émergés. La première statique, et la seconde dynamique. Les facteurs dynamiques sont responsables des interdépendances à l'intérieur du système global. Ensuite, nous avons investi la notion d'interdépendance. Nous avons identifié une partie fonctionnelle qui représente la relation de dépendance et une partie dysfonctionnelle se rapportant à l'influence. Le défi était d'intégrer ces notions dans la modélisation des réseaux à l'aide de la théorie des graphes. L'approche de modélisation que nous avons proposée prend en compte toutes les configurations possibles des réseaux d'infrastructure. Ensuite, nous avons proposé un modèle d'évaluation de la vulnérabilité. Avec ce modèle, il est possible de déterminer entre autres la vulnérabilité d'un composant ou celle du réseau entier. Il modèle confirme le point de vue de nombreux auteurs, à savoir que la vulnérabilité est composée de robustesse et de résilience. L'évaluation de la vulnérabilité n'étant pas une fin en soi, elle doit conduire à la décision. Par conséquent, chaque composant de la décision dans un contexte de crise a été identifié et décrit. Le processus proposé peut être utilisé dans divers situation de crise identifié. Il fait référence à la méthode multicritère d'agrégation la mieux adaptée. Dans le but de fournir aux décideurs un outil informatique, nous avons caractérisé les Systèmes Interactifs d'Aide à la Décision et construit un prototype. Ce prototype n'implémente pas toutes les fonctionnalités. Il est toujours en cours de développement à la rédaction de ce manuscrit. La dernière contribution dans cette thèse a été de signaler tous les problèmes qui se sont produites dans l'application du modèle au cas réel. Avec notre contribution les décideurs trouverons des éléments de réponse aux questions suivantes :

- Qu'est ce qui est à craindre?: événement, scénario, configuration du système ;
- Qu'est ce qui est vulnérable?: simple composant, réseau, enjeu, territoire ;
- Que peut-on faire?: action sur un ou plusieurs élément (s) du système global ;
- Comment on peut on le faire?: les processus de décision, l'approche d'agrégation ;

Ces résultats conduisent à certaine perspectives dans la section suivante.

### ✓ *Perspectives*

---

Les résultats obtenus dans cette thèse sont tout à fait satisfaisants. Mais ils pourraient être améliorés par le biais de certains éléments de nos perspectives résumé dans ce qui suit :

- Utilisation de système Multi Agent pour une simulation de grande échelle ;
- Déploiement de l'outil sur l'internet et dans les appareils mobiles ;
- Intégration de la collaboration entre les décideurs ;

- Prise en compte de l'impact direct de l'événement redouté sur les enjeux ;
- Intégration de la mode de défaillance du composant après l'occurrence de l'événement redouté.

L'utilisation de l'approche Multi Agent semble indiquée à plus d'un titre. Dans le cadre de cette thèse, un agent pourrait être considéré comme un module informatique autonome et capable de prendre des décisions dans un environnement incertain. De ce point de vue, les éléments du modèle pourraient être considérés comme des agents interagissant. Cela favorisera l'émergence de nouvelles structures dans le réseau. Ces structures ne sont pas directement accessibles par analyse humaine. En outre, l'utilisation de système Multi Agent offre la possibilité de déterminer des actions alors que les décideurs sont eux-mêmes touchés par l'événement redouté. Cette situation est malheureusement très fréquente en cas de catastrophe naturelle. Un autre point à mentionner est que l'approche multi-agents est adaptée pour la simulation des systèmes complexes et un modèle de vulnérabilité peut être considéré comme un système complexe.

Nous l'avons déjà souligné l'importance de la distribution de logiciels. Par distribution, nous entendons la répartition géographique. Un logiciel situé à différents endroits semble être moins vulnérable que lorsqu'il est situé dans un endroit unique. En outre, son utilisation et sa capacité de survie sera plus grande lorsqu'il est déployé sur tablette et appareils mobiles. À ce niveau, le logiciel peut être construit de manière collaborative. Par exemple, les utilisateurs peuvent déterminer la localisation exacte des facteurs d'aggravation, des composants affectés etc.

Dans cette thèse, nous nous sommes intéressés seulement à l'effet indirect des événements redoutés. Notre modèle pourrait être améliorée en prenant en compte l'impact direct sur les enjeux. Dans les situations réelles, ce sont les effets directs qui sont souvent investis. En outre, la défaillance d'un composant n'est pas binaire. L'effet de l'événement redouté est lié au mode de défaillance du composant. Un composant affecté résistera ou non en fonction de sa structure.



## REFERENCES

- [1] F. Leone, « Caractérisation des vulnérabilités aux catastrophes « naturelles » : contribution à une évaluation géographique multirisque (mouvements de terrain, séismes, tsunamis, éruptions volcaniques, cyclones) », Habilitation à Diriger des Recherches, Université Paul Valéry, Montpellier III, Montpellier, 2007.
- [2] J.-F. Gleyze, « La vulnérabilité structurelle des réseaux de transport dans un contexte de risques », Université Paris 7 - Denis Diderot, Paris, 2005.
- [3] E. Michel-Kerjan, « Vulnérabilité financière face aux « risques à grande échelle » : la parole est à la première industrie au monde », *Responsabilité & Environnement*, n° 43, p. 14-28, juill. 2006.
- [4] J. L. Gross et J. Yellen, *Handbook of Graph Theory*. CRC Press, 2003.
- [5] V. Baláž, V. Kvasnička, et J. Pospíchal, « Two metrics in a graph theory modeling of organic chemistry », *Discrete Applied Mathematics*, vol. 35, n° 1, p. 1-19, janv. 1992.
- [6] J. Tang, « Mechanical system reliability analysis using a combination of graph theory and Boolean function », *Reliability Engineering & System Safety*, vol. 72, n° 1, p. 21-30, avr. 2001.
- [7] O. Shai et K. Preiss, « Graph theory representations of engineering systems and their embedded knowledge », *Artificial Intelligence in Engineering*, vol. 13, n° 3, p. 273-285, juill. 1999.
- [8] M. Barthelemy, « Betweenness Centrality in Large Complex Networks », *cond-mat/0309436*, sept. 2003.
- [9] A. J. Holmgren, « Using graph models to analyze the vulnerability of electric power networks », *Risk Anal*, vol. 26, n° 4, p. 955-969, août 2006.
- [10] E. W. Weisstein, « Scale-Free Network -- from Wolfram MathWorld », 10:07:00. [Online]. Available: <http://mathworld.wolfram.com/Scale-FreeNetwork.html>. [Accessed: 28-déc-2010].
- [11] P. Crucitti, V. Latora, M. Marchiori, et A. Rapisarda, « Error and Attack Tolerance of Complex Networks », 2004.
- [12] M. E. J. Newman, « The structure and function of complex networks », *cond-mat/0303516*, mars 2003.
- [13] L. Dall'Asta, A. Barrat, M. Barthelemy, et A. Vespignani, « Vulnerability of weighted networks », *physics/0603163*, mars 2006.

- [14] Å. J. Holmgren, « A Framework for Vulnerability Assessment of Electric Power Systems », in *Critical Infrastructure*, Springer Berlin Heidelberg, 2007, p. 31-55.
- [15] M. Cioca et L.-I. Cioca, « Decision Support Systems used in Disaster Management », *InTech*, janv-2010.
- [16] T. Thedéen, « Vulnerability of Infrastructures », in *Risks in Technological Systems*, Springer London, 2010, p. 161-173.
- [17] R. Benoît et M. Luviano, *Réduire la Vulnérabilité des infrastructures essentielles*, TEC & DOC. France: Lavoisier, 2009.
- [18] Y. Y. Haimes, « On the Definition of Vulnerabilities in Measuring Risks to Infrastructures », *Risk Analysis*, vol. 26, n° 2, p. 293-296, avr. 2006.
- [19] J. Johanson, « Risk and vulnerability Analysis of Interdependent Technical Infrastructures », Lund University, Dept. of Measurement Technology and Industrial Electrical Engineering, 2010.
- [20] G. Laurentius, « The vulnerability of the city », *Geographical Reports*, vol. Planning a Hight Resilience Society, n° 11, 1994.
- [21] K. Berdica, « An introduction to road vulnerability: what has been done, is done and should be done », *Transport Policy*, vol. 9, n° 2, p. 117-127, avr. 2002.
- [22] United States., *Critical foundations : protecting America's infrastructures : the report of the President's Commission on Critical Infrastructure Protection*. [Washington DC]: The Commission ;[Supt. of Docs. U.S. G.P.O. distributor, 1997.
- [23] I. Eusgeld, C. Nan, et S. Dietz, « "System-of-systems" approach for interdependent critical infrastructures », *Reliability Engineering & System Safety*, vol. 96, n° 6, p. 679-686, juin 2011.
- [24] J. Johansson, H. Jonsson, et H. Johansson, « Analysing the vulnerability of electric distribution systems: a step towards incorporating the societal consequences of disruptions », *International Journal of Emergency Management*, vol. 4, n° 1, p. 4 - 17, 2007.
- [25] W. A. Wallace et F. D. Balogh, « Decision Support Systems for Disaster Management », *Public Administration Review*, vol. 45, p. 134-146, janv. 1985.
- [26] D. E. Snediker, A. T. Murray, et T. C. Matisziw, « Decision support for network disruption mitigation », *Decis. Support Syst.*, vol. 44, n° 4, p. 954-969, mars 2008.
- [27] S. H. Strogatz, « Exploring complex networks », *Nature*, n° 410, p. 268-276, 2001.

- [28] R. Criado, J. Flores, B. Hernández-Bermejo, J. Pello, et M. Romance, « Effective measurement of network vulnerability under random and intentional attacks », *Journal of Mathematical Modelling and Algorithms*, vol. 4, n° 3, p. 307-316, nov. 2005.
- [29] A. Yazdani et P. Jeffrey, « A note on measurement of network vulnerability under random and intentional attacks », *1006.2791*, juin 2010.
- [30] B. C. Ezell, « Infrastructure Vulnerability Assessment Model (I-VAM) », *Risk Analysis*, vol. 27, n° 3, p. 571-583, juin 2007.
- [31] P. Crucitti, V. Latora, et M. Marchiori, « A topological analysis of the Italian electric power grid », *Physica A: Statistical Mechanics and its Applications*, vol. 338, n° 1-2, p. 92-97, juill. 2004.
- [32] J. M. Anthonisse, « Stichting Mathematisch Centrum », Technical Report BN 9/71, 1971 (unpublished), 1977.
- [33] P. Holme, B. J. Kim, C. N. Yoon, et S. K. Han, « Attack vulnerability of complex networks », *Phys. Rev. E*, vol. 65, n° 5, p. 056109, mai 2002.
- [34] L. Dueñas-Osorio, J. I. Craig, et B. J. Goodno, « Seismic response of critical interdependent networks », *Earthquake Engng Struct. Dyn.*, vol. 36, n° 2, p. 285-306, févr. 2007.
- [35] E. Bompard, M. Maserà, R. Napoli, et F. Xue, « Assessment of Structural Vulnerability for Power Grids by Network Performance Based on Complex Networks », in *Critical Information Infrastructure Security*, vol. 5508, Springer Berlin / Heidelberg, 2009, p. 144-154.
- [36] S. Arianos, E. Bompard, A. Carbone, et F. Xue, « Power grids vulnerability: a complex network approach », *0810.5278*, oct. 2008.
- [37] V. Latora et M. Marchiori, « Vulnerability and protection of infrastructure networks », *Phys. Rev. E*, vol. 71, n° 1, p. 015103, janv. 2005.
- [38] P. Crucitti, V. Latora, et M. Marchiori, « Model for cascading failures in complex networks », *Phys. Rev. E*, vol. 69, n° 4, p. 045104, avr. 2004.
- [39] V. Latora et M. Marchiori, « Efficient behavior of small-world networks », *Phys. Rev. Lett.*, vol. 87, n° 19, p. 198701, nov. 2001.
- [40] U. Brandes, « A faster algorithm for betweenness centrality », *Journal of Mathematical Sociology*, vol. 25, n° 2, p. 163-177, 2001.
- [41] L. Zhao, K. Park, et Y.-C. Lai, « Attack vulnerability of scale-free networks due to cascading breakdown », *Phys. Rev. E*, vol. 70, n° 3, p. 035101, 2004.
- [42] A. Jamakovic et P. Van Mieghem, « On the robustness of complex networks by using the algebraic connectivity », Berlin, Heidelberg, 2008, p. 183-194.

- [43] R. Kast, *La théorie de la décision*. La Découverte, 1993.
- [44] A. Tsoukiàs, « De la théorie de la décision à l'aide à la décision ». 2003.
- [45] « RAND at a Glance | RAND ». [Online]. Available: <http://www.rand.org/about/glance.html>. [Accessed: 19-avr-2013].
- [46] P. Lévine et J. Pomerol, *Systèmes interactifs d'aide à la décision et systèmes experts*. Hermès, 1989.
- [47] B. Roy et D. Bouyssou, *Aide multicritère à la décision méthodes et cas*. Paris: Économica, 1993.
- [48] H. Mintzberg, *The Structuring of Organization: A Synthesis of the Research*. Prentice-Hall, 1979.
- [49] H. A. Simon, *The new science of management decision*. Prentice-Hall, 1977.
- [50] A. Adla, « Aide à la facilitation pour une prise de décision collective : proposition d'un modèle et d'un outil », Université Toulouse III - Paul Sabatier Discipline ou spécialité : Informatique, Toulouse, 2010.
- [51] D. Trentesaux, « Conception d'un système de pilotage distribué, supervisé et multicritère pour les systèmes automatisés de production », Institut National Polytechnique de Grenoble - INPG, 1996.
- [52] B. Roy, *Méthodologie multicritère d'aide à la décision*. Paris: Économica, 1985.
- [53] B. Longueville, « Capitalisation des processus de décision dans les projets d'innovation: Application à l'automobile », Ecole Centrale Paris, 2003.
- [54] M. Merad, *Aide à la décision et expertise en gestion des risques*. Tec & Doc Lavoisier, 2010.
- [55] W. Taggart et D. Robey, « Minds and Managers: On the Dual Nature of Human Information Processing and Management », *The Academy of Management Review*, vol. 6, n° 2, p. 187, avr. 1981.
- [56] R. Rosness et J. Hovden, « From power games to hot cognition – a contingency model of safety related decision-making », presented at the Workshop on Decision Making under Uncertainty, 2001.
- [57] J.-P. Lavergne, *La décision : psychologie et méthodologie*, Les éditions E.S.F. Paris: , 1983.
- [58] J. C. COURBON, « Processus de décision et aide à la décision », *Economies et Sociétés*, vol. XVI, n° 12, p. 1455-1476, 1992.
- [59] A. SEGUY, « DÉCISION COLLABORATIVE DANS LES SYSTÈMES DISTRIBUÉS: APPLICATION À LA E-MAINTENANCE », University of Toulouse, Toulouse, 2008.
- [60] J. Stal-Le Cardinal, « Etude des dysfonctionnement dans la prise de décision. Application au choix d'acteur », Ecole Centrale de Paris, Paris, 2000.
- [61] M. S. S. Morton, *Management Decision Systems: Computer-Based Support of Decision Making*. Harvard University Press, 1971.

- [62] L. Y. Maystre, J. Pictet, et J. Simos, *Méthodes multicritères ELECTRE: description, conseils pratiques et cas d'application à la gestion environnementale*. PPUR presses polytechniques, 1994.
- [63] A. Guitouni et J.-M. Martel, « Tentative guidelines to help choosing an appropriate MCDA method », *European Journal of Operational Research*, vol. 109, n° 2, p. 501-521, sept. 1998.
- [64] A. Nafi et C. Wery, « Aide à la décision multicritère : introduction aux méthodes d'analyse multicritère de type ELECTRE ». ENGEES Ingénierie Financière, 2010.
- [65] P. Vincke, *L'aide multicritère à la décision*. Ellipses Marketing, 1998.
- [66] M. Merad, « Processus d'aide à la décision en gestion des risques », Université de Paris Dauphine, Paris, 2011.
- [67] C. Zopounidis et M. Doumpos, « Multicriteria classification and sorting methods: A literature review », vol. 138, n° 2, p. 229-246, 2002.
- [68] R. Ginting, « Intégration du système d'aide à la décision et du système d'intelligence économique dans l'ère concurrentielle », l'Université de droit et des sciences d'Aix-Marseille, 2000.
- [69] J. Figueira, V. Mousseau, et B. Roy, « ELECTRE Methods », in *Multiple Criteria Decision Analysis: State of the Art Surveys*, Springer New York, 2005, p. 133-153.
- [70] J. Figueira, V. Mousseau, et B. Roy, « ELECTRE Methods », vol. 78, 2005, p. 1-35.
- [71] A. Wilhelmsson et J. Johanson, « Assessing Response System Capabilities of Socio Technical Systems », 2009.
- [72] International Electrotechnical Commission, *Application of Markov techniques- norme IEC 61165*. 2006.
- [73] IEC, *Norme internationale CEI 61165: Application des techniques de Markov, édition bilingue français-anglais, édition 2006*, 2e édition. IEC, 2007.
- [74] G. Leonardo et Z. Rodríguez, « L'émergence de la complexité dans l'histoire de la science », Toulouse, avr-2011.
- [75] F. F.G., « Decision support and control for large-scale complex systems », *Annual Reviews in Control*, vol. 32, n° 1, p. 61-70, avr. 2008.
- [76] H. Jönsson et J. Johansson, « Identifying critical components in technical infrastructure networks », *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, vol. 222, n° 2, p. 235-243, juin 2008.
- [77] E. Zio, « Vulnerability assessment of critical infrastructures », 2009.

- [78] S. Wang, L. Hong, M. Ouyang, J. Zhang, et X. Chen, « Vulnerability analysis of interdependent infrastructure systems under edge attack strategies », *Safety Science*, vol. 51, n° 1, p. 328-337, janv. 2013.
- [79] Council, Scientific And Technical, « Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures », p. 1-51, 2006.
- [80] F. Ravat, « Modèles et outils pour la conception et la manipulation de systèmes d'aide à la décision », Habilitation à Diriger des Recherches, Université de Toulouse 1, Institut de Recherche en Informatique de Toulouse (IRIT), 2007.
- [81] J. Johansson et H. Hassel, « An approach for modelling interdependent infrastructures in the context of vulnerability analysis », *Reliability Engineering & System Safety*, vol. 95, n° 12, p. 1335-1344, déc. 2010.
- [82] R. G. Little, « Toward more robust infrastructure: observations on improving the resilience and reliability of critical systems », presented at the Proceedings of the 36th Annual Hawaii International Conference on System Sciences, 2003, 2003.
- [83] « President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures (1997). [Online]. Available: <http://www.ciao.gov> ». .
- [84] I. I. Earl E. Lee, J. E. Mitchell, et W. A. Wallace, « Assessing Vulnerability of Proposed Designs for Interdependent Infrastructure Systems », Los Alamitos, CA, USA, 2004, vol. 2, p. 20054c.
- [85] J. Gottmann, « The evolution of the concept of territory », *Social Science Information*, vol. 14, n° 3, p. 29-47, janv. 1975.
- [86] G. Le Boulch, « The Dynamic Concept of Territory in a Globalized World », in *17th EGOS Colloquium*, 2001, p. ?
- [87] I. B. Utne, P. Hokstad, et J. Vatn, « A method for risk modeling of interdependencies in critical infrastructures », *Reliability Engineering & System Safety*, vol. 96, n° 6, p. 671-678, juin 2011.
- [88] J. B. Dugan, K. J. Sullivan, et D. Coppit, « Developing a Low-Cost, High-Quality Software Tool for Dynamic Fault Tree Analysis », 1999.
- [89] B. c Ezell, J. V. Farr, et I. Wiese, « Infrastructure Risk Analysis Model », *Journal of Infrastructure Systems*, vol. 6, n° 3, 2000.
- [90] C. for C. P. S. (CCPS) et D. et.al, *Guidelines for Hazard Evaluation Procedures, with Worked Examples*, 2<sup>e</sup> éd. Wiley-AIChE, 1992.
- [91] D. Kamissoko, F. Pérès, et P. Zaraté, « Infrastructure Network Vulnerability », presented at the 20th IEEE International conference on Collaboration Technologies and Infrastructures, Paris, 2011.
- [92] S. Kaplan et B. J. Garrick, « On The Quantitative Definition of Risk », *Risk Analysis*, vol. 1, n° 1, p. 11-27, mars 1981.

- [93] S. M. Rinaldi, J. P. Peerenboom, et T. K. Kelly, « Identifying, understanding, and analyzing critical infrastructure interdependencies », *Control Systems, IEEE*, vol. 21, n° 6, p. 11-25, 2001.
- [94] G. BOARU et G.-I. BĂDIȚA, « CRITICAL INFRASTRUCTURE INTERDEPENDENCIES », presented at the Conference on Defense Resources Management, Braşov, 2008.
- [95] R. Albert, H. Jeong, et A.-L. Barabasi, « Error and attack tolerance of complex networks », *Nature*, vol. 406, n° 6794, p. 378-382, juill. 2000.
- [96] Hogarth R.M. et Kunreuther H., « Decision making under ignorance: arguing with yourself. », *Insurance: Mathematics and Economics*, vol. 16, p. 281, juill. 1995.
- [97] J. Agarwal, D. Blockley, et N. Woodman, « Vulnerability of structural systems », *Structural Safety*, vol. 25, n° 3, p. 263-286, juill. 2003.
- [98] A. Leroy et J.-P. Signoret, *Le risque technologique*. France: Presses Universitaires de France (PUF), 1992.
- [99] J. C. Chicken, *Managing Risks and Decisions in Major Projects*. Thomson Learning, 1994.
- [100] R. M. Wideman, *Project and Program Risk Management: A Guide to Managing Project Risks and Opportunities*, Preliminary Ed. for Trial Use. Project Management Institute, 1992.
- [101] W. O'Shaughnessy, *La faisabilité de projet : Une démarche vers l'efficience et l'efficacité*. Les éditions SMG, 1992.
- [102] R. Gouriveau, « Analyse des risques : Formalisation des connaissances et structuration des données pour l'intégration des outils d'étude et de décision », Institut National Polytechnique de Toulouse, 2003.
- [103] PMI Project Management Institute, *A Guide to the Project Management Body of Knowledge (PMBOK Guide) -- 2000 Edition*, 2000 ed. Project Management Institute, 2000.
- [104] P. Simon, *Project Risk Analysis and Management Guide: PRAM*. APM Group Ltd, 1997.
- [105] R. Manian, J. Bechta Dugan, D. Coppit, et K. J. Sullivan, « Combining various solution techniques for dynamic fault tree analysis of computer systems », presented at the High-Assurance Systems Engineering Symposium, 1998. Proceedings. Third IEEE International, 1998, p. 21-28.
- [106] G. W. Klau et R. Weiskircher, « Robustness and Resilience », in *Network Analysis*, U. Brandes et T. Erlebach, Éd. Springer Berlin Heidelberg, 2005, p. 417-437.
- [107] M. Snelder, H. J. van Zuylen, et L. H. Immers, « A framework for robustness analysis of road networks for short term variations in supply », *Transportation Research Part A: Policy and Practice*, vol. 46, n° 5, p. 828-842, juin 2012.
- [108] « IEEE Std 610.12-1990, IEEE Standard Glossary of Software Engineering Terminology, 1990. » .

- [109] M. A. Salido, F. Barber, et L. Ingolotti, « Robustness for a single railway line: Analytical and simulation methods », *Expert Systems with Applications*, vol. 39, n° 18, p. 13305-13327, déc. 2012.
- [110] A. B. Wildavsky, « Searching for Safety ». New Brunswick, NJ: Transaction., 1988.
- [111] J. F. Home et J. E. Orr, « Assessing behaviors that create resilient organizations », *Employment Relations Today*, vol. 24, n° 4, p. 29–39, 1997.
- [112] Asian Disaster Preparedness Center, « COMMUNITY-BASED DISASTER RISK MANAGEMENT ». .
- [113] K. Tierney et M. Bruneau, « Conceptualizing and Measuring Resilience, A key to Disaster Loss Reduction ». .
- [114] G. van Kessel, « The ability of older people to overcome adversity: A review of the resilience concept », *Geriatric Nursing*, vol. 34, n° 2, p. 122-127, mars 2013.
- [115] J. Cabanyes Truffino, « Resiliencia: una aproximación al concepto », *Revista de Psiquiatría y Salud Mental*, vol. 3, n° 4, p. 145-151, oct. 2010.
- [116] L. H. Gunderson, *Panarchy: Understanding Transformations in Human and Natural Systems*. Island Press, 2001.
- [117] S. Einarsson et M. Rausand, « An Approach to Vulnerability Analysis of Complex Industrial Systems », *Risk Anal*, vol. 18, n° 5, p. 535-546, oct. 1998.
- [118] P. Hellstom et T. Kvist, « Eval-u-a-tion of deci-sion sup-port mod-ules and human inter-faces using the Top-Sim sim-u-la-tor », presented at the 5th World Con-gress on Rail-way Research (WCRR 2001), Cologne, Ger-many, 2001.
- [119] S. Eom et E. Kim, « A survey of decision support system applications (1995–2001) », *Journal of the Operational Research Society*, vol. 57, n° 11, p. 1264-1278, déc. 2005.
- [120] J. P. Shim, M. Warkentin, J. F. Courtney, D. J. Power, R. Sharda, et C. Carlsson, « Past, present, and future of decision support technology », *Decision Support Systems*, vol. 33, n° 2, p. 111-126, juin 2002.
- [121] R. H. Sprague, « A framework for the development of decision support systems », *MIS Q.*, vol. 4, n° 4, p. 1–26, déc. 1980.
- [122] M. Demarest, « Technology and Policy in Decision Support Systems ». DP Applications, Inc., janv-1998.
- [123] T. W. Harding, F. Romerio, C. Frischknecht, et J.-J. Wagner, *Management des risques majeurs: des disciplines à l'interdisciplinarité*. Programme plurifacultaire du Rectorat Management des Risques Majeurs, 2001.



- [124] R. Ginting et H. Dou, « L'approche multidécideur multicritère d'aide à la décision ». Institute de Technologie d'Indonésie, Serpong-Tangerang 15320, Indonesia, 2000.
- [125] D. Kamissoko, P. Zaraté, et F. Pérès, « Decision aid problems criteria for infrastructure networks vulnerability analysis », presented at the International Conference on Control, Decision and Information Technologies (CoDIT'13), Hammamet, Tunisia, 2013.
- [126] D. Baker, D. Bridges, R. Hunter, et G. Johnson, « Guidbook to decision-making methods ». Department of Energy, USA, 2001.
- [127] P. Zaraté, « Conception et mise en oeuvre de systèmes interactifs d'aide à la décision: application à l'élaboration des plannings de repos du personnel navigant », Université Paris Dauphine, Paris, 1991.
- [128] D. Kamissoko, F. Pérès, et P. Zaraté, « Technological networks robustness and resilience assessment », presented at the 5th International Conference on Industrial Engineering and Systems Management, Rabat, Morocco, 2013.
- [129] M. Reghezza, « Réflexions autour de la vulnérabilité métropolitaine : la métropole parisienne face au risque de crue centennale », Université Paris X, Nanterre, 2006.
- [130] M. Behzadian, R. B. Kazemzadeh, A. Albadvi, et M. Aghdasi, « PROMETHEE: A comprehensive literature review on methodologies and applications », *European Journal of Operational Research*, vol. 200, n° 1, p. 198-215, janv. 2010.
- [131] Y. Leung et N. T. Shatin, *Intelligent Spatial Decision Support Systems*. Springer-Verlag Berlin and Heidelberg GmbH & Co. K, 1997.
- [132] S. Alter, « A work system view of DSS in its fourth decade », *Decision Support Systems*, vol. 38, n° 3, p. 319-327, déc. 2004.
- [133] R. H. Sprague et E. D. Carlson, *Building effective decision support systems*. Prentice-Hall, 1982.
- [134] R. D. Hackathorn et P. G. W. Keen, « Organizational Strategies for Personal Computing in Decision Support Systems », *MIS Quarterly*, vol. 5, n° 3, p. 21-27, sept. 1981.
- [135] A. K. Aggarwal, « A TAXONOMY OF SEQUENTIAL DECISION SUPPORT SYSTEMS ». *Informing Science*, juin-2001.
- [136] *Lecture - 1 Introduction to Software Engineering*. India: IIT Bombay, 2008.
- [137] C. Larman et V. R. Basili, « Iterative and incremental developments. a brief history », *Computer*, vol. 36, n° 6, p. 47-56, 2003.
- [138] B. W. Boehm, « A spiral model of software development and enhancement », *Computer*, vol. 21, n° 5, p. 61-72, 1988.

- [139] « StarUML, The Open Source UML/MDA Platform ». [Online]. Available: <http://staruml.sourceforge.net/en/>. [Accessed: 10-avr-2013].
- [140] P. Roques, *UML 2 par la pratique: études de cas et exercices corrigés*. Eyrolles, 2009.
- [141] « Balsamiq Mockups ». [Online]. Available: <http://www.balsamiq.com/>. [Accessed: 09-avr-2013].
- [142] « Eclipse Java EE IDE for Web Developers ». [Online]. Available: <http://www.eclipse.org/>. [Accessed: 09-avr-2013].
- [143] « JUNG, Java Universal Network/Graph Framework ». [Online]. Available: <http://jung.sourceforge.net/index.html>. [Accessed: 10-avr-2013].
- [144] Asghar, A. Damminda, et L. Churilov, « A dynamic integrated model for disaster management decision support systems », *International journal of simulation systems science technology*, vol. 6, n° 10-11, p. 95-114, 2005.

## PERSONAL PUBLICATION

- [1] D. Kamissoko, F. Pérès, et P. Zaraté, « Technological networks robustness and resilience assessment », presented at the 5th International Conference on Industrial Engineering and Systems Management, Rabat, Morocco, 2013.
- [2] D. Kamissoko, P. Zaraté, et F. Pérès, « Decision Support System for infrastructure network disruption management », presented at the PROCEEDINGS OF THE EWG-DSS THESSALONIKI-2013 WORKSHOP "EXPLORING NEW DIRECTIONS FOR DECISIONS IN THE INTERNET AGE ", Thessaloniki, GREECE, 2013.
- [3] D. Kamissoko, P. Zaraté, et F. Pérès, « Decision aid problems criteria for infrastructure networks vulnerability analysis », presented at the International Conference on Control, Decision and Information Technologies (CoDIT'13), Hammamet, Tunisia, 2013.
- [4] D. Kamissoko, F. Pérès, et P. Zaraté, « Infrastructure Network Vulnerability », presented at the 20th IEEE International conference on Collaboration Technologies and Infrastructures, Paris, 2011.
- [5] D. Kamissoko, F. Pérès, et P. Zaraté, « MODEL AND METHODOLOGY FOR INTERDEPENDENT CRITICAL SYSTEMS VULNERABILITY AND RISK ANALYSIS », presented at the La maitrise des risques des systèmes complexes, Tours, 2012.
- [6] D. Kamissoko, F. Pérès, et P. Zaraté, « Vulnérabilité des réseaux face aux catastrophes naturelles », presented at the Congrès des doctorants EDSYS 2013, Tarbes, 2023.

## GLOSSARY

DBMS	Data Base Management System
DSDM	Dynamic software development method
DSS	Decision Support System
EIS	Executive Information System
ELECTRE	Elimination Et Choix Traduisant la Réalité-
(Elimination and Choice Expressing the Reality)	
FEMA	Federal Emergency Management Agency)
GSS	Group Support System
HMI	Human Computer Interface
IDEF1X	Integration Definition for Information Modeling
IRGC	International Risk Governance Council
MCDA	Multicriteria Decision Aiding
MDA	Model Driven Architecture
MDBS	Model Based Management System
NIAM	Natural Language Analysis Method
RAND	Research and Development. The RAND
Corporation is a nonprofit institution that helps improve policy and decision making through research and analysis.	
ROMC	Representations, Operations, Memory Aids,
Control Mechanisms.	
RUP	Rational Unified Process
ULM	Unified Modeling Language

## ANNEXES