International Conference
on Industrial Engineering and Systems Management
IESM'2013
October 28 - 30, 2013
RABAT - MOROCCO

Technological networks robustness and resilience assessment*

Daouda KAMISSOKO [a], François PÉRÈS [b], Pascale ZARATÉ [c]

[a] *University of Toulouse, LGP/IRIT, Toulouse*

[b] *University of Toulouse, LGP, Tarbes*

[c] *University of Toulouse, IRIT, Toulouse*

Abstract

Infrastructure network failure such as power grid, gas and telecommunication systems might perturb societies well-functioning. A failure in the natural disaster context could lead to a crisis situation. This paper deals with robustness and resilience assessment of such systems under natural disaster. Through a case study, a methodology is presented. The way of including environmental relevant parameters is presented. Our method includes territory specifics, flow circulation, influence of mitigation and aggravation factors, feared event evaluation. We provide a vulnerability assessment methodology and formula. The approach is based on views from infrastructure initial and final states. Inherent vulnerability assessment constraints are also presented. We found that vulnerability is multi-views. It depends on the system robustness and resilience. Hence any analysis might begin by parameters identification. Parameters static and dynamic attributes are identified. Vulnerability analysis is not the end in itself. The analysis might lead to decisions to enhance weak points. This paper provides the foundation to go towards a decision aiding process.

Key words: risk, vulnerability, interdependence, interdependency, network, infrastructure, resilience, robustness

* This paper has not been presented at any other revue. Corresponding author D. Kamissoko. Tel. +33562442700. Fax +33 5 62 44 27 27

Email addresses: daouda.kamissoko@enit.fr (Daouda Kamissoko), francois.peres@enit.fr (François Pérès), pascale.zarate@irit.fr (Pascale Zaraté).

1. Introduction

Societies well-functioning rely on many aspects. Political stability and good finance seem to be obvious. On the technical aspect, infrastructure might furnish goods and services. Among these infrastructures, networks such as power grid, telecommunication and gas systems occupy a prominent place. In these recent years, these infrastructures have been threatened by a lot of disasters. The most current failure cause seems to be inherent to the conception and the working environment. Such failures are well assessed by network manager. They are more or less predictable. Less predictable events are natural disasters, terrorist attacks and human errors. Among these causes, natural disasters are the most unpredictable. They could affect state institutions, forests, habitations, firms, infrastructure networks etc. For instance, in March 2011, a tsunami in Japan made 18,079 deaths and many other consequences. But the part of consequence due to network failure is difficult to determine.

When a network is affected, one of the aggravation causes is the interdependence between different networks. For instance in July 2012, a blackout in India affected over 620 million people. Activity of the most affected area was paralysed. Because of these interdependences cascading failure could occur. The worst scenario is when a network included in interdependence is affected by a natural disaster. The 2010 volcanic eruption in Iceland well illustrated this situation. It affected about 20 countries. For these reasons it is important to determine the vulnerability of infrastructure networks. Vulnerability assessment is a good foundation to go forwards a crisis management.

Vulnerability, robustness and resilience assessment is investigated by many authors. Many of them focus on the network structure. Others focus on the management of furnished service. The best approach in our point of view is to take account of the network structure, dynamic, functions, and management. The objective of paper is to analyse crisis situation to determine vulnerabilities. Vulnerability has two components, robustness and resilience. We distinguish among others classes of vulnerability: Network vulnerability, Vulnerability of a territory like a city, stake vulnerability as human being or firm and the vulnerability induced by flow circulation. In this model, stakes are not supposed to be directly threatened by natural disasters. The aim is to assess the indirect vulnerability through critical networks. The methodology consists of modelling including parameters: External environment, territory specifics, flow circulation, aggravation and mitigation factors, and feared events. Graph theory is adopted for infrastructure modelling. Constraints of vulnerability component are also presented. For each component the assessment formula is given.

In this paper, we begin by describing a case study which illustrated all specificities of a vulnerability analysis. Next the methodology is described. It consists of the identification of the parameters of the models: External environment, Territory, Flow; Feared Events, Mitigation and Aggravation Factors. Afterwards, a simulation is performed to determine the system final state. The way of resilience and robustness assessment are then given. Last, the obtained results are analysed.

Our methodology is described through the case study presented in the next section.

2. Case study

In this paper the case study is a generic network presented in Figure 1. The network is depicted at it full blast. It is hosted by two territories T1 and T2. These territories are two cities administratively independent.

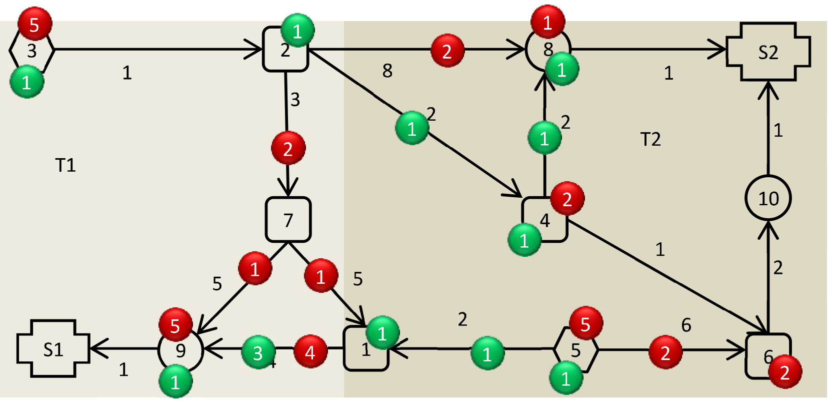

Figure 1: Case study

Two generic flows circulate in the networks: Electricity (Flow A in red) and Gas (flow B in 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 flows destinations. The number on each flow corresponds to its quantity. For instance there are 2 flows 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.

The methodology presented in the next section allows such situation assessment.

3. Methodology

Societies good functioning depends on hosted networks. We have identified 17 networks: Road, Air transportation, Shipping, Rail, Electricity, Gas, Hydro Carbide, Drinking Water, Hospital, waste and Nuclear Biological Chimical (NBC), Food, Information Technologies (IT), Telecommunication and GPS, Audio Visual, Post, Bank and Finance. There is no unanimous methodology for vulnerability analysis of such networks. Used tools and steps are often inspired from risk analysis. The methodology presented in this paper tries to answer the following questions:

- What is feared? This question is presented by some authors as "What can happen?"[1], [2];
- What is likely to be disrupted?
- What consequences this might have?

The used approach in this paper is based on graph theory. Critical infrastructure can be seen as set of Nodes and Edges. For example, in the power grid, nodes are power plants, and edges are lines between them. Network dynamic is illustrated by flow circulation. Then any network can be represented by graph with circulating flow inside [3].

Edge weight depends on the environment. The methodology begins by environment identification. In many realistic situation, infrastructure network provide many territories. Territory might be a city or a country. As a rule, territories are administratively independent. For this reason its specifics 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 events might encounter some factors that can mitigate or aggravate them. For example a flood barrier prevents territory from flood. The way of taking them into account is indicated.

From these elements network good functioning is determined by a nominal state. An 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 of environment, Territory, Flow, Mitigation and aggravation factors and feared events.
The following section discusses how the working environment influences the network model.

3.1. Environment

Figure 1 shows weighted edges. Edge weight is indicated by a number. For example the weight of the edge (7)-(1) is 5. Weight might be geodesic distance between nodes, or any relevant criteria for the analysis (cost, time). For 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: The season, 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 paper.

Edge weight determines the flows circulation. Because of that, environment affects the resulting robustness and resilience

Network might be hosted by many territories administratively independent. Territory attributes influencing the model are presented in the next section.

3.2. Territory

Territory is the geographic area gathering the other elements. Many territories might be deserved by a single network. Territories are administratively independent. Decisions taken by one of them might be different from even contradictory to others. Hence there is a need to separate them.

Territory is characterized by it limits, decisions makers, set of actions, feared events and a stretch. In the case study, territories stretches are respectively 10000000 m2, and 5000000 m2. They are threatened by an earthquake.

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

3.3. Flow

Flow circulates from source to target nodes according to circulation law. Flow circulation facility network is a vulnerability indicator [4]. We have identified 15 flows: Human, Electricity, Drinking water, Sewage, Information, Good, Gas, Car, Truck, Boat, Train, Hydro carbide, Waste, Plane and Money. They are characterized by a speed, and its circulation law [3].

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

- Path of flow B produced in (3) is: (3)➔(2)➔(4)➔(8)➔(11);
- Path of flow B produced in (5) is: (5)➔(1)➔(9)➔(12);
- The 5 flows A produced in (3) are distributed in five different paths:
    - (3)➔ (2)➔ (7)➔ (9)➔ (12);
    - (3)➔ (2)➔ (7)➔ (1)➔ (9)➔ (12);
    - (3)➔ (2)➔ (8)➔ (11);

  - (3)➔ (2)➔ (4)➔ (8)➔ (11);
  - (3)➔ (2)➔ (4)➔ (6)➔ (10)➔ (11).
- The 5 flow A produced in (5) are distributed in two paths:
  - Two flows follow the path (5)➔ (6)➔ (10)➔ (11);
  - Three flows follow (5)➔ (1)➔ (9)➔ (12).

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

3.4. Feared events

In the literature a feared event is sometimes called *Incident* or *Hazard* [5], [6]. The term *"Hazard"* is chosen here because according to common sense, a hazard is “a generic class grouping a set of potential causes as well as causes’ generators” [7]. In this paper, Hazard is defined as natural or anthropic phenomenon for which it’s not possible to predict together with the occurrence and the intensity, and susceptible to affect stake [3]. Thus, a hazard may be natural, climatic, technical, human, an act of sabotage, terrorism or war [8]. It is characterized by the fact that it has a negative influence on the network functioning [5].

In the nature, mainly, there are seven types of hazard that may affect the networks: earthquake, flood, volcano, tsunami, fire, cyclone, and storm. These hazards are dependent to each other. An earthquake can cause a tsunami or fire. In most cases, it is not necessary to analyse the critical system for all hazards.

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

Earthquake	Amplitude	4
	Frequency	0,128
	Stretch	5000000 m^2
	Speed	1000 m/s
	Duration	1000 ms

Table 1: Hazard parameters

From its occurrence point, hazard is situated at 1000 meters from node (7), 3000 meters from nodes (4) and (1); 2500 meters from edge (2)-(7); 2800 m 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 is presented in the following section.

3.5. Mitigation or aggravation factors

In the nature, some elements might mitigate or aggravate consequences to stakes. For example a dam can mitigate vulnerability related to flood, but its failure is an aggravation source. Factors are characterised by a type, amplitude and a stretch.

In the case study, the barrier near node (7) is an aggravation factor (A). Parameters of this factor are given in Table 2. This aggravation factor would increase the hazard amplitude of 2 point (+2) in a radius of 10 meters. From its position only the node (7) is in its stretch.

A	Amplitude	2
	Stretch	10 m
	Type	Hazard amplitude

Table 2: Aggravation factor parameters

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

4. System final state

Final state is obtained after hazard occurrence through a simulation. The simulation tools have been implemented in Java with the Eclipse IDE [9]. The user is invited to see [10] for more information. In the case study, when the hazard is insatiate it will affect only the node (7) in one second. Node (7) could resist the hazard amplitude. But because of the aggravation factor, the amplitude is rolled up to 6: Hazard amplitude plus aggravation factor amplitude (4+2). The node (7) will then break down after 1 second simulation.

At 2 second the edge (2)-(7) will go 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 2.

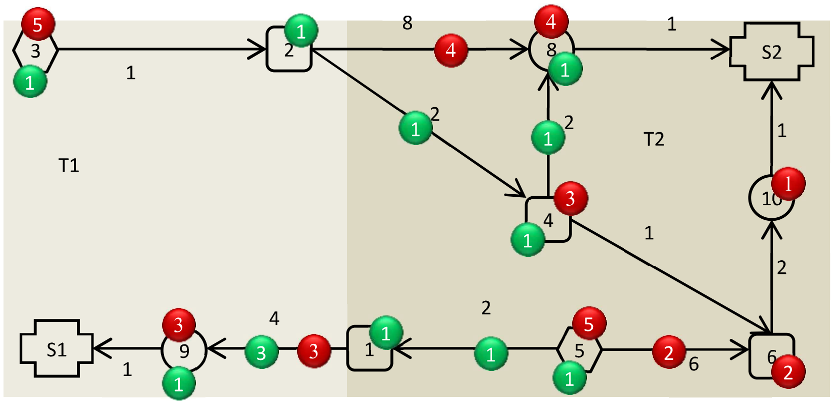

Figure 2: Network after hazard occurence

It can be observed that the network structure has changed. Flow repartition, and stake consumption have also changed. Initially, the consumption of the stake S1 and S2 were 5 flows A and 1 flow B. After the hazard occurrence, this consumption is now:

- For Stake S1: 3 flows A and 1 flow B;
- For Stake S2: 7 flows A and 1 flow B.

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

5. Vulnerability assessment

Vulnerability is "a stake's inability to resist the hazard's occurrence and to recover effectively to its nominal functioning for a given period of time" [3]. It includes two components: the structural component related to the network's physical organization (Robustness); and a functional component related to the movement of different fluxes (Resilience). Robustness is a static property. It defines the ability to withstand a constraint [11], and means that the system will maintain its functions intact when exposed to disturbances [8]. Resilience in turn, implies that the system can adapt and find a new stable position close to its initial state after the occurrence of the hazard [8]. According to these definitions, network state after hazard occurrence is needed for vulnerability assessment. There are many vulnerability classes. The more important are Network Vulnerability, Territorial vulnerability, Stake vulnerability and Component vulnerability. From this point of view, vulnerability is given by:

$$V = P(Hazard) \times \vartheta \qquad (1)$$

ϑ is the overall vulnerability induced by network components. $P(Hazard)$ is the probability associated to the hazards.

Vulnerability is assumed to be between 0 and 1. The system is assumed to be vulnerable if its vulnerability tends to be 1.

In case of many hazards the resulting probability is:

$$P(Hazard) = \mathrm{P}(\cup P_{j}{}_{j=1}^{J}) \qquad (2)$$

Where P_j is the probability of the hazard j, and J is the number of hazard.

For a composed component, vulnerability is the function of subcomponent vulnerability and given by:

$$\vartheta = 1 - \prod_{n=1}^{N}(1 - \vartheta_n) \qquad (3)$$

ϑ_n is the vulnerability of the component n, and N the number of component. Component includes nodes, edges and stakes.

ϑ_n depends on the resilience (R_s) and the robustness (R_b). To determine the function ϑ_n, many constraints might be satisfied.

$$\begin{cases} \vartheta_n \in [0,1]; \\ if\ R_s = 0\ and\ R_b = 0\ then\ \vartheta_n = 1; \\ if\ R_s = 1\ or\ R_b = 1\ then\ \vartheta_n = 0; \\ if\ R_b\ is\ contante\ then\ \vartheta_n\ decreases\ with\ the\ increase\ of\ R_s; \\ if\ \ R_s\ is\ contante\ then\ \vartheta_n\ decreases\ with\ the\ increase\ of\ R_b. \end{cases} \qquad (4)$$

Where R_s is the resilience and R_b is the robustness. From these constraints, the proper vulnerability is given by:

$$\vartheta_n = 1 - \ R_b \times \ R_s \qquad (5)$$

The resilience is defined as considering the nominal state of the system to be analysed and determining the stake's aptitude to recover this nominal state. Its assessment depends on actions efficiency and rapidity. It depends on the cumulated time of the bad functioning states (t_2), and those of the good functioning (t_1). Resilience assessment might respect some constraints presented in the following.

$$\begin{cases} if\ t2 = t1\ then\ \ R_s = 0{,}5; \\ if\ t2\ decreases\ then\ \ \ R_s\ increases; \\ \quad if\ t1\ decreases\ then\ \ \ R_s\ decreases. \end{cases} \qquad (6)$$

$$\mathrm{R_s} = \frac{t_1}{t_1 + t_2} \qquad (7)$$

For the case study, the new full blast is obtain after 6 second simulation, then $t1\ = 6$. $t2$ depends on existent corrective actions and decision makers reactivity. Actions might be adding new components, changing flow circulation law changing component resistance etc. The decision aiding process to determine the action is out of the scope of this paper. The reader is invited to see [12] for more information.

A component might be composed of many other components. In such situations, the resulting robustness is the product of its subcomponent robustness.

The robustness of a component depends on its flow consumption. Let us note that $C_{p1\mathrm{i}}$ is the component i consumption in flow p before the hazard and $C_{p2\mathrm{i}}$ it consumption after the hazard. R_{bpi} is the robustness inducing the flow p to the component i. Its assessment is under the following constraints:

$$\begin{cases} if\ C_{p2\mathrm{i}} = C_{p1\mathrm{i}}\ then\ R_{bpi} = 1 \\ if\ C_{p2\mathrm{i}} = C_{p1\mathrm{i}} = 0, then\ R_{bpi} = 1 \\ if C_{p2\mathrm{i}} =\ 0\ then\ R_{bdpi} = 0 \\ For\ \ C_{p2\mathrm{i}} > C_{p1\mathrm{i}}\ then\ R_{bpi}\ increases\ if\ C_{p2\mathrm{i}}\ increases \\ For\ \ C_{p2\mathrm{i}} < C_{p1\mathrm{i}}\ then\ R_{bpi}\ decreases\ if\ C_{p2\mathrm{i}}\ increases \end{cases} \qquad (8)$$

Robustness induced by a flow p to the component i for $C_{p2\mathrm{i}} \neq C_{p1\mathrm{i}}$ is given by:

$$R_{bpi} = 1 - \frac{|C_{p2\mathrm{i}} - C_{p1\mathrm{i}}|}{C_{p1\mathrm{i}} + C_{p2\mathrm{i}}} \qquad (9)$$

In case of many flows consumed by stake i, the resulting robustness is the product of robustness. Results of this approach are presented in the new section.

6. Results

Component	E1		E2		RbA	RbB	Rb	t1	t2	Rs	v
	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	0,333	1
Edge (7)-(9)	1				0	1	0	1	5	0,166	1
Edge (7)-(1)	1				0	1	0	1	5	0,166	1
Edge (1)-(9)	4	3	3	3	0,857143	1	0,86	6	0	1	0,14
Edge (9)-(S1)					1	1	1	6	0	1	0
Edge (2)-(8)	2		4		0,666667	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	0,833333	1	0,83	6	0	1	0,17

Table 3: Results

Table 3 shows simulation results for the case study. These numbers are obtained from Figure 1 (State E_1) and Figure 2 (State E_2) based on above formulae.

As shown in this table, many observations could be drawn:

- 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) illustrate this situation;
- Stakes are supposed to be hazard resistant, then their robustness might be different from 1 because of the flow circulation. For the stake S1, its consumption in flow A is dropped from 5 to 3. Those of the stake 2 for the same flow have increased from 5 to 7. For both of them the difference between initial and final flow is 2. But the result shows that S1 is more vulnerable than S2. 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 make sense. For this reason, they are supposed to be dynamically robust. From the results we can distinguish many classes of vulnerability: Network vulnerability, Territorial vulnerability, Component type vulnerability, Stake vulnerability, Flow vulnerability.

7. Conclusion

Natural disasters are stressful events for the society. Through the networks, they can affect many people and lead to a crisis situation. In this situation, any decisions can have consequences - sometimes irreversible damages - and need to be justified. It should lead to rational and objective choices.

The objective of this paper is to provide a methodology for infrastructure network vulnerability assessment through two components: robustness and resilience. Needed parameters for the assessment have been investigated. For each of them, relevant attributes are presented.

The approach is based on the system state before and after and hazards. From the initial state, a simulation is performed to obtain the final state. The vulnerability is then the function of the network structure, its dynamic, and its functions management.

The structure is taken into account through the number of component before and after the hazard. Dynamic is determine by flow. And the function and management is through the resilience. Indeed, the recovery time depends on the management capability to restore the system after a failure.

We found that vulnerability depends mostly on the resilience. Indeed, whatever the hazard is, the more the system recovers to its initial state, the less it is vulnerable. In addition, vulnerability is not only lack of flux. Flux surcharge might be a vulnerability source.

With our model, it can be deduced among others: optimal time to repair, response curve based on the scenarios, critical areas, the unpredictable and potentially damaging; component availability, critical components; vulnerability maps; component failure rate limit, etc.

Model presented in this paper does not take account of interferences between networks. Indeed, networks are linked from one to another. In such situations, failure of one component might lead to those of others. Analysis of cascading failure will be our future study.

8. Bibliography

[1] Y. Y. Haimes, « On the Definition of Vulnerabilities in Measuring Risks to Infrastructures », Risk Analysis, vol. 26, no 2, p. 293‑ 296, avr. 2006.

[2] J. Agarwal, D. Blockley, et N. Woodman, « Vulnerability of structural systems », Structural Safety, vol. 25, no 3, p. 263‑ 286, juill. 2003.

[3] D. Kamissoko, F. Pérès, et P. Zaraté, « Infrastructure Network Vulnerability », presented at the 20th IEEE International conference on Collaboration Technologies and Infrastructures, Paris, 2011.

[4] J. B. Dugan, K. J. Sullivan, et D. Coppit, « Developing a Low-Cost, High-Quality Software Tool for Dynamic Fault Tree Analysis », 1999.

[5] B. c Ezell, J. V. Farr, et I. Wiese, « Infrastructure Risk Analysis Model », Journal of Infrastructure Systems, vol. 6, no 3, 2000.

[6] K. Berdica, « An introduction to road vulnerability: what has been done, is done and should be done », Transport Policy, vol. 9, no 2, p. 117‑ 127, avr. 2002.

[7] C. for C. P. S. (CCPS) et D. et.al, Guidelines for Hazard Evaluation Procedures, with Worked Examples, 2e éd. Wiley-AIChE, 1992.

[8] Å. J. Holmgren, « A Framework for Vulnerability Assessment of Electric Power Systems », in Critical Infrastructure, Springer Berlin Heidelberg, 2007, p. 31‑ 55.

[9] « Eclipse Java EE IDE for Web Developers ». [Online]. Available: http://www.eclipse.org/. [Accessed: 09-avr-2013].

[10] 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.

[11] 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, no 1, p. 4 ‑ 17, 2007.

[12] 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.