Infrastructure network vulnerability

Daouda Kamissoko, François Peres, Pascale Zaraté

Infrastructure Network Vulnerability

Kamissoko Daouda
University of Toulouse
LGP-IRIT
Tarbes, France
daouda.kamissoko@enit.fr

Zaraté Pascale
University of Toulouse
IRIT
Toulouse, France
pascale.zarate@irit.fr

Pérès François
University of Toulouse
LGP
Tarbes, France
francois.peres@enit.fr

***Abstract*—The work presented in this paper aims to propose a methodology of analyzing infrastructure network vulnerability in the field of prevention or reduction of the natural disaster consequences. After a state of the art on vulnerability models in the academic literature, the various vulnerability factors are classified and discussed. Eventually, a general model of vulnerability analysis including societal parameters is presented.**

Keywords-risk; vulnerability; decision support; network; natural disaster; complex system, modelisation

I. INTRODUCTION

Our societies depend increasingly on complex infrastructure [1], [2], [3]. These infrastructures (transport, energy, telecommunication etc.) are critical and vital for the society [4], but are also vulnerable to hazards [3].

Systems represented by networks can aggravate or mitigate the hazard effects with respect to their use. The analysis of networks vulnerability is a way of prevention during the design phase in order to effectively integrate the networks in their environment, but also as a detection of critical elements throughout its exploitation phase.[5]. Hence there is a need for network and vulnerability models to analyze the performances before a feared event and to support decision in the crisis phase. This is the objective of our study because a network failure in some cases can cause paralysis of an entire country [6]. In the following lines we define the key concepts for the analysis of the vulnerability and risk before proceeding to a literature review of network modeling. We then describe the vulnerability models used in the literature. Following, we present the limitations of these models and introduce the elements to be incorporated. Finally, we comment the analysis model and conclude with some working perspectives.

II. CONCEPTS AND DEFINITIONS

The analysis of the vulnerability is often related to risk analysis [7]. The concept of vulnerability is sometimes confused with the risk in the literature [7], [8]. To distinguish the two concepts, let us consider a system to analyze (Figure 1).

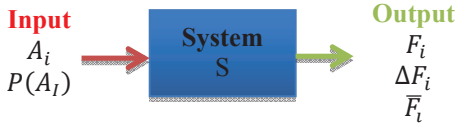

Figure 2: Elementary system to analyze

From the two standpoints (risk and vulnerability), the output may be represented by a function F_i (health of populations), a difference ΔF_i (increase of water consumption), a wrong output (bad information) $\overline{F_i}$, or a probability of one or more of these elements. The system input is described by uncertain causes (A_i) or a probability on these causes $P(A_i)$. Risk analysis deal with the Outputs and the Inputs without considering the structure and the dynamic of the system. The risk in this case is an entity composed of a probability ($P(A_i)$) on one hand and the consequences ($\overline{F_i}$ or ΔF_i) on the other hand [9]. Some authors consider the risk as the probability of an undesirable result ($P(\overline{F_i})$ or $P(\Delta F_i)$) [10] . Others authors define the risk as the cumulative effects of uncertain occurrences (A_i) adversely affecting ($\overline{F_i}$ or ΔF_i) the goals (F_i) [11], or the possibility that a fact (A_i) having undesirable consequences ($\overline{F_i}$) occur [12]. Reference [13] present the risk as the consequences ($\overline{F_i}$ or ΔF_i) of a set of causes (A_i) on the system. References [14] and [15] define risk as an uncertain event (A_i) or condition ($P(A_I)$) which, if it occurs, has a positive (F_i) or negative ($\overline{F_i}$) effects on a project objectives. All these authors take into interest the effects or consequences of the Inputs on the Outputs.

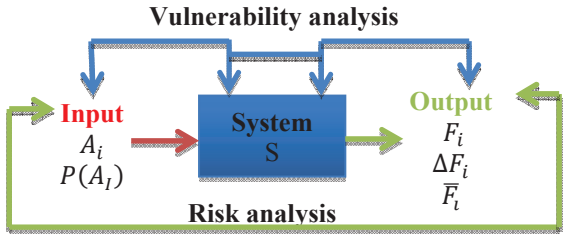

Figure 1: Risk and vulnerability analysis

The vulnerability is documented in various ways in the literature. Contrary to the risk analysis, vulnerability analysis is used to characterize the lack of robustness or lack of resilience of a system. [7], [16]. Robustness is the system's ability to resist to the random evolution of its environment while resilience is its ability to recover its nominal function following the occurrence of a disruption. We are then interested in the system itself (structure and function) rather than its Outputs or its Inputs. Vulnerability is often defined as "the probability of a complete or partial failure of infrastructures and loss of their ability to maintain their important functions for a certain period" [3], or as "the

propensity to damage or malfunction of various elements exposed to risk (commodities, peoples, activities, functions, systems) constituent a territory and a given society" [17]. Based on these definitions, the fundamental difference between risk and vulnerability 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).

We define the vulnerability and the risk considering three elements: The Population, the Territory and the Hazard

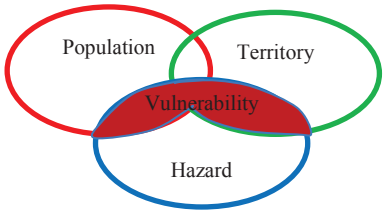

Figure 3 Elements of vulnerability

A. Stake

The stake is the union of *Population* and *Territory*. We define it like "a material or immaterial entity providing a function whose deterioration is damageable or prejudicial for the society. The term damage alludes to materials damage while losses refer to human lives [18] and prejudice concerns peoples damages [17]. The vulnerability analysis is on the intersection of hazard and stake. We will not talk about vulnerability in the case of a hazard that does not affect any stake.

B. Hazard

The vulnerability analysis assumes the presence of anthropic or natural phenomena which is not under control and that we call *Hazard*. The specificity of hazard 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 hazard. On the other hand, if for some reason, this intensity cannot be approximated with an acceptable leeway, the snowstorm becomes in this case a hazard. The accident is in this case a manifestation of a hazard.

It should be noted that a phenomenon which do not affect any stake could not be considered as a hazard. For instance, an earthquake in an inhabited area without infrastructure will not be a hazard whatever its frequency and its intensity. Others parameters than frequencies and intensities are to be taken into account in the hazard analysis. Like failure mode, number and detectability of heralds signs.

C. Population.

The consequences of hazard often depend on the societal position of the occurrence place [7]. The population is the group of people living on a given territory or likely to be affected by a hazard. It is the central element of our model and is divided into three dependents factors: psychological (stress, fear); physiological (age, sex, health), economical (healthiness or poverty).

D. Territory

The territory is the component that will mitigate or aggravate the hazard effect on the population. We have chosen to distinguish the territory from the population insomuch as there are some populations that have no stable territory[1]. On a territory we can distinguish various factors of vulnerability: soil and subsoil, infrastructures (networks and buildings), institutions, economy and environment. A distinction may be done between infrastructures like buildings, bridges and networks.

Networks are presents at all levels of our lives. There are four categories of networks [19]: technological networks (the electric power grid, the internet), information networks (network of citations between academic papers, World Wide Web), social networks (the patterns of friendships between individuals, business relationships between companies, intermarriages between families) and biological networks (genetic regulatory network, food web, Neural[2] networks) [19]. Technological networks are man-made networks for transporting materials and information. The hazard effects are felt by the population through perturbations of network performances. The vulnerability analysis might take into account the network structure, its dynamic and its background (Machinery, Manpower, Material, Measurement, and Method).

E. Vulnerability

Vulnerability has two main components. The robustness (or resistance) and the resilience. The resilience is defined considering the nominal state of the system to be analyzed and determine the stake's aptitude to recover this nominal state. We define the vulnerability as "the incapacity of a stake to resist to the occurrence of a hazard and to recover efficiently its nominal function during a given period of time". A stake can be vulnerable to a hazard without being exposed to this hazard. More a stake will resist to the hazard effects and will recover quickly its nominal functions less it will be vulnerable.

F. Risk

Sometimes, vulnerability is considered as a component of risk which is then perceived as the conjunction of hazard and vulnerability [20]. We define the risk as an exposition probability of a stake to a hazard and/or the probability of negatives consequences at a given time in specified conditions.

III. NETWORKS MODELLING

In the literature we often use the graph theory to model network. Most of the communication and transportations systems (technological networks) can be represented by a graph [21]. A finite graph $G = (V, E)$ is defined by a finite set of nodes $V = \{V_1, V_2 \ldots . V_N\}$; $(|V| = N)$ and a finite set of edge E } ( ). The analysis of

[1] This is true of some nomadic peoples. Otherwise territory can be uninhabited

[2] Referring to the topology of real neural networks

some structural parameters enables to quantify networks vulnerabilities. Following, we describe these parameters.

A. Degree

For a graph, a node degree is the sum of incoming and outgoing edges. For a node V_i the degree is: [22]:

$$d(V_i) = d^+(V_i) + d^-(V_i) \quad (1)$$

There are a lot of ways to quantify the edge degree in the literature [23]. The product of incident node degrees seems to be the best choice, because it offers the best correlation between the edge degree and the coefficient of centrality. For an edge E_i the degree is given by:

$$d(E_i) = d(V_i) \times d(V_k) \quad (2)$$

The degree is the vulnerability analysis parameter in an intuitive way [24] but not stand for determining the network global state [25]. The degree is not all the time the most important term of efficiency and vulnerability [2]. In the case of ponderated network, the weight is often used in place of degree. The degree is then the sum of edge weight [24].

B. Betweenness

The betweenness define the fraction of path going through a node V_i [23].

$$G(V_i) = \sum_{s \neq i \neq t} \frac{\sigma_{st}(i)}{\sigma_{st}} \quad (3)$$

Where σ_{st} is the number of total paths from the edge V_s to the edge V_t and $\sigma_{st}(i)$ is the number of paths going through V_i. The load is defined in the same way for an edge E_i [23].

$$G(E_{ij}) = \sum_{s \neq i \neq t} \frac{\sigma_{st}(i)}{\sigma_{st}} \quad (4)$$

The centrality determines the importance of a node in the network [23] and defines the resilience to attacks [26]. It is calculated before and after the occurrence of the hazard (which means the removal of one or many nodes/edges) [5], [22], [27].

C. Average Path Length

The average path length between two nodes is the mean of the edges number of shortest paths [16].

$$\ell = < l(V_i, V_j) > = \frac{1}{N(N-1)} \sum_{i \neq j \in V} D(V_i, V_j) \quad (5)$$

To avoid infinite mean (the distance is infinite if no link exists between the nodes), we use the inverse of the average path [22] and [23].

$$\ell' = \frac{1}{N(N-1)} \sum_i \sum_j \frac{1}{D(V_i, V_j)} \quad (6)$$

The average path measures the dispersion of the network and expresses the difficulty of transferring elements between two nodes. [4]. It also indicates the flow of traffic on the network.

D. 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 [16]. The number of possible connections for a vertex of degree $d(V_i)$ is [16]:

$$\binom{d(V_i)}{2} = \frac{d(V_i)[d(V_i)-1]}{2} \quad (7)$$

By noting M_i the number of links between vertices incident to vertex V_i, the clustering coefficient of vertex V_i is then [16]:

$$C_i = \frac{M_i}{\binom{2}{d(V_i)}} \quad (8)$$

And that of the graph is [16] and [23]:

$$C(G) = \frac{1}{N} \sum_i C_i \quad (9)$$

E. Connectivity:

The connectivity of vertices (respectively edges) of a graph is the minimum number of vertices (respectively edges) to remove from the graph to disconnect it [28] and [25]. A disconnected graph is a graph for which no element can reach its destination. Connectivity is a measure of vulnerability [16]. Connectivity of the vertices is also called cohesion of the graph and that of edges; adhesion of the graph. We can classify networks according to one of these parameters. We introduce below one of these classifications.

IV. MODELS OF NETWORK

From a structural point of view, we can classify networks according to their degree distribution P(k) [26]. This classification gives rise to three categories of network [16]: scale-free network, random graphs, and small word network.

A. Scale-free Network (Barbàsi-Albert)

These are networks for which the node fraction with a degree k follows a power law [29], [16], [26]:

$$P(k) \sim k^{-\gamma} \quad (10)$$

This is the case of networks like the power grids [29], the World Wide Web, the internet, and the air networks [5].

B. Random graph (Erdös-Rényi)

In general, in the Erdös-Rényi model, the probability that a vertex is of degree k is given by the binomial law [26], [16]:

$$P(k) = \binom{N-1}{k} p^k (1-p)^{N-1-k} \quad (11)$$

The average distance for these networks is proportional to $\log N$ [16].

C. Small word network

For these networks, the distance between two nodes decreases very slowly with the number of nodes [24]. 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 [16].

V. LITERATURE REVIEW OF STRUCTURAL VULNERABILITY

Often some authors consider that the effectiveness of the realization of the network functions is affected by its structure [30]. At the occurrence of a hazard, loses and damage depends on the structural organization and varies from one network to another [31]. Analyzing the topology of the network allows a better comprehension of the dynamic phenomena that affects its performances [25] and the identification of its weaknesses [8]. Some structural parameters defined above enable an estimation of the vulnerability [25], [6]. In the literature, there are other parameters related to resilience, component of vulnerability, which can be simulated by removing one or more vertices and edges [2]. The second component, the robustness is defined in [4] as the ability to maintain its connectivity properties after damage of one or more of its components (nodes and edges). Others authors consider that it depends on the network degree distribution [25]. From a structural point of view, the vulnerability can be defined as 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 [3]. The main parameters of vulnerability measure include the degree, the clustering coefficient, the average distance, and the load [25]. Besides these obvious parameters, there are 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 [25] and its analysis should help to measure the system response after the attacks [31].

A. Efficiency

References [2], [5], and [4] define vulnerability as the lack of network performance. This performance also known as efficiency is defined as a function of the average distance between nodes [4] and [32]:

$$\phi(G) = E(G) = \frac{1}{N(N-1)} \sum_{i \neq j \in G} \frac{1}{D(V_i, V_j)} \quad (12)$$

The efficiency of a path between two vertices is the average efficiency of all the edges constituting the path and determines the movement fluidity of the elements between the two nodes. Resilience, which is one of the measures of vulnerability, is the drop of efficiency induced by the deterioration of edges [4] and [27].

$$V(E_i) = \frac{E(G) - E\prime(G)}{E(G)} \quad (13)$$

$E(G)$ 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 is then defined by:

$$V(G) = \max[V(E_i)] \quad (14)$$

Finally, some authors consider the loss of performance caused by the removal of a vertex instead of an edge [33] and [31].

B. Integrity

References [24], [1] and [34] define vulnerability as a lack of integrity. Integrity is the quotient N_g/N_0. WhereN_g is the size of the graph after damage of a fraction g of nodes compared with the initial size N_0. Others authors define integrity in relation to the weight, the geodesic distance and the range (ratio between the distance and weight) [2].

C. Probability

The vulnerability of a system is measured in [16] and [35] 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 hazard A_i, the total probability would be the sum of probabilities.

$$P(\max_{t \in T}(X(t)) > x) = \sum_i P(A_i) * P\left(\max_{t \in T}(X(t) > x \,/\, A_i\right) \quad (15)$$

D. Vulnerability functions

Several authors suggest vulnerability functions in the literature. Reference [2] defines vulnerability and improvability of a network G as elements of evaluation. D (respectively I) is the set of damages (respectively set of improvements) possible in the infrastructure G. (G, d) (respectively $IM(G, i)$ is the network configuration after the damage $d \in D$ (respectively after the improvement $i \in IM$). The importance of damage d (respectively improvement i) is measured by the relative decrease (increase) of performance $\Delta\phi^- / \phi$ (respectively $\Delta\phi^+ / \phi$). With $\phi[G] \geq 0$ and $\Delta\phi^- = \phi[G] - \phi[\mathcal{D}(G, d)]$ the relative decline in system performance caused by the damage d . ($\Delta\phi^+ = \phi[IM(G, i)] - \phi[G]$ is the relative increase in performance due to the improvement action i. The critical damage (improvement) $d^* \in \mathcal{D}$ ($i^* \in I$) is the damage (improvement) that minimizes $\phi[\mathcal{D}(G, d)]$ (maximize $\phi[IM(G, i)]$). Vulnerability and improvability are given by:

$$V[G, \mathcal{D}] = \frac{\phi[G] - W[G, \mathcal{D}]}{\phi[G]} \quad (16)$$

$W[G, \mathcal{D}] = \phi[D(G, d^*)]$ is the worst performance of G in the set of damage $\mathcal{D}$

$$IP[G, I] = \frac{B[G,I]-\phi[G]}{\phi[G]} \qquad (17)$$

$B[G, I] = \phi[D(G, i^*)]$ is the best performance of G in the set of improvement I.

For a graph with N nodes et M edges, Criado defines a vulnerability function by:

$$V(G) = \exp\left(\frac{\sigma}{N} + N - M - 2 + \frac{2}{N}\right) \qquad (18)$$

Its value varies between 0 and 1. σ is the standard deviation of the degree distribution. This function does not take into account the vulnerability indicators such as cohesion (degree of the vertices) and adhesion (edges degree) [25] and [28]. Moreover, the term does not allow comparison between networks of different sizes and structures [25]. Different ways of quantifying the vulnerability do not consider some elements that however seem important from our point of view. We analyze this potential lacuna in the next section.

VI. LIMITATIONS OF MODELING TOOLS

A. *The edges are directed*

In network modeling, the edges orientations are not often taken into account which skews the results [27]. Let us consider the two unweight graphs shown in (Figure 4).

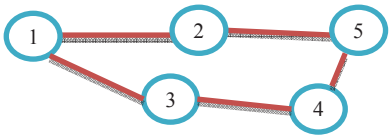

Figure 4 (a) : Undirected network

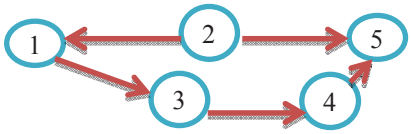

Figure 4 (b) : Directed network

In the graph (a), the edges are not oriented; the distance between nodes 1 and 5 is 2 units. On the contrary in the graph (b), edges are oriented bringing this same distance to 3 units. Because of it, it is no longer possible to go from 1 to 5 through 2, the edge between 1 and 2, allowing only a flow from 2 to 1in one way. 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 structural parameters seen above. We propose to consider two new elements: reversibility and reciprocity.

Reversibility: It determines the ability of an edge to transport the material or the information in the opposite direction in case of disaster. This ability may be a function or be set by decision-makers.

Reciprocity: Obviously, the non-orientation of edges has no significant influence on some networks. Therefore we define reciprocity as the average probability that two vertices are linked in both directions.

$$R(G) = \frac{\text{Number of pairs of vertices}}{\text{Number of loops linking two adjacent vertices}} \qquad (19)$$

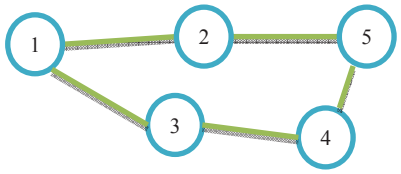

Figure 5 (a): Unweight network

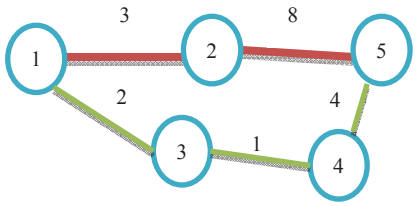

Figure 5 (b) :Weighted network

B. *The graphs must be weighted*

Some authors do not take into account the weight of edges in their analysis. In reality, the edges are often weighted. This weight can be a length, cost, impedance etc. To show the importance of weight, let us consider the following graphs.

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 figure (b), 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.

C. *The nodes are of different types*

In some networks, such as power grids, it is essential to distinguish different types of vertices [6].

By analyzing the above two networks (Figure 6), one can say about the graph (a) that node 3 is the most important in the point of view of efficiency, and centrality. On the

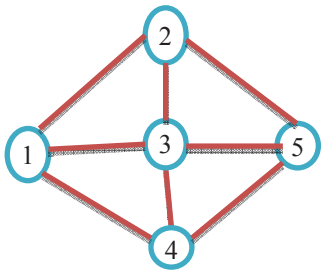

Figure 6 (a): Identical nodes

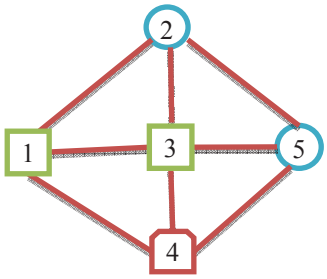

Figure 6 (b): Different nodes

contrary, by considering in the second graph that node 4 is the source of the element circulating in the network, 3 is used as a transporting relay and 2 and 5 are the destinations we cans say that node 4 will be the most important. By removing it in the network, the element will not flow over the network 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 define a component class shown in figure 7.

D. Component class in the analysis of network vulnerability

There are three types of components: *Sources*, *Targets* and *Relays* [6]. This distinction is not important enough to analyze the networks. To show this, let us consider three networks, one modeling a subway system, the other a power grid, and the last a bus network in the same geographical zone. The vulnerability of the subway system is very depending on the bus network capacity - which in reality can be substituted to the subways. Moreover, the two networks interact with the power grid, which supply them. The last is vulnerable to disruptions of bus and metro (staff transport for example). Analysis of the three networks separately does not allow understanding their dynamics. We therefore propose a multi network analysis by defining several types.

Potential component: A potential component is a component that does not physically exist in the structure but that we can make functional depending on time and / or investment. Practically, there are often ways to link a node to another one in case of emergency. This may be true in the case of roads which are not usable for some reason but with

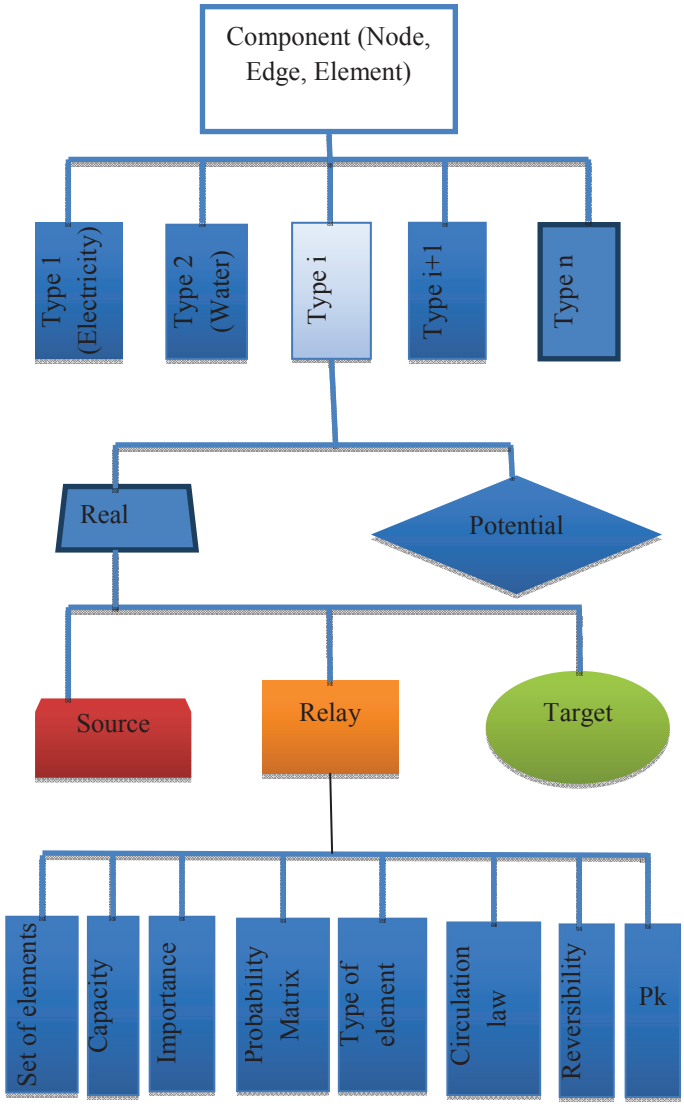

Figure 7: Element class

some slight adaptations can be used at the occurrence of a disaster. Their numbers and their restorability3 are factors that significantly reduce the vulnerability of the entire network. The network analysis must take into account these structures by describing them as much as possible before the disaster. The potential vertices and edges are characterized by the same parameters as the real component (nodes and edges) but will have different influences on networks for identical topology.

Element: It is the object that travels through the network; this may be information, matter, energy, etc. We define the set of elements types by $\epsilon = (\epsilon_1, \epsilon_2 \ldots \varepsilon_F; |\epsilon| = F)$. Modeling multi-network traffic involves several elements.

Shunting or circulation rules: Let's consider the network shown in Figure 7. Parameters respectively indicate the distance, cost and travel time. Given an element located in 1 and wishing to travel to 7. From the perspective of the

[3] ability to be restored

distance, the path is 1-4-7. But if we consider the cost of transporting, this path becomes 1-2-4-7. Considering only the travel time, this same path is made of nodes 1-3-5-6-7. The rule of circulation can vary with time or other constraints. It is therefore important to define it clearly for all

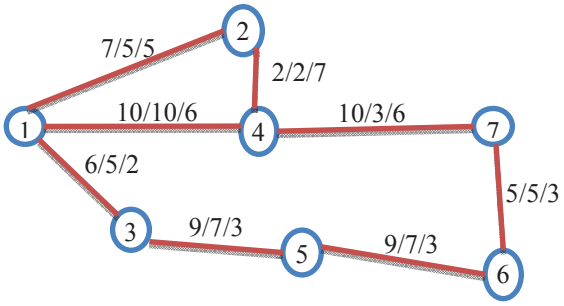

Figure 8: circulation law

elements, because they play a major role in the dynamics of the networks.

Simplicity : To reflect the multiplicity of elements flowing through the network, we introduce the notion of simplicity. The simplicity S_{ijk} of two nodes of type k ($V_{ik}, V_{jk}, V_{ik} \neq V_{jk}$) is the number of edges of type k incidents with the nodes V_{ik} and V_{jk}. The simplicity of two nodes is then the average of the simplicities of all types.

$$S_{ij} = (1 / \varepsilon_k) \sum_k S_{ijk} \qquad (20)$$

where ε_k is the number of edges of type K.
The simplicity of a graph is then:

$$S(G) = \left[\frac{2}{N(N-1)}\right] * \sum S_{ij} \qquad (21)$$

Physical and / or functional Interdependence: The damage to a component disrupts the function of other network elements. To illustrate it, it is sometimes defined a conditional probability function between vertices [22].

Parameters: The vulnerability analysis requires considering parameters that are not only structural (see different classes of vulnerability). A parameter may be a function of other parameters. The geographical coordinates of a vertex may, for example, inform about the related risks by the way of a correlation with an external database. The parameters are used to distinguish one vertex or edge from another one. For example, a node may be a central power whose properties are different from another one according to the power.

VII. VULNERABILITY MODEL ANALYSIS

For the analysis of vulnerability, we propose a closed loop system. The output is determined by decision makers and may be damage, prejudice, loses or a service function (eg electricity consumption). The entry model is the hazard. The system itself is broken down into *Population* and *Territory*. The population is affected by the effects of the

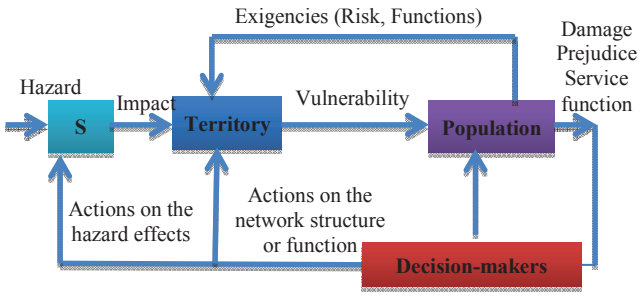

Figure 9 : Vulnerability model

hazard through the Infrastructure components. A hazard has a frequency and / or magnitude. It impacts on the structure and / or function of the territory elements. This influence is reflected by the element S which converts the intensity and/or frequency on the network parameters. (Failure rate, centrality, etc.). Through the vulnerability model obtained, we can estimate the damage or, for a set of damage, determine the critical points of the network and the actions to be carried out. This task concerns the decision makers which will use the decision support model to inform the population and define the actions to be undertaken on the network or on the hazard effects.

VIII. CONCLUSION AND PERSPECTIVES

Natural disasters with severe consequences have increased over the last decade. The material and human losses also depend on the state of infrastructure affected and on the ability of decision makers to manage the crisis. The objective of this study was first to analyze the academic work dealing with network modeling and second to propose a model of vulnerability. The vulnerability analysis being often confused with risk analysis, we have distinguished the two concepts, which however appear to be very complementary. This distinction and the specification of components have been essential to define vulnerability. The literature review of network modeling based on graph theory made it possible to distinguish the structural indicators of vulnerability. We then noted some shortcomings and propose ways to overcome them. The vulnerability model we proposed considers the dynamics of the network. We have shown that the knowledge of circulation rules is crucial for the analysis of infrastructures. We have taken into account structural, dynamic and environmental aspects of the considered infrastructure. This study can be considered as a stepping stone toward an algorithm-based approach for calculating the parameters of vulnerability by taking into account the new elements introduced. Further developments will deal with the design of decision support integrating societal settings.

IX. BIBLIOGRAPHY

[1] L. Zhao, K. Park, et Y.-C. Lai, « Attack vulnerability of scale-free networks due to cascading breakdown », *Physical Review E*, vol. 70, n°. 3, p. 035101, 2004.

[2] V. Latora et M. Marchiori, « Vulnerability and protection of infrastructure networks », *Physical Review E*, vol. 71, n°. 1, p. 015103, janv. 2005.

[3] T. Thedéen, « Vulnerability of Infrastructures », in *Risks in Technological Systems*, Springer London, 2010, p. 161-173.

[4] S. Arianos, E. Bompard, A. Carbone, et F. Xue, « Power grids vulnerability: a complex network approach », *0810.5278*, oct. 2008.

[5] P. Crucitti, V. Latora, M. Marchiori, et A. Rapisarda, « Error and Attack Tolerance of Complex Networks », 2004.

[6] 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, 2004.

[7] S. Einarsson et M. Rausand, « An Approach to Vulnerability Analysis of Complex Industrial Systems », *Risk Analysis*, vol. 18, n°. 5, p. 535-546, 1998.

[8] B. C. Ezell, « Infrastructure Vulnerability Assessment Model (I-VAM) », *Risk Analysis*, vol. 27, n°. 3, p. 571-583, 2007.

[9] A. Leroy et J.-P. Signoret, *Le risque technologique*. Presses Universitaires de France (PUF), 1992.

[10] J. C. Chicken, *Managing Risks and Decisions in Major Projects*. Thomson Learning, 1994.

[11] 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.

[12] W. O'Shaughnessy, *La faisabilité de projet: Une démarche vers l'efficience et l'efficacité*. Smg, 1999.

[13] R. Gouriveau, « Analyse des risques, formalisation des connaissances et structuration des donnéespour l'intégration des outils d'étude et de décision », Systèmes Industriels, Institut National Polytechnique de Toulouse, 2003.

[14] PMI Project Management Institute, *A Guide to the Project Management Body of Knowledge (PMBOK Guide) -- 2000 Edition*, 2000e éd. Project Management Institute, 2000.

[15] P. Simon, *Project Risk Analysis and Management Guide: PRAM*. APM Group Ltd, 1997.

[16] A. J. Holmgren, « Using graph models to analyze the vulnerability of electric power networks », *Risk Analysis: An Official Publication of the Society for Risk Analysis*, vol. 26, n°. 4, p. 955-969, août. 2006.

[17] F. Leone, « Caractérisation des vulnérabilités aux catastrophes Â« naturelles » : contribution à une évaluation géographique multirisque (mouvements de terrain, séismes, tsunamis, éruptions volcaniques, cyclones) ». 29-nov-2007.

[18] M. Reghezza, « Réflexions autour de la vulnérabilité métropolitaine : la métropole parisienne face au risque de crue centennale. », 05-déc-2006. [Online]. Available: http://tel.archives-ouvertes.fr/tel-00123255/en/. [Accessed: 27-févr-2011].

[19] M. E. J. Newman, « The structure and function of complex networks », *cond-mat/0303516*, mars. 2003.

[20] C. Beler, « Modélisation générique d'un retour d'expérience cognitif. Application à la prévention des risques », PhD Thesis, 2008.

[21] 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.

[22] L. Dueñas-Osorio, J. I. Craig, et B. J. Goodno, « Seismic response of critical interdependent networks », *Earthquake Engineering & Structural Dynamics*, vol. 36, n°. 2, p. 285-306, 2007.

[23] P. Holme, B. J. Kim, C. N. Yoon, et S. K. Han, « Attack vulnerability of complex networks », *Physical Review E*, vol. 65, n°. 5, p. 056109, mai. 2002.

[24] L. Dall'Asta, A. Barrat, M. Barthelemy, et A. Vespignani, « Vulnerability of weighted networks », *physics/0603163*, mars. 2006.

[25] A. Yazdani et P. Jeffrey, « A note on measurement of network vulnerability under random and intentional attacks », *1006.2791*, juin. 2010.

[26] M. Barthelemy, « Betweenness Centrality in Large Complex Networks », *cond-mat/0309436*, sept. 2003.

[27] E. Bompard, M. Masera, 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.

[28] U. Brandes, « A faster algorithm for betweenness centrality », *Journal of Mathematical Sociology*, vol. 25, n°. 2, p. 163-177, 2001.

[29] E. W. Weisstein, « Scale-Free Network -- from Wolfram MathWorld ». [Online]. Available: http://mathworld.wolfram.com/Scale-FreeNetwork.html. [Accessed: 28-déc-2010].

[30] S. H. Strogatz, « Exploring complex networks », *Nature*, n°. 410, p. 268-276, 2001.

[31] 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.

[32] P. Crucitti, V. Latora, et M. Marchiori, « Model for cascading failures in complex networks », *Physical Review E*, vol. 69, n°. 4, p. 045104, avr. 2004.

[33] V. Latora et M. Marchiori, « Efficient behavior of small-world networks », *Physical Review Letters*, vol. 87, n°. 19, p. 198701, nov. 2001.

[34] A. Jamakovic et P. Van Mieghem, « On the robustness of complex networks by using the algebraic connectivity », in *Proceedings of the 7th international IFIP-TC6 networking conference on AdHoc and sensor networks, wireless networks, next generation internet*, Berlin, Heidelberg, 2008, p. 183–194.

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