MÉTHODOLOGIE ET MODÈLE D'ANALYSE DE LA VULNÉRABILITÉ ET DU RISQUE DES SYSTÈMES CRITIQUES INTERDÉPENDANTS

MODEL AND METHODOLOGY FOR INTERDEPENDENT CRITICAL SYSTEMS VULNERABILITY AND RISK ANALYSIS

Kamissoko Daouda
Université de Toulouse
LGP-IRIT
Tarbes, France
daouda.kamissoko@enit.fr

Pérès François
Université de Toulouse
LGP
Tarbes, France
francois.peres@enit.fr

Zaraté Pascale
Université de Toulouse
IRIT
Toulouse, France
pascale.zarate@irit.fr

Résumé

Le travail présenté dans ce papier a pour objectif l'analyse des réseaux interdépendants, en vue de modéliser la vulnérabilité et le risque. Les concepts de Système et de composant critique sont définis. Une approche de modélisation des réseaux est présentée. Cette modélisation compatible avec la théorie des graphes, est basée sur l'analyse des interdépendances et des influences du milieu extérieur. Une démarche pour quantifier la vulnérabilité et le risque est également présentée. Celle-ci se décline en plusieurs étapes intégrant une analyse qualitative et quantitative. La méthodologie proposée inclue l'identification des systèmes à analyser, du contexte ainsi que l'évaluation des évènements redoutés.

Summary

The work presented in this paper aims interdependent networks analysis, for vulnerability and risk assessment. Concepts of system and critical component are defined. An approach for network modelling is also presented. This modelling supporting graph theory is based on interdependences and external influences analysis. An approach for vulnerability and risk modelling is also presented. It comes in several steps including qualitative and quantitative analysis. The proposed methodology includes identification of the systems to be analysed, context and feared events assessment.

Introduction

Dans un contexte de forte industrialisation, nos sociétés dépendent de plus en plus de réseaux tels que l'eau, l'électricité, le gaz et les télécommunications. Le nombre et la diversité des évènements comme l'épisode neigeux en île de France l'hiver 2010, ou le Tsunami au Japon en mars 2011 ont démontré la vulnérabilité de ces infrastructures vis-à-vis des catastrophes naturelles. Par ailleurs les flux de matière, de service, d'énergie et d'information échangés peuvent aggraver ou atténuer les conséquences. À cause de ces interdépendances, le dysfonctionnement d'une entité réseau est susceptible de se propager aux autres, à une échelle pouvant dépasser celle d'un pays, rendant ardue toute analyse de vulnérabilité.

L'objectif de ce papier est de proposer une méthodologie d'analyse du risque et de la vulnérabilité de tels systèmes dans un environnement incertain en tenant compte des interdépendances.

Pour y parvenir, les concepts clés sont définis, puis la méthodologie d'analyse détaillée. Celle-ci commence par une circonscription du contexte. Étape cruciale pour poser les limites des systèmes à analyser. Après l'analyse fonctionnelle permettant de cerner les spécificités de fonctionnement dues aux interdépendances, une méthode de modélisation de celles-ci intégrable à la théorie des graphes est proposée. Par la suite, est décrit la manière de tenir compte des influences du milieu de fonctionnement sur le modèle obtenu. Les derniers paragraphes présentent le modèle de vulnérabilité, des conséquences et du risque.

Définitions

Nos sociétés dépendent d'un grand nombre d'infrastructures techniques non tolérantes aux fautes (Johansson, Jonsson, et Johansson 2007). Les réseaux électriques, eaux, gaz, télécommunications font partie de cette catégorie. Ces réseaux sont parfois appelées Réseaux Supports de Vies (RSV), Infrastructures Critiques (IC), Infrastructures Essentielles (IE), Systèmes Complexe, ou encore Systèmes Critiques (SC). Face à la diversité des points de vue sur les systèmes et sur leurs criticités, nous présentons ci-dessous le nôtre.

1. Système et Système Critique

Certains auteurs définissent les systèmes par rapport à leurs constitutions. D'autres les définissent au regard des services qu'ils fournissent. Du point de vue des premiers auteurs, on peut définir un système comme un nombre fini d'éléments en relation, formant un tout (Wihelmsson et Johanson 2009) ou comme un ensemble d'éléments interactifs, reliés entre eux. Du second point de vue, (Benoît et Luviano 2009) définissent un système comme un ensemble cohérent d'éléments ou de processus liés par des objectifs, des responsabilités ou des missions communes fixées. Nous définissons un système comme un *ensemble d'entités interconnectées facilitant la circulant de flux afin de remplir des*

fonctions spécifiées. Dans la suite de ce document nous appellerons Systèmes Critiques (SC) les réseaux tels que l'électricité, l'eau, le gaz etc. Nous définissons un système critique comme *un système dont la perturbation engendre un risque non acceptable pour le territoire et les enjeux considérés*. Nous avions défini l'enjeu comme un « élément matériel ou immatériel assurant une fonction dont la détérioration est dommageable ou préjudiciable pour la société ».

2. Composant Critique

Les SC sont composés d'un ensemble d'éléments qui fonctionnement comme des entités individuelles appelées composants. On peut citer à titre d'exemple une centrale nucléaire pour la production de l'électricité, ou encore une canalisation de Gaz. Les SC ont été définit en tenant compte des risques encourus par les enjeux. De même nous définissons un composant critique par rapport à la vulnérabilité du SC lui-même. La vulnérabilité est « l'incapacité d'un enjeu à résister à l'occurrence d'un aléa et à retrouver efficacement son fonctionnement nominal durant une période de temps donnée». Ainsi, un composant critique est un *composant dont la défaillance place le système constitutif dans un état de vulnérabilité non admissible*.

L'acception de ces mots clés fixée, nous détaillons dans les paragraphes suivants les différentes étapes pour mener à bien l'analyse des SC.

Méthodologie d'analyse

Il n'y a pas une méthodologie d'analyse de la vulnérabilité admise de tous. Les étapes et les outils sont assez souvent inspirés de l'analyse du risque. La nôtre commence par mieux cibler le contexte. Puis tout au long de l'analyse, nous essayons de répondre aux questions suivantes : *Qu'est ce qui est redouté ?*, *Qu'est ce qui est susceptible d'être perturber ?, Quelles conséquences cela peut-il avoir ? Comment cela peut-il se produire ? Comment retrouver un état normal ?* (Petit, Robert, et Rouselle 2004).

Les paragraphes suivants présentent les différentes étapes pour élucider ces interrogations.

3. Contexte

Les SC étant interdépendants, leurs limites géographiques et administratives sont peu identifiables. D'une part, divers acteurs sont impliqués dans leurs mises en œuvre (exploitants, communes, départements…). D'autre part, un dysfonctionnement peut affecter des enjeux multiples et variés, souvent sur des territoires administrativement indépendants. Le contexte est l'ensemble des attributs permettant aux décideurs de cadrer l'analyse. Il se décline en cinq axes : Acteurs, SC, Enjeux, Aléas, Environnement. Ces éléments sont identifiés par l'analyste. Leurs évaluations nécessitent la participation des autres décideurs. La section suivante commence par présenter l'évaluation des aléas.

4. Évaluation des évènements redoutés

Dans la littérature l'évènement redouté est parfois appelé *Incident* ou *Aléa* (Ezell, Farr, et Wiese 2000), (Berdica 2002). L'appellation *Aléa* est préférée car de son sens commun, un aléa est « *une classe générique regroupant un ensemble potentiel de cause ou encore comme un générateur de causes* » ((CCPS) et et.al 1992). De notre point de vue, un aléa est un phénomène naturel ou anthropique pour lequel on ne peut prévoir l'occurrence et l'intensité à la fois, et susceptible d'affecter un enjeu. Il peut être naturel, climatique, technique, humain, un acte de sabotage, de terrorisme ou de guerre (Petit, Robert, et Rouselle 2004). L'une de ses principales caractéristiques est le fait qu'il a une influence négative sur le fonctionnement du réseau (Ezell, Farr, et Wiese 2000).

Dans la nature, il existe sept types d'aléa interdépendants susceptibles d'affecter les réseaux : Séisme, Inondation, Volcan, Tsunami, Incendie, Cyclone, Tempête, et Mouvement de terrain. Dans la plupart des cas, il n'est pas nécessaire d'analyser les SC pour l'ensemble de ces aléas. La matrice d'interdépendance élaborée par les experts quantifie la probabilité conditionnelle que l'aléa θ se produise sachant que l'aléa μ s'est produit. La probabilité conditionnelle et l'amplitude de l'aléa sont obtenues par agrégation de critères (probabilité d'apparition, intensité, durée d'action, vitesse d'exécution, nombre et détectabilité des signes précurseurs, étendu, temps lattent entre les signes et l'événement, événements atténuateurs, l'environnement). Les techniques, comme celle de Morkov peuvent être utilisées pour l'évaluation de la probabilité de l'aléa :

$$P(A) = P\left(\cap E_{\theta\mu}\right) \quad \{1\}$$

Les $E_{\theta\mu}$ correspondent aux états redoutés. La prochaine étape consiste à identifier les systèmes susceptibles d'être affectés par ces aléas. Les aléas identifiés n'affectent que certains systèmes. L'identification de ces derniers est présentée dans la section suivante.

5. Identification des Systèmes

Comme sa définition l'indique, un système critique pour un enjeu ne l'est pas forcement pour un autre. La première difficulté à laquelle sont confrontés les analystes est le choix des systèmes pertinents. D'une manière exhaustive, il existe cinq classes de SC : Transport (Autoroutier, Aérien, Maritime, Ferré), Énergie (Électricité, Gaz, Hydro carbure), Sanitaire (Eau usée, eau potable, Hospitalier, Déchets NBC, Alimentaire), Information (Informatique, Télécommunication, GPS, Audiovisuel, Postal), Banque et finance.

Concrètement, il est peu envisageable de mener une analyse pour tous ces systèmes. Pour des raisons budgétaires, temporelles - mais aussi en ce qui concerne l'obtention des données. Une alternative consiste donc à se fier à la règlementation en vigueur. En France, la Direction Protection et Sécurité de l'État, définit les activités d'importances vitales dans l'instruction N° 6600/SGDN/PSE/PPS du 26 septembre 2008. Le conseil international de gouvernance du risque (IRGC) quant à lui recommande aux nations cinq réseaux stratégiques (électricité, gaz, eau, transport ferré, internet). D'une manière générale les réseaux électriques semblent être les plus critiques (Kaplan et Garrick 1981), compte tenu du degré de dépendance des autres réseaux vis-à-vis de l'électricité. En plus de celui-ci, on peut ajouter d'autres tels que l'eau, les télécommunications, le transport etc. (Benoît et Luviano 2009), (Kaplan et Garrick 1981).
Après les choix du ou des SC, leurs analyses fonctionnelles, présentées dans la section suivante permettront de mieux comprendre le fonctionnement global.

6. Analyse fonctionnelle

L'analyse fonctionnelle est une méthode intuitive permettant de rechercher, formuler, ordonner, caractériser, hiérarchiser et valoriser les fonctions de service et techniques des SC (Holmgren 2007). Avant la modélisation, elle permet d'identifier les composants impliqués dans une interdépendance. Elle doit comprendre au moins les étapes suivantes :

- Définition de l'arborescence physique et/ou fonctionnelle des systèmes et des sous-systèmes ;
- Identification des fonctions de service ;
- Identification des infrastructures et des ressources permettant de réaliser ces fonctions ;
- Définition des fonctions de contrainte, des flux circulant dans les composants ainsi que des actions nécessaires à leurs bons fonctionnements.

L'analyse fonctionnelle facilite à ce titre la représentation et la modélisation du système présentées dans la section suivante.

7. Modélisation du Système

La modélisation est une représentation du système réelle en vue de l'analyser. Cette représentation peut être mathématique ou graphique. Elle permet d'évaluer l'impact des évènements redoutés. La modélisation par la théorie des graphes a été choisie car celle-ci permet de représenter la plupart des réseaux technologiques. Un graphe G est composé d'un ensemble de sommets et d'arêtes. À titre d'exemple dans le transport ferré, les sommets sont les gares et les arêtes les rails. Dans (Kamissoko, Pérès, et Zaraté 2011) a été montré l'intérêt de l'orientation et du poids des arêtes. Les auteurs argumentent que :

- Les graphes soient orientés ;
- Les graphes soient pondérés ;
- Il y ait plusieurs flux (caractérisés par des vecteurs) pour chaque composant. Ces flux peuvent être une information, un service, de l'énergie, de la matière, etc. Ils circulent d'un sommet producteur vers un sommet consommateur ;
- Il y ait différents types de sommets. Le type dépend de la fonction réalisée dans le réseau. Cette fonction peut être : Produire, Relayer, Utiliser (Petit, Robert, et Rouselle 2004), (Jönsson et Johansson 2008); auxquels nous ajoutons, Traiter, et Transporter quand il s'agit d'une arête.

En considérant ce qui a été dit dans ce paragraphe, on peut modéliser tout SC par un ensemble de quatre sommets et d'arêtes pondérées. Les types de sommet correspondent aux fonctions réalisées. Ainsi un sommet peut être de type *Produire, Relayer, Utiliser ou Traiter*. Les SC identifiés dans la section 5, quel que soit leurs natures, utilisent l'une de ces fonctions sur les flux circulant. Pour des raisons de représentation en cas de conflit entre les types de sommet, la priorité est donnée au type du flux principal. Ce flux peut être obtenu par Analyse Fonctionnelle du sommet concerné. Cette modélisation restera partielle tant qu'on n'y intègre pas les interdépendances. Nous proposons ci-dessous une approche pour modéliser celles-ci.

8. Modélisation des Interdépendances

Les SC sont non seulement dépendants les uns des autres, mais le sont aussi avec leurs environnements. Une interdépendance est un lien entre deux composants. Ce lien peut être fonctionnel ou représenter une contrainte. La science des dépendances est relativement immature. Les dépendances sont la cause principale de baisse de performance dans le SC (Albert, Jeong, et Barabasi 2000). Elles favorisent la propagation de l'aléa (Benoît et Luviano 2009), et placent les analystes dans une situation d'incertitude radicale ou d'ignorance (Rinaldi, Peerenboom, et Kelly 2001). La principale difficulté dans la modélisation des réseaux consiste donc à tenir compte des dépendances entre les composants.
(Rinaldi, Peerenboom, et Kelly 2001) identifient quatre catégories de dépendance: Fonctionnelle (ou Physique), Géographique, Cybernétique et Logique. Les dépendances physiques sont dues à un échange de flux entre les

composants. Par exemple le réseau d'eau a besoin de l'électricité pour fonctionner. Les dépendances géographiques sont dues à la proximité des composants. Elles se produisent lorsque deux composants sont géographiquement proches et que la défaillance de l'une entraine celle de l'autre. Par exemple l'explosion d'une canalisation de gaz endommageant les fils électriques à proximité. Les dépendances cybernétiques proviennent du transfert de l'information. Cette dépendance existe entre le système de contrôle et le monitoring d'un réseau électrique, et les réseaux informatiques. En effet, les informations nécessaires au monitoring doivent passer par les réseaux informatiques. Enfin les dépendances logiques sont liées aux réalités conjoncturelles, économiques, sociales et/ou politiques (Benoît et Luviano 2009). C'est par ce mécanisme que la guerre en Lybie fait augmenter le prix du carburant dans les états européens.

Dans ce papier, la dépendance physique, fonctionnelle et cybernétique sont regroupés sous l'appellation *dépendance*. En effet seule la nature du flux diffère dans les trois cas. Par ailleurs, pour des raisons d'étymologie nous appelons *influence* la dépendance géographique.

Pour modéliser les interdépendances, (Earl E. Lee, Mitchell, et Wallace 2004) identifient cinq types des liens. *Entrée* quand un composant fournie un autre ; *La mutuelle dépendance* si le service est dans les deux sens ; *La co-localisation* si les deux sont situés dans la même région géographique ; *Le Partage* quand ils ont une ressource commune ; et le *Ou-exclusif* quand seulement un et un seul composant est fourni à un instant donné. Les auteurs ne considèrent pas le sens du flux et les états des composants. Concrètement *L'entrée*, la *dépendance mutuelle* et le *partage* symbolisent le même lien, seul le sens du flux et le nombre de composant varient. Par ailleurs la *co-localisation* et le *ou-exclusif* sont aussi semblables. Ils symbolisent ce que nous appelons une *influence*.

En tenant compte de l'état des composants et du sens des flux, on peut modéliser tous types de liens soit par une dépendance, soit par une influence. La démarche pour y parvenir est explicitée dans les lignes qui suivent.

8.1 Dépendance

Toute arête entre deux sommets matérialise une dépendance. Cette dépendance est vitale si le flux transporté par l'arête est un flux principal. C'est le cas du réseau métropolitain où les gares ont besoin des rails pour exister. D'une manière générale B dépend de A s'il existe un flux partant de A à B. La dépendance entre les arêtes et les sommets de mêmes types n'est pas possible. En effet, ce lien s'intègre dans l'architecture du réseau et n'est plus considéré comme une dépendance. Nous représentons une dépendance par :

Figure 1. Arête de dépendance

8.2 Influence

Un composant B est géographiquement dépendant d'un composant A (A influe sur B) s'il n'y a pas de lien fonctionnel entre les deux composants, mais qu'une défaillance de A entraine une défaillance de B. Nous représentons une influence par une arête (en pointillé) de poids nul et ne transportant aucun flux.

Les deux types de liens définis opèrent entre les composants du réseau (arêtes et sommets). Ayant fait le choix d'une modélisation par les graphes, nous présentons ci-dessous comment intégrer ces liens dans un réseau représenté par un graphe pondéré et orienté.

8.3 Lien Sommet-Sommet

Le lien entre deux sommets de types différents peut être une dépendance ou une influence. (Johansson et Hassel 2010) matérialisent la dépendance entre deux sommets par une arête. Nous soutenons que les arêtes de dépendance sont orientées comme les autres arêtes. Ainsi, Si le sommet V_2 dépend fonctionnellement du sommet V_1, nous matérialisons cette dépendance par une arête partant de V_1 vers V_2. (En rouge sur la Figure 2). L'influence de V_2 sur V_1 est aussi matérialisée par une arête en pointillé.

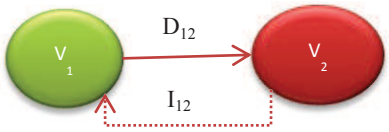

Figure 2. Lien entre deux sommets

Une influence peut exister entre les sommets de mêmes types (l'explosion d'un réservoir de gaz entrainant celle d'un autre réservoir de gaz), ou entre les sommets de types différents (La destruction d'un château d'eau inondant les postes de transformation). Par contre la dépendance entre deux sommets de même type est représentée par des arêtes standards. La dépendance n'existe qu'entre les sommets de types différents.

8.4 Lien Sommet-Arête

Un lien n'existe pas qu'entre les sommets. Dans certaines situations, une ligne électrique peut être endommagée par l'explosion d'un poste de détente de gaz. Dans ce cas il y a bien une influence du poste de détente sur la ligne électrique. On peut citer aussi les trajets maritimes qui dépendent des balises en haute mer. Pour modéliser la dépendance d'une arête E d'un sommet V, nous introduisons une *arête virtuelle* E' de poids nul et un *sommet virtuel* V' de capacité infinie. Les probabilités de défaillance des *composants virtuels* V' et E' sont nulles et une arête virtuelle est une instance d'une et d'une seule arête réelle (Figure 3).

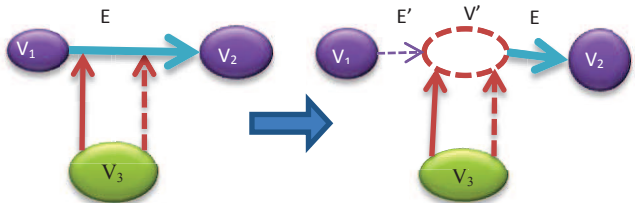

Figure 3. Lien sommet-Arête

8.5 Lien Arête-Sommet

Supposons maintenant que c'est le sommet V_3 qui dépende de l'arête E. C'est le cas d'une canalisation d'eau fournissant une centrale thermique, ou une défaillance de canalisation de gaz affectant un répartiteur téléphonique. Ce lien est modélisé par la Figure 4.

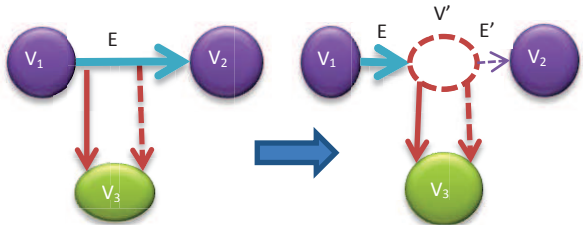

Figure 4. Lien Arête-Sommet

8.6 Lien Arête-Arête

On retrouve les dépendances et les influences entre les arêtes dans le transport ferroviaire. Les rails et l'alimentation électrique sont intimement liés d'un point de vue fonctionnel. La modélisation de ce type de lien est donnée par la Figure 5.

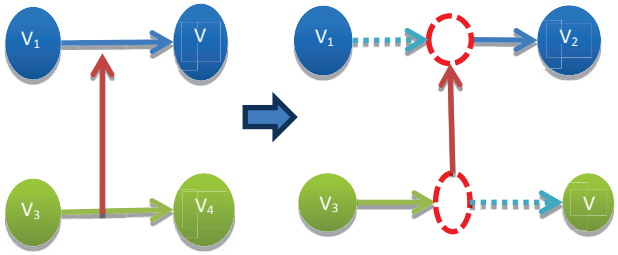

Figure 5. Lien Arête-Arête

Nous avons jusqu'ici pris en compte les effets des composants entre eux. Mais le fonctionnement d'un composant peut être altéré aussi par l'environnement dans lequel il opère. Dans le paragraphe suivant, nous présentons une démarche pour intégrer cette influence.

8.7 Modélisation de l'influence des éléments du milieu extérieur

Le milieu extérieur est composé par l'ensemble des éléments environnants un SC et ayant un impact significatif sur son fonctionnement. Identifiable par la méthode 5M, les éléments peuvent être liés à :

- Matériel : Système de détection, logiciels ;
- Matière : Les différents flux circulant dans les réseaux, avec leurs caractéristiques (vitesse, lois de circulation). Les facilités de circulation des différents flux dans le réseau est un indicateur de vulnérabilité ;
- Méthodes : Processus de maintenance, normes et réglementations ;

- Milieu : Température, Impulsion électromagnétiques, sol et le sous-sol ;
- La main d'œuvre : Les opérateurs, les analystes, les décideurs ;
- Le moment : La saison, l'heure. L'heure intervient dans la dynamique dans les SC. Elle influe principalement sur les lois de circulation des flux et sur le poids des arêtes. Dans le cas où le prix serait inclus dans le poids des arêtes d'un réseau électrique, ce poids serait plus élevé dans les heures pleines que dans les heures creuses.

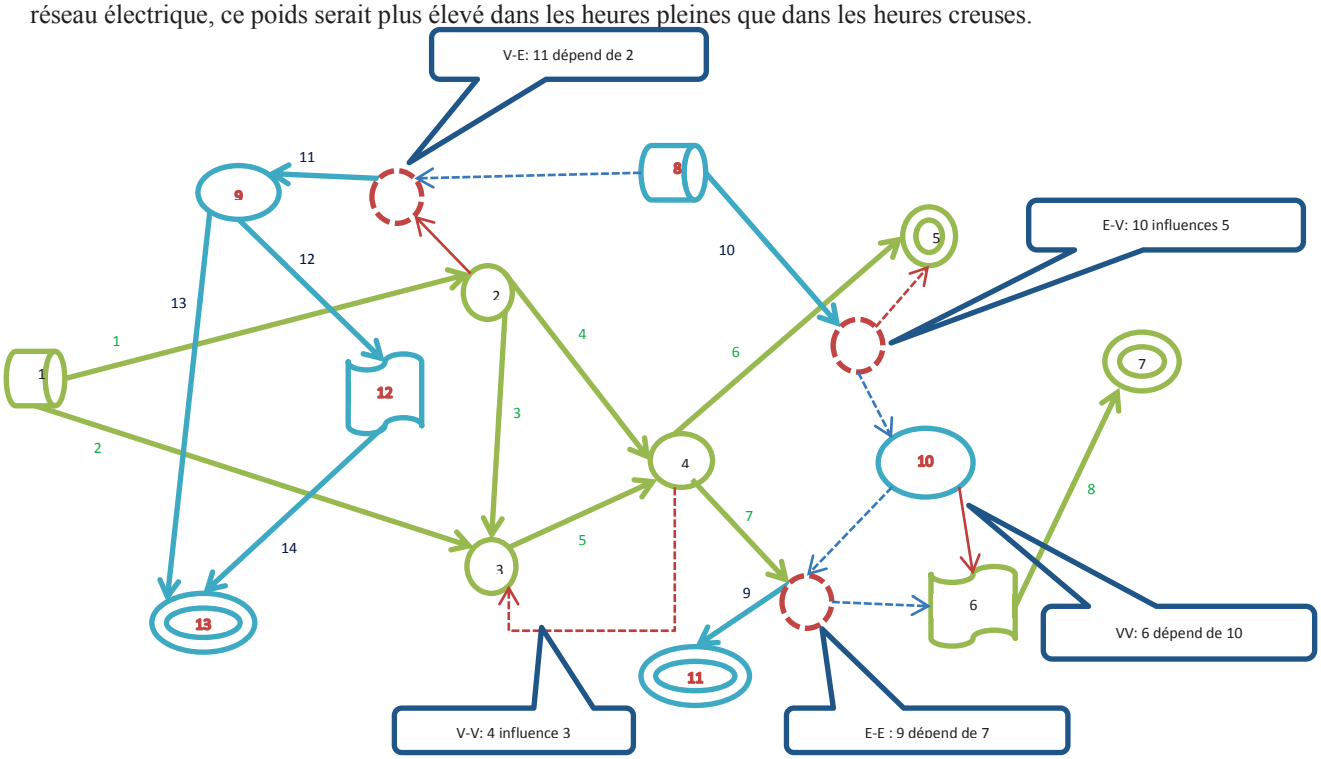

Figure 6. Exemple de Modèle Multi Systèmes Interdépendants

Ces différents éléments influencent les lois de défaillance des composants et le poids des arêtes. Nous argumentons que ces poids, ainsi que les probabilités de défaillance des composants soient des fonctions dépendantes du temps. En tenant compte tout ce qui a été dit plus haut, nous obtenons un graphe semblable à la Figure 6. Dans ce graphe, chaque composant est caractérisé par une *fonction de défaillance*. En plus de cette fonction, les arêtes sont dotées de *fonctions–poids*.

Ces éléments obtenus, nous proposons dans le chapitre suivant une démarche pour estimer le risque et la vulnérabilité.

9. Estimation de la vulnérabilité

La vulnérabilité inclue deux composants : Le composant structurel lié à l'organisation physique du réseau (Robustesse), et le composant fonctionnel lié à la circulation des différents flux (Résilience). La robustesse est une propriété statique. Elle définit l'aptitude de résister à une contrainte (Johansson, Jonsson, et Johansson 2007), et signifie que le système va maintenir ses fonctions intactes quand il est exposé aux perturbations (Petit, Robert, et Rouselle 2004). La résilience quant à elle, implique que le système peut s'adapter et retrouver une nouvelle position stable proche de sa situation initiale après l'occurrence de l'aléa (Petit, Robert, et Rouselle 2004).

Dans la littérature, certains auteurs s'accordent sur les propriétés de la vulnérabilité. Sont présentées ci-dessous celles qui nous semblent pertinentes :

- La vulnérabilité ne doit pas augmenter par ajout d'ajout d'arête ;
- La vulnérabilité est une fonction comprise entre $[0,1]$;
- Pour des réseaux différents de mêmes tailles, le graphe complet est le moins vulnérable ;
- La redondance de chemin et la présence de réseaux complémentaire pouvant transporter les mêmes éléments diminue la vulnérabilité ;
- La vulnérabilité est multidimensionnelle. C'est à dire qu'elle est liée à plusieurs paramètres.

En vertu de ces hypothèses, nous quantifions la vulnérabilité par :

$$V = \mathrm{P}(A).\frac{E_F}{E_I} \quad \{2\}$$

Où E_F est l'état final du système après l'occurrence de l'aléa, et E_I l'état initial du système avant l'occurrence de l'aléa. P(A) est la probabilité liée aux aléas considérés.

La vulnérabilité des réseaux dépend ainsi du type de sommet défaillant (Johansson, Jonsson, et Johansson 2007), de la probabilité que les composants ne remplissent pas leurs fonctions ; de la distance entre les sommets sources et cibles ; de l'importance structurelle et fonctionnelle des Sommets Sources et des Sommets Cibles ; et de l'importance relative des flux. L'état initial est calculé par :

$$E_I = \sum_k \sum_l \sum_i \alpha_i P_i \times \beta_l D_{kil} \times \gamma_k C_k \quad \{3\}$$

Où: α_i est l'importance relative du sommet cible V_i ;

P_i : Probabilité que les flux ayant pour cible le sommet V_i ne soient pas disponibles à ce même sommet. Cette probabilité est obtenue par arbre de défaillance basé sur la structure des SC résultant de la modélisation des interdépendances ;

β_l : Importance relative du flux l. Elle est donnée par agrégation des valeurs des intervenants ou de l'analyste ;

D_{kil} : Distance entre le sommet cible i et le sommet source le plus proche k, produisant le flux l ;

γ_k : Importance relative du sommet source k ;

C_k est la centralité du sommet source k. La centralité est un paramètre structurel donnant l'importance d'un composant dans le réseau.

L'état final est calculé de la même manière en tenant compte de l'impact des aléas sur le système. Cet impact peut se traduire par :

- Action sur les vecteurs de la fonction de défaillance des composants ;
- Action sur les variables de la *Fonction-Poids* des arêtes ;
- Suppression des composants selon l'amplitude et le mode d'endommagement de l'aléa ;
- Suppression aléatoire de composants (Petit, Robert, et Rouselle 2004), (Johansson, Jonsson, et Johansson 2007) ;
- Suppression de composants par degré (ou betweenness) croissant ou décroissant (Johansson, Jonsson, et Johansson 2007), (Petit, Robert, et Rouselle 2004) ;
- Suppression de composant par degré (ou betweenness) recalculé (Johansson, Jonsson, et Johansson 2007), (Petit, Robert, et Rouselle 2004).

10. Estimation des conséquences

Les conséquences résultent des impacts du système sur un ou plusieurs enjeux.

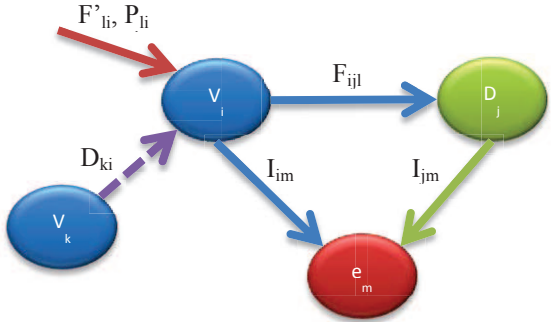

Figure 7. Graphes des conséquences

Beaucoup de méthodes d'analyse de la vulnérabilité ne tiennent pas compte des conséquences sociétales (Jönsson et Johansson 2008). Une structure est vulnérable si de faibles dommages aboutissent à des conséquences disproportionnées. Les conséquences doivent être déterminées en fonction des enjeux considérés. Ceux-ci peuvent être internes (le système lui-même) ou externe (humaine, économique, patrimonial, environnemental). Chacun de ces éléments est doté de paramètres quantifiant son niveau d'endommagement que nous appelons *Impact*. Par exemple le nombre de morts ou de blessés, les pertes économiques en euros, etc. Ces Impacts sont atténués ou aggravés par des dispositifs (hôpitaux, casernes de pompiers, cellule de crise). L'introduction des dispositifs permet d'analyser la vulnérabilité d'un groupe social attaché à un territoire donné. Entre les dispositifs circulent des flux. Les unités de ces flux sont agrégées pour obtenir un critère unique. Les dispositifs sont alimentés par divers sommets cibles du réseau. Ainsi on peut calculer l'importance de chacun de ces dispositifs, c'est-à-dire leurs centralités.

Nous estimons les conséquences pour l'ensemble des enjeux par :

$$C = \sum_m \varepsilon_m E_m \quad \{4\}$$

Où E_m : Les conséquences relatives à l'enjeu e_m , ε_m l'importance relative de l'enjeu e_m.

$$E_m = \sum_i \alpha_i I_{im} \times P_i + \sum_j I_{jm} C_j \times \sum_l \sum_i \frac{\beta_l F_{ijl} P_{li}}{M_{jl}} \quad \{5\}$$

F_{ijl} : La quantité du flux l partant du sommet source $S_i$au dispositif D_j ;

I_{im} : L'impact du sommet source S_i sur l'enjeu e_m ;

I_{jm} : L'impact du dispositif $D_j$sur l'enjeu e_m ;

P_{li} : La probabilité que le flux l soit disponible au sommet S_i ;

C_j : La centralité du dispositif D_j ;

M_{jl} : La consommation du dispositif D_j en flux l.

11. Estimation du risque

Le risque est la probabilité d'exposition d'un enjeu à un aléa et/ou la probabilité d'avoir des conséquences négatives à un moment donné dans des conditions spécifiées. Comme nous l'avons montré, le risque est fonction de la vulnérabilité, et la réduction de l'un entraine celle de l'autre. De ce point de vue, l'analyse de la vulnérabilité et du risque sont très peu dissociables. Les décisions visent le plus souvent à réduire les deux.

Le management du risque vise à répondre aux questions suivantes (Agarwal, Blockley, et Woodman 2003) :

- Qu'est qui peut être fait ?
- Quelles sont les options disponibles et quels sont les compromis associés en termes de couts, de risques et de bénéfices ?
- Quels sont les impacts des décisions de management sur les futures options ?

Le risque est souvent vu comme une entité à deux dimensions : Une Probabilité d'une part et des conséquences d'autre part (Leroy et Signoret 1992). Nous l'estimons par:

$$R = P(A) \times \frac{E_F}{E_I} \times C \quad \{6\}$$

Cette estimation ne tient compte que du risque inhérent aux réseaux considérés vis-à-vis des aléas. Mais elle ne tient pas compte de l'impact des aléas directement sur les enjeux.

Conclusion

Les catastrophes naturelles sont des événements éprouvants pour la société. Par l'intermédiaire des réseaux, elles peuvent affecter un grand nombre de population et conduire à une situation de crise. Dans cette situation, toute décision peut avoir des conséquences parfois irréversibles et mérite d'être justifiée. Pour y arriver, avant la prise de décision proprement dite, une formalisation du problème est nécessaire.

Le premier objectif de ce papier était de proposer cette formalisation et de trouver un moyen de modéliser les réseaux de manière générique avec la contrainte suivante : cette modélisation doit intégrer les interdépendances ainsi que de l'influence du milieu extérieur. Le traitement des décisions nécessitant une analyse du risque, le second objectif était de modéliser ce dernier à travers la vulnérabilité et les conséquences.

Les types d'interdépendances ont été définis et un modèle compatible avec la théorie des graphes a été proposé. Une démarche pour estimer la vulnérabilité, les conséquences et le risque a également été proposée.

Avec le modèle proposé dans ce papier, on peut en déduire entre autres : le temps de remise en état ; la courbe de réponse en fonction des scénarii ; les zones critiques ; les scenarii imprévisibles et potentiellement dommageables ; les composants critiques ; les états de vulnérabilité du système ; les cartes de vulnérabilité et du risque ; l'influence de chaque réseau sur les autres réseaux ; etc.

Par ailleurs, les décisions proprement dites reposent sur des critères. L'identification des ceux-ci et l'agrégation des certains d'eux seront notre prochain terrain d'investigation. Nous envisageons également l'usage des agents cognitifs pour la gestion de la crise, dans le cas où les décideurs seront eux-mêmes affectés par la catastrophe.

12. Bibliographie

(CCPS), Center for Chemical Process Safety, et Destree et.al. 1992. *Guidelines for Hazard Evaluation Procedures, with Worked Examples*. 2e éd. Wiley-AIChE.

Agarwal, Jitendra, David Blockley, et Norman Woodman. 2003. « Vulnerability of structural systems ». *Structural Safety* 25 (3) (juillet): 263-286. doi:16/S0167-4730(02)00068-1. http://www.sciencedirect.com/science/article/pii/S0167473002000681.

Albert, Reka, Hawoong Jeong, et Albert-Laszlo Barabasi. 2000. « Error and attack tolerance of complex networks ». *Nature* 406 (6794) (juillet 27): 378-382. doi:10.1038/35019019. http://dx.doi.org/10.1038/35019019.

Benoît, Robert, et Morabito Luviano. 2009. *Réduire la Vulnérabilité des infrastructures essentielles*. TEC & DOC. France: Lavoisier.

Berdica, Katja. 2002. « An introduction to road vulnerability: what has been done, is done and should be done ». *Transport Policy* 9 (2) (avril): 117-127. doi:doi: 10.1016/S0967-070X(02)00011-2. http://www.sciencedirect.com/science/article/pii/S0967070X02000112.

Earl E. Lee, I. I., John E. Mitchell, et William A. Wallace. 2004. « Assessing Vulnerability of Proposed Designs for Interdependent Infrastructure Systems ». In , 2:20054c. Los Alamitos, CA, USA: IEEE Computer Society. doi:http://doi.ieeecomputersociety.org/10.1109/HICSS.2004.1265182. http://www.computer.org/portal/web/csdl/doi/10.1109/HICSS.2004.1265182.

Ezell, Barry c, John V. Farr, et Ian Wiese. 2000. « Infrastructure Risk Analysis Model ». *Journal of Infrastructure Systems* 6 (3).

Holmgren, Åke J. 2007. « A Framework for Vulnerability Assessment of Electric Power Systems ». In *Critical Infrastructure*, 31-55. Advances in Spatial Science. Springer Berlin Heidelberg. http://dx.doi.org/10.1007/978-3-540-68056-7_3.

Johansson, Jonas, et Henrik Hassel. 2010. « An approach for modelling interdependent infrastructures in the context of vulnerability analysis ». *Reliability Engineering & System Safety* 95 (12) (décembre): 1335-1344. doi:doi: 10.1016/j.ress.2010.06.010. http://www.sciencedirect.com/science/article/pii/S0951832010001444.

Johansson, Jonas, Henrik Jonsson, et Henrik Johansson. 2007. « Analysing the vulnerability of electric distribution systems: a step towards incorporating the societal consequences of disruptions ». *International Journal of Emergency Management* 4 (1): 4 - 17. doi:10.1504/IJEM.2007.012385. http://www.inderscience.com/search/index.php?action=record&rec_id=12385.

Jönsson, H, et J Johansson. 2008. « Identifying critical components in technical infrastructure networks ». *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* 222 (2) (juin 1): 235 -243. doi:10.1243/1748006XJRR138. http://pio.sagepub.com/content/222/2/235.abstract.

Kamissoko, Daouda, François Pérès, et Pascale Zaraté. 2011. « Infrastructure Network Vulnerability ». In Paris.

Kaplan, Stanley, et B. John Garrick. 1981. « On The Quantitative Definition of Risk ». *Risk Analysis* 1 (1) (mars 1): 11-27. doi:10.1111/j.1539-6924.1981.tb01350.x. http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.1981.tb01350.x/abstract.

Leroy, Alain, et Jean-Pierre Signoret. 1992. *Le risque technologique*. Que sais-je 2669. France: Presses Universitaires de France (PUF).

Petit, Frédéric, Benoit Robert, et Jean Rouselle. 2004. « Une nouvelle approche pour la caractérisation des aléas et l'évaluation des vulnérabilités des réseaux de support à la vie », National Research Council of Canada, Ottawa, ON, CANADA (1974) (Revue) édition. http://cat.inist.fr/?aModele=afficheN&cpsidt=15748131.

Rinaldi, S.M., J.P. Peerenboom, et T.K. Kelly. 2001. « Identifying, understanding, and analyzing critical infrastructure interdependencies ». *Control Systems, IEEE* 21 (6): 11-25. doi:10.1109/37.969131.

Wihelmsson, Alexander, et Jonas Johanson. 2009. « Assessing Response System Capabilities of Socio Technical Systems ».