Etat de l'art sur les méthodes de modélisation pour les infrastructures critiques interdépendantes

Asma Merdassi, Raphaël Caire, Nouredine Hadjsaid, José Sanchez Torrès, Maria Viziteu, Mounir Kellil, Nouha Oualha, Sabine Machenaud, Daniel Georges, Choaib Bousba, et al.

Etat de l'art sur les méthodes de modélisation pour les infrastructures critiques interdépendantes

Asma Merdassi [1], Raphael Caire [1], Nouredine Hadj Said [1], Jose Sanchez Torres [1], Maria Viziteu [1] , Mounir Kellil[2], Nouha Oualha[2] , Sabine Machenaud [3], Daniel GEORGES [3], Choaib Bousba [3], Nadège VIGNOL [4], Philippe CARER [4], John McDONALD [4], Ludovic Piètre Cambacédès[4], Chaudet Claude[5], HECKER Artur[5]

[1]Grenoble InP/G2ELAB, [2]CEA List, [3]Atos Origin, [4]EDF(R&D), [5]TELECOM Paris Tech
G2Elab (Grenoble Génie Electrique - Grenoble Electrical engineering) ENSE3, Domaine Universitaire, BP 46, F-38402 Saint Martin d'Hères Cedex, FRANCE
Asma.Merdassi@g2elab.grenoble-inp.fr
Tél. : +33 (0) 4 76 82 64 38

Résumé – La modélisation des infrastructures critiques interdépendantes est un outil précieux pour l'identification de leurs modes de défaillance les plus critiques et d'en trouver des parades. Différentes approches ont déjà été utilisées pour modéliser les infrastructures critiques ainsi que leurs interdépendances en vue de leur sécurisation. Elles permettent de caractériser les systèmes critiques interconnectés afin de faciliter l'analyse de risques et la définition de méthodes et de mécanismes locaux et globaux de sécurisation efficaces. Cet article présente un état de l'art des méthodes adaptées à la modélisation des réseaux électriques et à leur dépendance aux systèmes TIC associés. Nous présenterons des approches basées sur la théorie des réseaux (ou systèmes) complexes, sur des outils spécialisés communicants (co-simulateur), sur des agents, sur les réseaux de Petri ou sur l'utilisation des BDMP (*Boolean logic Driven Markov Processes.*

Abstract – The objective of the modeling of critical infrastructure is the use of models to identify failure modes and the most critical to find parades. Interdependencies between the electrical networks create new vulnerabilities. In order to understand and reduce them, several approaches have been used. We wish to characterize critical systems interconnected to facilitate risk analysis and definition of methods and mechanisms to secure local and global effective. This paper deals on modelling of electrical, the communication and information networks. Several approaches are explored as complex networks theory, the building of a multi-infrastructure combined simulator (based on three dedicated software), Agent-Based Modeling, Petri nets and BDMP (Boolean logic Driven Markov Processes).

1. Introduction

Différentes approches ont déjà été utilisées pour modéliser les infrastructures critiques ainsi que leurs interdépendances en vue de leur sécurisation.

Par ce présent document, on vise à présenter un état de l'art des différentes méthodes de modélisation pour les infrastructures critiques interdépendantes que sont les réseaux électriques et leurs systèmes TIC associés telles que les Réseaux de Petri, la modélisation par agents [1] et explorer des pistes prometteuses comme la modélisation basée sur la théorie des réseaux (ou systèmes) complexes et la modélisation basée sur des outils spécialisés communicants (co-simulateur).

D'autres méthodes pourront aussi être explorées comme l'utilisation des BDMP [2] (Boolean logic Driven Markov Processes).

Dans un premier temps, nous expliquons le principe de la modélisation basée sur agents dite ABM (Agent-Based Modelling) en vue de la simulation nécessairement informatique dans ce cas, on parle alors de ABS (Agent-Based Simulation) ou ABM&S (Agent-Based Modelling and Simulation).

Ensuite, nous présenterons les différents types de réseaux de Pétri exploités de manières significatives dans les contextes TIC et électriques. Un autre type de modélisation comportementale a retenu notre attention est celui basé sur la co-simulation. Dans ce contexte, des précédents travaux à Grenoble InP portant sur la co-simulation (thèse de Benoit Rozel [3]) et un partenariat entre le Laboratoire de Génie Electrique de Grenoble (G2Elab/Inp) et la société Atos Origin ont montré la faisabilité de ce type de modélisation.

La dernière méthode de modélisation qui sera étudiée dans ce document est celle basée sur la théorie des réseaux (systèmes) complexes et qui s'intéresse à une caractérisation statique ou statistique des réseaux. Enfin, nous décrirons brièvement l'utilisation des BDMP.

2. Modélisation par agents

2.1 Principe de modélisation

La modélisation basée sur agents dite ABM (Agent-Based Modeling) est une technique de modélisation en vue de la simulation nécessairement informatique dans ce cas [4], on parle alors de ABS (Agent-Based Simulation ou ABM&S (Agent-Based Modeling and Simulation). Cette approche de modélisation a tout d'abord été utilisée en sciences sociales [4] et en écologie [5] où elle fut habituellement appelée Individual-Based Modeling (IBM). C'est une approche intrinsèquement distribuée, de bas en

haut (bottom-up), utilisant une société d'agents intelligents connectés entre eux.
Ces techniques permettent de modéliser une très large gamme de systèmes, des sociétés humaines aux systèmes électrotechniques en interaction. La sous-famille de ces modèles, les agents « cognitifs », modélisent des entités capables de raisonner sur la base de leur perception du monde et est par conséquent surdimensionnées pour les cas d'étude envisagés dans SINARI. En revanche, les systèmes composés d'agents dits « réactifs » s'intéressent à l'émergence de comportements et de propriétés à partir des comportements d'entités unitaires dépourvues d'intelligence et peut par conséquent bien rendre compte des cas d'étude envisagés dans ce projet.
Dans le cas d'étude de SINARI, les systèmes qui doivent être modélisés sont de tailles importantes. Les systèmes complexes peuvent être représentés par un ensemble d'agents passifs (objets) ou actifs (personnes) et les agents doivent interagir entre eux d'une manière simple pour faciliter leur analyse par la suite. La technique de modélisation la plus appropriée devra, par conséquent, permettre de sélectionner des niveaux de détails différents, composant par composant afin de rester calculable tout en préservant les propriétés du système réel.
De nombreux logiciels sont disponibles pour réaliser de telles modélisations, dont plusieurs comparatifs sont disponibles dans des rapports techniques [6] et en ligne [7].

2.1.1 Avantages/Inconvénients

Cette approche possède différents avantages par rapport aux techniques de modélisations classiques comme explicités dans [8] et [9]. Tout d'abord, il n'y a pas besoin de concevoir un modèle de haut niveau pour décrire le comportement complexe d'une infrastructure. À la place, on part du comportement relativement simple de différents composants de bas niveau et on les laisse coopérer. Le comportement émergeant complexe de haut niveau apparaît alors de lui même. De plus, le modèle est modulaire.

Chaque agent intègre sa propre modélisation (algorithme complexe, chaînes de Markov, ou autres), qui peut donc être différente pour chaque composant élémentaire d'un même environnement.
Un autre avantage réside dans son approche intrinsèquement distribuée, ce qui facilite la répartition du calcul sur plusieurs processeurs, si le besoin s'en fait sentir lors de la simulation.
La complexité de la modélisation multi-agent est démontrée dans les résultats simulés, et non pas dans les hypothèses émis sur le modèle. Néanmoins, les méthodes mises en œuvre dans les systèmes multi-agents sont parfois assez complexes et constituent souvent un frein à la modélisation des grands systèmes complexes.

3. Les Réseaux de Petri

3.1 Définition des Réseaux de Petri pour les systèmes TIC

3.1.1 Classe des réseaux de Petri colorés

Dans [10] R. Wu et al., un modèle de réseaux de Petri colorés (Colored Petri Net : CPN) a été proposé pour analyser de manière dynamique le flux d'information et mettre en avant les approches qui conduisent à la fuite d'information en examinant l'accessibilité du modèle CPN. En particulier, la solution introduit la reconnaissance des marquages sécurisés dans le but de vérifier de manière optimale si un flux est sécurisé ou non. Dans cette solution, les places représentent les canaux d'échange d'information dans le système. Une transition, quant à elle, correspond à un processus dans le système. La solution utilise la notion de classe de sécurité, qui peut être associée soit un jeton soit à un canal. Une classe de sécurité associée à un jeton reflète la sensibilité de l'information, alors qu'une classe associée à un canal reflète la sensibilité de l'information que le canal peut véhiculer. Un jeton contient les données à transférer et la classe de sécurité. L'ensemble des jetons dans une place correspond à l'information présente dans le canal.

3.1.2 Classe des réseaux de Petri hybrides

M. Bitam et al. [11] proposent un modèle de Petri hybride pour évaluer la performance des transmissions TCP/IP sur Internet (en particulier : l'influence des réseaux communication sur la transmission des données TCP/IP). Le comportement des communications TCP/IP (le flux de données) est modélisé en un système continu alors que celui du protocole TCP est vu comme un modèle à événements discrets. Dans cette solution la mémoire tampon (buffer) est approximée à des nombres réels alors que le flux des données est approximé à un flux continu et associé aux transitons. Le router est représenté par une place continue dont la capacité de la mémoire tampon est un nombre entier fixe. La capacité mémoire du canal quant à elle est nulle. La solution considère les débits entrant et sortant au niveau d'un routeur ; appelés aussi vitesses (ou débits) de transition.

D. Xu et al. [12] proposent un modèle qui vise à représenter les menaces de sécurité informatiques (par exemple, paiements par carte bancaire). Ce modèle est nommé réseau de Petri orienté aspect (Aspect-Oriented Petri Net).

Pour identifier les menaces de sécurité, les auteurs vérifient les transitions dans le modèle fonctionnel pour déterminer si elles sont éventuellement associées à des abus ou des anomalies qui violeraient les objectifs de sécurité.

3.2 Définition des Réseaux de Petri pour les systèmes électriques

3.2.1 Classe des réseaux de Petri hybrides

Lu, Chow et Desrochers présentent dans [13] un modèle hybride basé sur des réseaux de Petri et adapté à la modélisation de réseaux électriques (transport d'électricité et d'information). Le modèle proposé consiste en trois couches. La couche inférieure, correspondant à la modélisation de la couche physique (électricité) est implémentée à l'aide d'un modèle continu dont les jetons sont continus et dont les arcs ont des poids variables. La couche supérieure, correspondant à la modélisation du transport de l'information est implémentée à l'aide d'un modèle discret dont les jetons sont des entiers et dont les arcs ont des poids fixes. Entre ces deux couches, une interface est définie.

3.2.2 Classe des réseaux de Petri hybrides colorés

Le processus présenté dans [14] permet d'isoler et de diagnostiquer des erreurs dans des systèmes complexes, modélisés au moyen de réseaux de Pétri hybrides colorés selon la méthode du Latent Nestling. Dans un premier temps, il est nécessaire d'établir le modèle hybride du système considéré en définissant les variables discrètes et continues qui y sont utilisées.

Selon la méthodologie des réseaux de Pétri colorés, le système est ensuite séparé en sous-systèmes. On doit ensuite établir des jeux d'erreurs potentielles à diagnostiquer. A cet effet, on s'appuie sur la connaissance "physique" du système considéré, avant modélisation. On peut ensuite déterminer, en fonction des valeurs discrètes des capteurs du système, à quels états peut correspondre l'apparition de certaines erreurs du jeu préalablement identifié. Afin d'isoler les erreurs ou de détecter des erreurs simultanées le système de diagnostic s'appuie sur une analyse des variables continues.

3.3 Avantages/Inconvénients

L'analyse de la modélisation Rdp peut identifier, d'une manière qualitative seulement (cependant, un niveau de granularité approprié des INPUT est nécessaire), l'impact et les conséquences des risques de part et d'autre des deux infrastructures. Les Rdp peuvent rallier les composants des deux systèmes TIC et électrique sur le même modèle, avec leur interdépendances.

Pour les systèmes complexes, la robustesse reste à prouver pour les Rdp, il y a notamment un risque d'explosion combinatoire et malheureusement aucun outil/plateforme traitant le contexte électrique n'a pu être trouvé.

4. La Co-Simulation

4.1 Principe de modélisation

Il existe déjà quelques simulateurs multi infrastructures utilisés dans le cadre de plusieurs études de recherche. Nombre d'entre eux sont développés aux Etats-Unis à savoir le MITS (Multiple Infrastructures Tokens Simulator) dont l'objectif est de modéliser l'ensemble des réseaux de différentes infrastructures tout en minimisant les coûts de ces systèmes et en maximisant leur efficacité en cas de grandes catastrophes. Chaque système est décrit à l'aide de jetons, de cellules, de noeuds et de canaux de transports.

Cette modélisation est confrontée à de nombreuses difficultés à cause de la complexité des systèmes étudiés. En effet, chaque modèle possède son propre domaine de validité (comme par exemple la durée d'un pas de simulation ou le niveau de détail pris en compte) qui peut ne pas être compatible avec d'autres modèles.

De plus, cette approche ne permet pas forcément de rendre compte du comportement émergeant des systèmes composés de multiples infrastructures. Une autre difficulté pour cette modélisation, c'est la prise en compte du comportement humain en interaction avec les infrastructures, comportement que l'on peut considérer comme totalement imprévisible. Malheureusement, aucun des simulateurs prenant en considération le réseau électrique et les infrastructures de communication et d'information, n'est disponible.

Dans ce contexte, un partenariat entre le Laboratoire de Génie Electrique de Grenoble (G2Elab) et la société Atos Origin a abouti à la création d'un co-simulateur associé aux réseaux de transport de l'électricité. Il a été conçu pour permettre une simulation couplée (ou combinée) des infrastructures, en utilisant pour chacune, les outils déjà existants. Il s'agit d'un co-simulateur, pour l'infrastructure électrique, celle du réseau de communication et celle du centre de conduite associé (système d'information) [3].

La co-simulation est basée sur une modélisation intégrée des comportements dynamiques des différents composants d'un système/infrastructure d'une part et de leur interdépendance d'autre part pour une meilleure prise en compte des impacts mutuels sur l'ensemble.

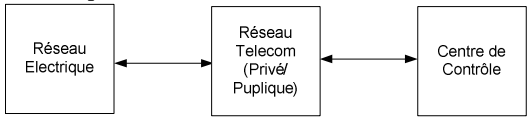

FIG.1 : Infrastructure Electrique dans la Co-Simulation du G2ELAB

4.2 Avantages/Inconvénients

La co-simulation est une extension relativement naturelle de la « mono » simulation du réseau électrique, qui pour le rappeler, existe depuis le début des années 60/70. Elle vise à élargir le périmètre de celle-ci afin d'intégrer des éléments influant sur le réseau électrique, comme le réseau de télécommunication et le centre contrôle. Ce faisant, elle permet d'affiner certaines hypothèses par rapport à celles faites dans la « mono » simulation, afin de construire des scénarios opérationnels plus réalistes.

Elle présente cependant un inconvénient, qui est probablement surmontable, il s'agit de la construction de scénarios opérationnels intégrant les trois composants

(Réseau électrique, Réseau de télécommunications, Système de supervision et de contrôle).

5. Les réseaux complexes

5.1 Utilisation des réseaux complexes dans les réseaux électriques

L'évolution des méthodologies de modélisation des réseaux électriques est liée à l'évolution des réseaux complexes, par conséquent, les premiers modèles ont utilisé la théorie des graphes pour étudier l'observabilité du système [15] et le partitionnement des réseaux électriques [16], [17]. Alvaro Torres et Anders George présentent une introduction aux classements des différentes méthodes en fonction de l'importance des postes sources sur un réseau électrique [18]. Ces méthodes utilisent la théorie spectrale des graphes. Les auteurs identifient les propriétés structurales des réseaux électriques par classement des nœuds et ils séparent par la suite le réseau en un ensemble de sous-systèmes autonomes.

D'autres auteurs comme Hongshan Zhao, Chao Zhang et Hui Ren ont appliqué la théorie des réseaux complexes afin d'étudier la vulnérabilité des réseaux électriques pour les défaillances en cascade provoquées par des défauts d'une ligne électrique [19]. Ils ont eu recours à des systèmes de test comme IEEE-30 noeuds, IEEE -57 noeuds et IEEE-118 noeuds.

Dans ce contexte, Zhenbo Wei et Liu Jungong ont proposé un modèle sur la décomposition du réseau PQ et les réseaux orientés « avec poids » afin d'analyser les vulnérabilités des réseaux électriques [20]. Ils ont utilisé le système de test IEEE 14 afin de vérifier le bon fonctionnement de leur modèle et ont conclu qu'il était important de considérer deux aspects dans l'évaluation et l'étude de la vulnérabilité : 1-) l'influence de la défaillance dans le réseau complexe et 2-) l'état de fonctionnement du réseau électrique (sensibilité QV).

Par ailleurs, S. Pahwa, A. Hodges, C. et S. Wood Scoglio ont utilisé le flux de puissance à courant continu (DC Load Flow) pour analyser les réseaux électriques par rapport à la redistribution des flux d'énergie et des pannes en cascade dans le réseau en raison de la surcharge présente dans quelques lignes de transmission [21]. Pour cela, ils ont exploité la théorie des graphes et les systèmes de test IEEE 300, IEEE 118 et WSCC 177 afin de vérifier leur méthodologie.

Leur idée est d'abord d'étudier les défaillances en cascade, puis de proposer des différentes méthodes afin de diminuer les impacts de défaillance dans le système. Malheureusement, on ne peut pas conclure sur l'efficacité de ces méthodes. Toutefois, ils ont conclu que la topologie du réseau électrique contribue efficacement à sa robustesse. D'un autre côté, ils travaillent sur l'élimination intelligente de nœuds afin de réduire la charge électrique et donc d'atténuer les défaillances en cascade.

Les développements récents dans le domaine des réseaux complexes et l'analyse des réseaux électriques permettent d'étudier les réseaux électriques d'un autre point de vue. Il existe un intérêt croissant dans ce domaine, car il permet de faire le lien entre les différentes propriétés des réseaux électriques, telles que la topologie, le flux d'énergie et les relations avec d'autres infrastructures.

5.2 Utilisation des réseaux complexes pour la technologie TIC

Les technologies de l'information et de la communication ont été étudiées depuis l'invention des réseaux complexes, surtout pour modéliser l'Internet [23], les réseaux des routeurs [24] et la propagation des virus dans l'Internet [25].

Paul Oman, Axel Krings, Daniel Conte de Leon et Jim Alves-Foss ont constaté que les systèmes complexes de contrôle en temps réel peuvent avoir des problèmes qui peuvent être résolus en utilisant la théorie des graphes [25]. Pour atteindre cet objectif et vérifier le fonctionnement du modèle, ils ont fait appel au système SCADA comme un système de test.

Les études pour modéliser les réseaux de communication et d'information ont été réalisées par plusieurs instituts de recherche. A titre d'exemple, Luciano da Fontoura, Gonzalo Travieso and Carlos Ruggiero ont étudié les caractéristiques des réseaux de communication et d'information en utilisant les réseaux complexes [26].

Ying-Ju Chi, Ricardo Oliveira et Lixia Zhang ont étudié l'interconnexion entre les routeurs sur les systèmes autonomes, ils ont obtenu un réseau de plus de 30000 noeuds et 100000 liaisons [27]. Cette méthode permet l'analyse des défaillances ainsi que les événements imprévisibles.

5.3 Avantages/Inconvénients

Les réseaux complexes sont utilisés pour la modélisation des systèmes complexes dans plusieurs domaines (les systèmes biologiques, technologiques, sociologiques,…) et l'analyse des différents phénomènes (en cascade) qui s'appliquent aux réseaux d'électricité, des phénomènes épidémiologiques, des attaques ciblées et des attaques aléatoires. Ils possèdent plusieurs caractéristiques topologiques qui reflètent le comportement du réseau. Ainsi, ils aident à la modélisation des réseaux et l'extraction de caractéristiques topologiques telles que le degré d'interconnexion et la distance entre les paires de nœuds. Ils offrent également la possibilité d'étudier la fiabilité, la sécurité et la vulnérabilité des réseaux électriques. Par contre, les inconvénients des réseaux complexes résident dans l'absence de méthode d'analyse pour l'étude des multi-infrastructures, tels que les réseaux électriques et les réseaux de communication et de logiciels dédiés à nos besoins. En effet au jour d'aujourd'hui, les outils existants sont développés en fonction du domaine d'application et des besoins spécifiques des utilisateurs.

6. BDMP

6.1 Origine et présentation générale

Les BDMP (*Boolean logic Driven Markov Processes*) désignent un formalisme graphique issu du domaine de la

sûreté de fonctionnement. Inventés par Marc Bouissou au début des années 2000 [2], ils sont depuis employés à EDF dans par exemple des études de sûreté de systèmes élémentaires de centrales nucléaires, de systèmes d'évacuation des crues de barrages hydrauliques, ou dans des analyses de disponibilité de postes électriques ou d'alimentation électrique d'installations diverses (e.g. *data centers*, usines, aéroports).

Ils combinent l'aspect visuel des arbres de défaillances, héritant de leur lisibilité et de leur facilité d'appropriation, avec la puissance de modélisation des modèles de Markov. En première approche, on peut présenter les BDMP comme modifiant la sémantique classique des arbres de défaillances selon deux modalités principales :

- ils associent aux feuilles de l'arbre des processus de Markov qui modélisent le comportement des composants selon plusieurs modes. Plus explicitement, chaque feuille peut être considérée dans un mode « sollicité », correspondant à un état du système où le composant modélisé par la feuille contribue au fonctionnement global du système, ou dans un mode « non-sollicité », qui signifie que le composant correspondant n'est pas requis (il est par exemple au repos car en redondance à froid).

Un processus de Markov simple modélise pour chaque mode le comportement du composant en termes de défaillance et de réparation. La Figure 2, ci-dessous, correspond aux processus d'une feuille permettant de modéliser les redondances. La valeur des taux de défaillance (λ) diffèrent selon le mode (celle du taux de réparation μ est par contre supposée identique) ; la feuille correspond à une redondance à froid quand $\lambda_0 = 0$.

- ils introduisent un nouveau type de lien, nommé gâchette, représenté par une flèche rouge en pointillé, qui permet de sélectionner le mode des feuilles en fonction de l'état d'autres feuilles. En d'autres termes, ce lien spécifie graphiquement de quels autres composants le mode de sollicitation d'un composant dépend.

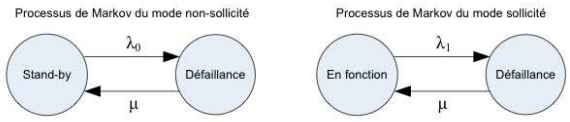

FIG.2 : Exemples de processus de Markov associés aux modes des feuilles

Pour une feuille donnée, les processus correspondant à chaque mode et les fonctions spécifiant le passage d'un mode à l'autre, déclenché notamment par les gâchettes, forment un « processus de Markov piloté ». Ce formalisme offre trois avantages essentiels par rapport aux autres modèles dynamiques en sûreté de fonctionnement :

- d'une part, il permet la définition de modèles dynamiques complexes tout en restant presque aussi lisible et facile à construire qu'un arbre de défaillances. En particulier, les BDMP peuvent être utilisés pour construire simplement et rapidement des modèles correspondant à de nombreuses situations courantes dans les études de sûreté de fonctionnement, telles que redondances passives, simples ou en cascade, défaillances de cause commune, reports de charge, fonctionnements différenciés selon les séquences d'événements, etc. ;
- d'autre part, leurs propriétés mathématiques autorisent le traitement efficace de BDMP équivalents à des processus de Markov avec un espace d'états extrêmement grand. Un mécanisme d'élagage, dit de « filtrage des événements pertinents », permet en effet de réduire considérablement la combinatoire dans l'exploration des chemins menant à l'événement redouté, effectuée lors du traitement du modèle ;
- enfin, en plus des calculs classiques de disponibilité et de fiabilité, ils permettent d'obtenir des informations qualitatives d'intérêt sous la forme de listes des séquences menant à l'événement redouté, caractérisées quantitativement et ordonnées selon leur contribution à la probabilité d'occurrence de l'événement redouté dans le temps de mission considéré pour le système.

6.2 Avantages et inconvénients

Les avantages génériques des BDMP ont déjà été mentionnés : représentations compactes et lisibles de systèmes complexes, formalisation mathématique robuste, traitement efficaces des modèles, retour d'expérience industriel. Sur ce dernier plan, il faut en effet souligner que les BDMP bénéficient de la plate-forme logicielle KB3, utilisée par EDF depuis plus de quinze ans pour ses études de sûreté de fonctionnement [29] et que de nombreuses études ont été menées sur cette base.

Un avantage plus spécifiquement lié à SINARI tient dans le fait que les BDMP ont été employés dans des contextes très pertinents pour le projet et que certains partenaires possèdent une bonne maitrise à la fois théorique et pratique les concernant.

Evidemment, la modélisation des interdépendances entre infrastructures électrique et télécom, dans une approche incluant défaillances accidentelles et malveillantes, n'a jamais été entreprise avec des BDMP. Si elle semble séduisante à première vue, une telle approche comporte donc des risques du fait de la nouveauté de la démarche.

D'une façon moins spécifique, les BDMP ont un certain nombre de défauts intrinsèques qu'il conviendra de confronter aux exigences de la problématique traitée. En outre, on peut citer leur difficulté à prendre en compte des créations/destructions d'éléments en cours de vie du système modélisé, et leur difficulté à modéliser les comportements cycliques/boucles. Dans ces cas particuliers, les réseaux de Petri s'avèrent souvent plus pertinents.

7. Conclusion

L'utilisation croissante et le progrès des technologies de l'information et de la communication, qui répondent à des besoins réels, ont clairement apporté de nombreux bénéfices. Néanmoins, l'utilisation de ces techniques, qui certes évoluent très rapidement, a parfois un impact sur le fonctionnement du réseau électrique et peut s'avérer source de vulnérabilités.

Afin de bien situer l'état de l'art dans le domaine de la modélisation des interdépendances entre les infrastructures critiques, une étude bibliographique a été réalisée. Ces méthodes seront exploitées et testées ultérieurement dans le cadre du projet SINARI.

8. Bibliographie

[1] Charles M. Macal and David Sallach, editors. Workshop on Agent Simulation : Applications, Models, and Tools, The University of Chicago, October 1999.

[2] M. Bouissou and J.-L. Bon, A new formalism that combines advantages of fault-trees and Markov models : Boolean logic driven Markov processes, Reliability Engineering & System Safety, vol. 82, p. 149–163, nov. 2003.

[3] B. Rozel, "La sécurisation des infrastructures critiques : recherché d'une méthodologie d'identification des vulnérabilités et modélisation des interdépendances". Thèse à l'Ecole Doctorale « Electronique, Electrotechnique, Automatique et Traitement du Signal », 2009

[4] E. Bonabeau. Agent-based modeling : Methods and techniques for simulating human systems. In Proc. of the National Academy of Sciences of the USA, volume 99, pages 7280–7287. National Academy of Sciences of the USA, May 2002.

[5] V. Grimm. Ten years of individual-based modelling in ecology : what have we learned and what could we learn in the future ? Ecological Modelling, 115(2–3) :129–148, 1999.

[6] Rob Allan, Survey of Agent Based Modelling and Simulation Tools, Available Online

[7] http://en.wikipedia.org/wiki/Comparison_of_agent-based_modeling_software

[8] Dianne C. Barton and Kevin L. Stamber. An agent-based microsimulation of critical infrastructure systems. In 8th International Energy Forum, Las Vegas, March 2000. International Energy Foundation's ENERGEX 2000.

[9] C. Macal and M. North. Tutorial on agent-based modeling and simulation. In Proc. of the 2005 Winter Simulation Conf., December 2005.

[10] Ruoyu Wu and al., "Colored Petri Nets Based Modeling of Information Flow Security," International Workshop on Knowledge Discovery and Data Mining, Janurary 2009, pp. 681-684.

[11] M. Bitam, H. Alla, "Performance evaluation of a TCP/IP transmission using hybrid Petri nets," Computer Systems and Applications, ACS/IEEE International Conference on, pp. 54-I, ACS/IEEE 2005 International Conference on Computer Systems and Applications (AICCSA'05), 2005

[12] D. Xu and K E. Nygard, "Threat-Driven Modeling and Verification of Secure Software Using Aspect-Oriented Petri Nets", IEEE Transactions on Software Engineering, April 2006, pp.265-278.

[13] Ning Lu Chow, J.H. Desrochers, A.A, "A multi-layer Petri net model for deregulated electric power systems", IEEE , pp.513-518.

[14] L. Rodriguez, E. Garcia, F. Morant, A. Correcher and E. Quiles , « Fault diagnosis for complex systems using Coloured Petri Nets », in Petri Nets Applications Edited by Pawel Pawlewski, February 2010.

[15] G. Korres and P. Katsikas, "A Hybrid Method for observability analysis using a reduced Network graph theory", IEEE Transactions on Power Systems, Vol. 18, No. 1, Février 2003.

[16] X. Wang and V. Vittal, "System Islanding using minimal cutsets with minimum Net Flow". IEEE PES Power Systems Conference and Exposition. pp. 379-384, 10 – 13 Octobre, 2004.

[17] R. Moreno, M.A.Rios et A. Torres, "Security Schemes of Power Systems against blackouts". VIII IREP Symposium – Bulk Power System Dynamics and Control, Buzios, Brazil. 1 – 6 Août, 2010.

[18] A. Torres and G. Anders, "Spectral Graph theory and network dependability". 4th International Conference on Dependability of Computer Systems RELCOMEX'09. pp. 356-363. June 30 – Juillet 2 2009.

[19] H. Zhao, C. Zhang et H. Ren, "Power Transmission Network Vulnerable Region Identifying Based on Complex Network theory". Electric Utility Deregulation and Restructuring and Power Technologies. DRPT2008, Nanjing China. pp. 1082-1085. 6-9 Avril 2008.

[20] Z. Wei and J. Liu, "Research on the Electric Power Grid Vulnerability under the Directed-weighted Topological Model Based on Complex Network Theory". International Conference on Mechanic Automation and control engineering (MACE), pp. 3927-3930. 26 – 28 Juin, 2010.

[21] S. Pahwa, A. Hodges, C. Scoglio et S. Wood, "Topological analysis of the power grid and Mitigation Strategies against Cascading Failures". 4th Annual international IEEE Systems conference, San Diego, USA. Pp. 272-276. Avril 5-8, 2010.

[22] R. Albert, H. Jeong, A.-L Barabasi. "Diameter of the world wide web". Nature. No. 401. Pp. 130 – 131. 1999.

[23] J.-P. Onnela, J. Saramaki, J. Hyvonen, G. Szabo, D. Lazer, K. Kaski, J. Kertesz, A.-L. Barabási. "Structure and tie strengths in mobile communication networks". Proceedings of the National Academy of Sciences. Vol. 104, No. 18, pp. 7332-7336, 2007.

[24] M.E.J. Newman, S. Forrest et J. Balthrop. “Email networks and the spread of computer viruses”. Physical Review E, Vol. 66, No. 3, 2002.

[25] P. Oman, A. Krings, D. Conte de Leon, J. Alves-Foss. “Analyzing the security and survivability of Real-Time control Systems”, Proceedings of the 2004 IEEE, Workshop on information Assurance. pp. 342-349. Juin 10-11 2004.

[26] L. Costa, G. Travieso and C.A. Ruggiero, “Complex Grid Computing”, The European Physical Journal B, Vol. 44, No. 1, pp. 119-129, 2005.

[27] Y-J. Chi, R. Oliveira et L. Zhang. “The AS-level connectivity observatory”. ACM Computer Communications Review. Vol. 38, No. 5. Oct. 2008.

[28] Ludovic Piètre Cambacédès, Des relations entre sûreté et séecurité, Thèse de doctorat, Télécom ParisTech, novembre 2010

[29]Schneier, B. Attack trees: Modeling security threats Dr. Dobb's Journal, 1999, 12, 21-29.