La sécurisation des infrastructures critiques : recherche d'une méthodologie d'identification des vulnérabilités et modélisation des interdépendances

Benoît Rozel

INSTITUT POLYTECHNIQUE DE GRENOBLE

N° attribué par la bibliothèque

THÈSE

pour obtenir le grade de

DOCTEUR DE L'Institut polytechnique de Grenoble

Spécialité : « Génie Électrique »

préparée au laboratoire de Génie Électrique de Grenoble (G2Elab)

dans le cadre de **l'École Doctorale « Électronique, Électrotechnique, Automatique et Traitement du Signal »**

présentée et soutenue publiquement par

Benoit ROZEL
Ancien élève de l'ENS Cachan – Agrégé de Génie Électrique

le 8 juillet 2009

La sécurisation des infrastructures critiques : recherche d'une méthodologie d'identification des vulnérabilités et modélisation des interdépendances

---

sous la direction du Pr Nouredine Hadjsaïd

JURY

Pr Mohamed Machmoum,	Président et rapporteur
Pr Ronnie Belmans,	Rapporteur
Ing Marcelo Masera,	Examinateur
Pr Nouredine Hadjsaïd,	Directeur de thèse
Dr Raphaël Caire,	Co-encadrant
Pr Jean-Pierre Rognon,	Examinateur

À mes parents
À Camille

Douter de tout ou tout croire sont deux solutions également commodes qui, l'une comme l'autre, nous dispensent de réfléchir.

Henri Poincaré

Remerciements

Je souhaite remercier tout d'abord l'ensemble des membres du jury. En particulier, les rapporteurs Mohamed Machmoum et Ronnie Belmans. En effet, ce sont eux qui donnent la valeur à cette thèse. Je remercie également les encadrants Nouredine Hadjsaïd pour la proposition du sujet et la direction de cette thèse, Raphaël Caire pour la codirection de stages M2R et la deuxième partie de la thèse (et tout le reste que je cache dans ces ...) et Jean-Pierre Rognon pour la première partie. Je souhaite également remercier ma cobureau Carolina Tranchita pour son implication dans l'encadrement en fin de ma thèse, ses apports, ses corrections et ses suggestions. J'en profite aussi pour remercier mon autre cobureau colombienne, Lina-Maria Ruiz. Je remercie fortement Maria Viziteu et Alexandre Teninge pour leurs contributions à l'amélioration de ma présentation. Pour l'organisation et l'aide apportée le 8 juillet, en plus du grand apport de Maria, merci aux deux compagnons de randonnées Damien Picault et Yann Riffonneau.

Je tiens également à remercier l'ensemble des collègues du laboratoire que j'ai pu côtoyer lors de ces trois années. Je ne saurais être exhaustif (heureusement pour le lecteur), mais je tiens particulièrement à citer Éric Vagnon et Benjamin Vincent pour les échanges que l'on a pu partager, les deux cachanais Olivier Deleage et Nicolas Rouger. Parmi les anciens : Bogdan, Erwan, Octavian et Sylvie ; les valeureux cyclistes : Jérémie Aymé, Guillaume Foggia, Édouard Bomme, Marcel Ebene Ebene, Boris Berseneff, Stéphane Vighetti et Philipp Tritschler. Je n'oublie pas non plus Sylvain Mandray, Diem Nguyen Ngoc, Marie-Cécile Alvarez et Szymon Racewicz. Je souhaite aussi (re-)citer dans cette page mes stagiaires M2R Maria et Silong Seng, mon tuteur de monitorat Daniel Roye ainsi que Gérard Meunier, Danielle Collin et Rosita Atienza pour leur accueil. J'ajouterais à cette liste Stéphane Catellani, Antoine Labonne, Delphine Riu et Bertrand Raison pour les enseignements et les Fêtes de la Science. Merci également à Pierre-Olivier Jeannin pour son aide et les discussions vis-à-vis des candidatures de PRAG ainsi que la direction du G2Elab.

Je remercie également le ministère de l'Éducation Nationale de m'avoir financé durant les sept dernières années.

Je ne peux pas clore cette page sans remercier mes parents de leur soutien. Merci à ma sœur Christelle, ainsi que mes neveux Émile et Antoine, d'être venus à ma soutenance. Une pensée à mes deux autres sœurs Céline et Bénédicte qui du fait de leur travail respectif n'ont pas pu y assister mais ne m'ont pas oublié.

Et pour finir un énorme **MERCI** à Camille pour son soutien, son enthousiasme, sa patience, son écoute, son efficacité et tout le reste.

Table des matières

Introduction générale

Ce travail de recherche s'inscrit dans un contexte de profondes mutations de la gestion des réseaux électriques aussi bien en termes de moyens techniques utilisés qu'en terme organisationnel.

Les technologies des systèmes de communication et d'information ont effectué des progrès immenses lors de ces dernières décennies. Ces deux technologies ont eu des répercussions importantes sur l'infrastructure essentielle et stratégique qu'est le réseau électrique. En effet, ce dernier a été créé à la fin du dix-neuvième siècle, à la même époque que l'invention du téléphone et bien avant la création du premier ordinateur dans les années 1940. L'utilisation de l'outil informatique pour l'exploitation des réseaux électriques est donc toute récente à l'échelle de leur histoire (dans les années 1950). Cette utilisation a, bien entendue, été progressive, en commençant par des outils d'aides à la conduite des gestionnaires, puis par la réalisation des fonctions non critiques pour arriver finalement à s'immiscer intimement dans son fonctionnement.

Par ailleurs, en parallèle à ce premier phénomène, il est devenu de plus en plus difficile de construire de nouvelles lignes électriques pour des raisons environnementales et d'acceptation par les populations locales.

Ces dernières années la conjonction de ces deux phénomènes a conduit à une utilisation croissante des technologies de l'information et de la communication par les gestionnaires de réseau électrique. L'infrastructure « physique », et plus particulièrement les lignes du réseau de transport, n'évolue quasiment plus. Pourtant, la demande de consommation d'énergie électrique n'a cessé de croître que ce soit en terme d'énergie totale (+1,2% pour la France en 2008 par rapport à 2007 et +9,1% sur les sept dernières années) ou d'amplitude du pic annuel. Pour illustrer ce dernier point, alors que le record de consommation en France datait de l'hiver 2007–2008 , il a déjà été battu trois fois au cours de l'année (2009) avec comme plus forte valeur 92 400 MW le 7 janvier 2009 à 19h malgré des actions de sensibilisation de maîtrise de la consommation [RTE09]. Un fait nouveau vient contraindre d'autant plus la gestion des réseaux électriques. Il s'agit de la production issue de sources d'énergies renouvelables et intermittentes. Ainsi, en France en 2008, l'éolien a atteint une production de 5,6 TWh, soit un peu plus d'un pour cent de la production française d'électricité. Cela représente une augmentation de 37,4% par rapport à l'année précédente et une multiplication par un facteur 14 en 5 ans. Au niveau européen en 2007, l'énergie éolienne représentait 3,7% de la production d'électricité. Des projections prévoient une augmentation de cette proportion à 5,0% en 2010, 11,7% en 2020 et 21,2% en 2030

[EWE09]. La nature intermittente et fatale de ce type de production et son niveau de moins en moins marginal amène, lui aussi, à un accroissement de la complexité des contraintes d'exploitation. Par conséquent, ces réseaux fonctionnent de plus en plus proches de leurs limites. N'étant plus capable de prédire avec certitude les flux de puissance dans les lignes, les marges de fonctionnement se réduisent. Auparavant, la sécurité était essentiellement basée sur cette importante marge entre le fonctionnement et la capacité. Il est maintenant difficile de maintenir ce mode d'opération. Cependant, l'infrastructure électrique continue de fonctionner. Les technologies de l'information et de la communication jouent un rôle de plus en plus important dans leur bon fonctionnement. Elles sont utilisées pour les fonctions de télé-conduite, d'estimation d'état du réseau électrique et du réglage coordonné de tension et de fréquence, entre autres. Elles sont également indispensable pour permettre la coordination entre les multiples acteurs dans le cadre de la dérégulation des marchés de l'électricité. L'usage de ces technologies permettent également de réduire les coûts de fonctionnement actuels. De même, on peut noter que ces dernières évoluent énormément et beaucoup plus rapidement que les techniques du réseau électrique. Par conséquent, elles sont de plus en plus complexes et difficiles à maîtriser totalement. De plus, on est passé de l'utilisation de technologies spécifiquement développées à l'usage de solutions génériques donc avec des vulnérabilités plus aisément exploitables.

Pour résumer, le contexte de ce travail concerne donc l'utilisation et la dépendance croissantes des technologies de l'information et de la communication par l'infrastructure électrique ayant pour origine un besoin accru de ces technologies. Il y a également une augmentation de la complexité de ces infrastructures. À cela, vient s'ajouter l'apparition de faiblesses dues à des défaillances en cascades entre les infrastructures.

En partant de ce contexte, on souhaite sécuriser les infrastructures critiques. Cette sécurisation ne peut pas se faire sans une meilleure compréhension des interdépendances et du comportement des systèmes couplés. Cette augmentation de la compréhension est atteignable grâce à la modélisation. On cherche donc à modéliser les interdépendances des infrastructures critiques. Les objectifs de cette modélisation sont :

- établir un modèle *commun / unique* de modélisation,
- mettre en évidence des modes communs de défaillances et des effets de cascade,
- caractériser la criticité du réseau de communication en vue de la sécurité du réseau électrique,
- rechercher des points les plus faibles, qui ne sont pas nécessairement des éléments physiques, cela peut être par exemple une topologie.

Afin de bien appréhender les interdépendances entre les différents systèmes couplés, il est important d'établir un modèle unifié et non pas simplement juxtaposer des modèles spécifiques distincts. Cette modélisation est importante car elle va permettre de mieux comprendre la complexité des phénomènes au sein des infrastructures couplées. Cette compréhension est la première étape en vue de la sécurisation des infrastructures.

Le plan de ce mémoire est le suivant : il sera tout d'abord exposé au premier chapitre les enjeux de la sécurisation des infrastructures critiques. Au chapitre deux, sera présenté un état de l'art de la modélisation des infrastructures critiques avec les différentes approches utilisées. Puis, une de ces approches, la simulation comportementale, fera l'objet du chapitre trois avec la présentation d'un cosimulateur multi-infrastructures. Le chapitre quatre exposera une approche différente, la théorie des réseaux complexes. Cette théo-

rie servira d'inspiration pour une proposition d'approche novatrice de modélisation des systèmes multi-infrastructures. Elle sera présentée, d'un point de vue théorique, mise en œuvre et résultats, au chapitre cinq.

Chapitre I

La sécurisation des infrastructures critiques

Sommaire

Résumé

Les infrastructures critiques sont constituées de l'ensemble des grands réseaux indispensables au bon fonctionnement d'une société. Leur sécurisation est donc, par nature, un enjeu majeur pour cette dernière. Ce mémoire s'attache particulièrement aux réseaux électriques et de télécommunications associés. Ces réseaux sont d'une importance majeure pour les autres infrastructures critiques. Après plus d'un siècle d'utilisation de l'électricité et à l'époque d'Internet, il est de plus en plus difficile d'accepter des pannes généralisées sur ces réseaux. Les conséquences d'un tel accident sont dramatiques à la fois socialement et économiquement. Les technologies de l'information et de la communication sont de plus en plus utilisées pour la conduite des réseaux électriques car ils permettent aux opérateurs de faire fonctionner leurs réseaux plus proche de leurs limites physique. Par conséquent cela conduit à une réduction des investissements à réaliser pour un niveau de service identique. Réciproquement, les réseaux informatiques et de télécommunications ne peuvent fonctionner que grâce à la disponibilité de l'énergie électrique, même si dans bien des cas des pannes de courtes durées sont tolérées du fait de l'usage d'alimentations sans interruptions. Cet accroissement des dépendances entre les infrastructures amène à l'apparition de nouvelles vulnérabilités qu'il s'agit d'identifier.

I.1 Enjeux de la sécurisation des infrastructures critiques

Le contexte de ce travail de recherche a été présenté dans l'introduction générale. Il a alors été vu que l'infrastructure électrique dépendait de plus en plus des moyens informatiques et de télécommunications ainsi que les raisons de cette dépendance. Cependant, cette dépendance accrue, malgré les aspects bénéfiques qu'elle apporte, ne va pas sans poser de nouveaux problèmes. Ainsi, le mauvais fonctionnement d'un composant de l'infrastructure de communication dans un système de supervision peut conduire des opérateurs à prendre des décisions non appropriées et affecter sévèrement le système supervisé. Ce dernier peut être, par exemple, une partie du réseau électrique ou bien une unité de production d'énergie électrique. Réciproquement, une panne localisée peut provoquer la saturation du réseau de télécommunication qui peut ensuite rendre indisponible le service des urgences dans des circonstances critiques comme montré dans l'article [OUCB05]. Ces deux exemples montrent que les interdépendances de plus en plus présentes entre les infrastructures conduisent à l'apparition de nouvelles vulnérabilités.

Ces vulnérabilités sont alors des sources potentielles d'incidents ou d'accidents impliquant le non fonctionnement d'une partie ou de la totalité des infrastructures considérées. Jusqu'au début du vingtième siècle, l'usage de ces infrastructures était réservé à une minorité de la population, par conséquent les conséquences d'un dysfonctionnement n'avaient qu'un impact relativement faible sur la société. Mais depuis la seconde moitié du vingtième siècle, l'usage de ces technologies s'est peu à peu répandu jusque devenir totalement indispensable. Ainsi, selon l'INSEE (Institut National des Statistiques et des Études Économiques), en 2006 87,6% des ménages français étaient équipés d'un téléphone fixe et 74,3% d'au moins un téléphone portables. Le taux d'utilisation de l'énergie électrique devant être compris entre 99% et 100%. Au niveau mondial, plus de quatre milliards de personnes ont accès à l'électricité (et donc son corollaire, plus de deux milliards en sont privés).

Un autre point à prendre en considération est le bon fonctionnement habituel de ces réseaux. Celui-ci a, en effet, un impact psychologique important. Ainsi dans les zones rurales, les coupures de réseau électrique ou téléphonique sont, relativement aux zones urbaines, plus fréquentes. Et quand une coupure un peu longue intervient, les populations du milieu rural étant plus habituées et donc préparées à ce genre d'évènement, elles sont moins impactées dans leur mode de vie. Tandis que lorsque de longues coupures touchent des zones urbaines (événement exceptionnel), cela devient rapidement catastrophique pour une partie de la population qui ne sais pas gérer ce genre de situation. Ainsi, lors du délestage de la soirée du 4 novembre 2006 d'une partie de la population française pendant 30 minutes, les standards des centres de secours ont été saturés d'appels de personnes littéralement catastrophées par l'absence d'électricité dans leur maison et leurs quartiers sans qu'aucun danger vital ne soit réellement avéré. En dehors de la population, c'est quasiment l'ensemble de l'activité économique qui est impactée par une panne généralisée. Bien que les processus critiques soient protégés par des alimentations sans interruptions (ASI), leur durée d'autonomie varie en fonction de l'importance perçue de la fonction réalisée et rares sont celles pouvant tenir la durée d'une panne généralisée (de l'ordre de une ou plusieurs dizaine d'heure suivant le temps de rétablissement). Ainsi, de telles pannes ont la capacité de paralyser totalement l'ensemble de l'activité économique de la

zone touchée. Par exemple, le coût économique global de la panne généralisée de août 2003 aux États-Unis est estimé entre 7 et 10 milliards de dollars [SM03]. Un des rares point positif de ce type d'incident est une hausse observée de la natalité dans les neuf mois suivant l'événement, phénomène observé aussi bien suite à la tempête de fin décembre 1999 en France ou en août 2003 aux États-Unis.

En ce qui concerne l'état des lieux, il faut noter que la majorité des pannes ont des causes accidentelles, c'est-à-dire qu'elles ont rarement pour origine des actions de malveillances mais proviennent d'évènements naturels ou d'erreurs humaines.

L'ensemble de ces risques ne sont pas que probables, mais bel et bien réels. Ainsi, les pannes généralisées de cette décennie en Europe et de par le monde ont montré que le système électrique était réellement vulnérable. Par ailleurs, dans la société actuelle, la tendance est de vouloir tout contrôler, tout maîtriser, tout sécuriser, comme le montrent par exemple la multiplication des caméras de vidéo surveillance dans les lieux publics ou l'omniprésence des processus de normalisation (au sens ISO 9001) et de traçabilité. Un problème non prévu sur la fourniture d'énergie électrique ou sur les moyens de télécommunication qui sont au cœur de nos modes de vies actuels devient alors difficile à admettre voir totalement inacceptable.

Pour toutes les raisons exposées précédemment, la sécurisation des infrastructure critiques est importante et même une préoccupation actuelle majeure pour notre société. Ainsi, la directive 2005/89/CE du parlement européen et du conseil du 18 janvier 2006 [peelcdle06] énonce des mesures visant à garantir les investissements dans les infrastructures et la sécurité de l'approvisionnement en électricité, c'est-à-dire la capacité du système électrique à fournir aux clients finals de l'énergie électrique. Dans le cadre du FP7 (*Seventh Framework Programme*), il existe des projets européens concernant cette thématique. Aux États-Unis, il existe une commission spécifique sur la protection des infrastructures critiques.

La sécurisation des infrastructures critiques est une tache complexe qui ne peut être atteinte seulement si le comportement des systèmes multi-infrastructures est bien compris et en particulier leurs interdépendances. Comme il s'agit avant tout de phénomènes physiques, cette meilleure compréhension peut-être atteinte par une modélisation. Ainsi la modélisation des interdépendances entre les infrastructures critiques est la première étape nécessaire en vue de les sécuriser. Comme on le verra par la suite, cette étape n'est pas triviale et la difficulté de la tâche due à la complexité des phénomènes conjuguée à la diversité d'objectifs possibles (comme par exemple minimiser un nombre de décès ou un coût financier, sécuriser une infrastructure ou l'ensemble) amène à l'utilisation de différentes approches qui peuvent être théoriques ou de simulation, de haut niveau à l'échelle d'un pays ou de bas niveau à l'échelle d'une ville en intégrant le facteur humain et en particulier son caractère imprévisible ou en l'évitant.

I.2 Définitions

Après avoir évoqué le contexte et les enjeux de la sécurisation des infrastructures critiques, il est maintenant important de définir avec précision la signification des termes infrastructure critique, interdépendance, défaillance, sécurisation et vulnérabilité pour cette étude.

I.2.a Infrastructure critique

Étymologiquement, le mot infrastructure vient du latin *infra- structura* de *struere* construire et signifie « au dessous de la construction » et le mot critique du grec *kritikos* de *krinein* discerner signifie « difficile, décisif ». Ainsi les infrastructures critiques sont les constructions décisives pour notre société.

On peut définir simplement les infrastructures critiques comme l'ensemble des systèmes essentiels. Ainsi, les réseaux électrique, de télécommunication, d'eau, de gaz et de pétrole, d'égouts, de transports qu'ils soient ferrés, routiers, aériens ou fluviaux, ainsi que les service d'urgences et médicaux sont considérés comme des infrastructure critiques. Aux États-Unis, la définition est même un peu plus large. Selon le rapport de la commission de protection des infrastructures critiques [Mea97], ces dernières sont les infrastructures qui sont tellement vitales que leur indisponibilité ou destruction aura un impact affaiblissant sur la sécurité nationale ou économique. Ces infrastructures sont celles citées précédemment plus les administrations publiques et le système bancaire et financier.

L'infrastructure de télécommunication a depuis quelques décennies évoluée en une infrastructure d'information et de communication composée principalement des différents réseaux téléphoniques (filaires et cellulaires) et de l'ensemble des réseaux formant l'Internet. Les principaux objectifs des réseaux de communication sont de partager les ressources, avoir une plus grande fiabilité du fait de la facilité de duplication des données et une réduction des coûts [Tan99]. L'infrastructure électrique est quant à elle composée de l'ensemble des moyens de production, de transport et de distribution de l'énergie électrique. Elle se décompose en réseau de transport, réseau de répartition et réseau de distribution. Parmi eux, on va s'intéresser seulement au réseau de transport car c'est celui dont le non fonctionnement provoque le plus de conséquences négatives. En plus des composants purement électrotechniques tels que les générateurs, les lignes, les transformateurs et les postes sources, cette infrastructure nécessite également un système de contrôle appartenant à l'infrastructure d'information et de communication. Ses fonctions sont de conduire et réguler les paramètres physiques de l'infrastructure électrique ainsi que de permettre des reconfigurations en situation d'urgence. Les principales caractéristiques de ces deux infrastructures sont qu'il s'agit de réseaux composés de milliers, de millions ou de milliards de nœuds dont la structure est irrégulière, complexe et évolue dynamiquement dans le temps. Cette évolution se fait avec des échelles de temps plus rapides pour l'infrastructure d'information et de communication que l'électrique.

Dans la suite de cette thèse, on a choisi de s'intéresser plus particulièrement à ces deux infrastructures qui sont importantes pour le bon fonctionnement de toutes les autres.

I.2.b Interdépendance

D'une manière générale, une interdépendance entre deux entités est une relation de dépendance réciproque entre celles-ci. Le dictionnaire de l'académie française dans sa huitième édition défini les dépendances comme les rapports qui lient certaines choses, certains êtres, et qui les rendent nécessaires les uns aux autres, du latin *dependere*, pendre, se rattacher à. Ainsi, les interdépendances entre les infrastructures critiques correspondent à toutes liaisons qui rendent nécessaire une infrastructure à une autre et réciproquement.

Dans cette étude, la définition utilisée est plus restrictive en ne considérant que les

interactions plus ou moins explicites entre les systèmes pouvant aboutir à des défaillances.

L'article [RPK01] définit quatre classes d'interdépendances : physique, cybernétique, géographique, logique. Chacune possède ses propres caractéristiques mais ces classes ne sont pas mutuellement exclusives :

Physique Deux infrastructures sont physiquement interdépendantes si l'état de chacune dépend d'une sortie matérielle de l'autre. Un exemple est les infrastructures d'approvisionnement d'eau et électrique. La première a besoin d'électricité pour faire fonctionner les pompes et l'infrastructure électrique a besoin d'eau pour le refroidissement de ses composants.

Cybernétique Une infrastructure a une dépendance cybernétique si son état dépend d'informations transmises via une infrastructure informatique. Du fait du processus d'informatisation et d'automatisation des infrastructures lors des dernières décennies, la quasi-totalité, si ce n'est la totalité de celles-ci ont une dépendance cybernétique.

Géographique Des infrastructures sont géographiquement interdépendantes si un événement local, tel qu'un incendie, un tremblement de terre, peux créer un changement d'état dans elles. Ici, l'interdépendance peux concerner plus que deux infrastructures.

Logique Deux infrastructures sont interdépendantes de manière logique si l'état de chacune dépend de l'état de l'autre par des procédés autres que physique, cybernétique ou logiques. En général, ce type d'interdépendance implique des décisions humaines. Par exemple, les autoroutes pendant les vacances seront moins surchargées lorsque le prix des carburants sera plus élevé [RPK01].

Toujours dans le même article [RPK01], il est définit quatre caractérisations du couplage entre les infrastructures : fort ou faible, ordre du couplage, linéaire ou complexe et adaptatif ou inflexible :

fort ou faible : un fort couplage correspond à une infrastructure hautement dépendante d'une autre. Les défaillances ont alors tendances à se propager rapidement via et à travers les infrastructures couplées. Par exemple un générateur à gaz sans stockage local est fortement couplé à l'infrastructure d'acheminement du gaz. Tandis qu'une centrale nucléaire est faiblement couplée à l'infrastructure de transport pour son acheminement en combustible car elle peut fonctionner plusieurs mois sans nouveau combustible.

ordre : l'ordre de couplage indique si les deux infrastructures sont directement connectées ou indirectement via une ou plusieurs autres infrastructures. Un couplage du premier ordre correspond à une liaison directe, celui du second ordre avec un intermédiaire et ainsi de suite.

linéaire ou complexe : les interactions linéaires sont celles que l'on attend par conception. C'est une définition plus large que la définition mathématique de linéaire. Tandis que les interactions considérées comme complexes sont celles qui ne sont pas prévues ou attendues, pas directement visible ou pas immédiatement compréhensibles. Par conséquent, ces dernières sont les plus difficiles à détecter.

adaptatif ou inflexible : un couplage adaptif définit la capacité du système à apprendre du passé et ainsi s'adapter aux situations futures. À l'opposé, un système avec un couplage inflexible restera rigide, c'est-à-dire qu'il gardera toujours le même comportement quelque soit les expériences passées.

I.2.c Défaillance

Une défaillance d'un système correspond à un défaut, c'est-à-dire une imperfection ou une absence d'une partie ou de la totalité du fonctionnement attendu de ce système.

Pour cette étude, trois types de défaillances multi-infrastructure peuvent être distinguées :

en cascade : une défaillance en *provoque* une autre. Autrement appelée défaillance en escalade ou effet dominos,

en aggravation : l'*interaction* entre deux infrastructures provoque une augmentation de la sévérité et de l'indisponibilité,

de mode commun : défaillances simultanées de plusieurs éléments ayant une cause externe *identique*, souvent de nature géographique et exogène.

I.2.d Sécurisation

D'après les dictionnaires actuels de langue française, la sécurisation est tout simplement l'action de sécuriser. Le problème est que ensuite, sécuriser est définit comme un terme de psychologie signifiant donner un sentiment de sécurité. Cette définition ne convient pas exactement pour les infrastructures critiques où l'on ne souhaite pas avoir un sentiment de sécurité, mais réellement plus de sécurité. On considère alors que la sécurisation d'un système consiste à éviter les défaillances du système les plus fréquentes ou les plus inacceptables, les diagnostiquer et effectuer les opérations de réparations. C'est donc l'ensemble des opérations de défense limitant les défaillances ou contribuant à ce qu'elles ne causent pas de problème, c'est-à-dire rendant le système plus sûr.

I.2.e Vulnérabilité

Selon la huitième édition du dictionnaire de l'académie française, un système qui est vulnérable est un système qui peut être attaqué. Vulnérable venant du latin *vulnerare*, blesser, qui vient de *vulnus*, blessure d'après le Littré. Les vulnérabilités sont donc les faiblesses permettant cette attaque pouvant mener ensuite à une défaillance.

I.3 Exemples d'interdépendances

Pour illustrer les définitions données dans la section précédente, en particulier les différents type de défaillances, et également bien situer le cadre de la suite de cette étude, cinq événements récents sont présentés par ordre chronologiques. Ces différents exemples d'interdépendances entre infrastructures critiques se sont déroulés lors des six dernières années.

25/01/2003 – Ohio Le ver Slammer s'est introduit dans le réseau informatique privé de la centrale nucléaire de Davis-Besse aux États-Unis et a désactivé le système de surveillance de la sécurité pendant près de cinq heures, en dépit que ce réseau soit normalement protégé par un pare-feu bloquant les ports utilisés par le ver pour se propager. Cette pénétration fut possible du fait de l'existence d'une ligne de connexion non officielle entre ce réseau et celui non sécurisé d'un sous-traitant, ligne

contournant alors le pare-feu. Heureusement, la centrale était hors production depuis onze mois et disposait d'un système de secours redondant analogique non touché par le ver. D'après les rapports, les informaticiens de la centrale n'avaient pas effectué une mise à jour de sécurité d'une faille MS-SQL que le ver exploite, mise à jour existant depuis six mois. Il y avait au moins un serveur Windows vulnérable sur le réseau. À seize heures le 25 janvier, les employés remarquèrent un ralentissement du réseau de la centrale et cinquante minutes plus tard, la congestion créée par les scans du ver mettait totalement hors d'usage le panneau d'affichage informatisé qui affiche les informations des différents capteurs, tels que la température du cœur et du liquide de refroidissement ou les radiations externes, informations qui nécessitent d'être suivies avec attention, même lorsque la tranche est arrêtée. Vingt-trois minutes plus tard, c'était au tour du *Plant Process Computer (PPC)* de devenir inopérant. Il fallu alors quatre heures et cinquante minutes pour remettre le panneau en fonctionnement et le PPC nécessita six heures et neuf minutes. Ici, une vulnérabilité informatique a eu comme conséquence de toucher un élément de l'infrastructure électrique, il s'agit donc de défaillances en cascade.

14/08/2003 – Est des États-Unis La panne généralisée ayant affecté la côte est des États-Unis en août 2003 (déjà évoquée dans la section I.1) a pour origine un problème informatique. En effet, à cause d'une erreur de programmation, un bogue du système de gestion de l'énergie (EMS) développé par General Electric (le logiciel XA/21) a conduit à la défaillance du système d'alarme du centre de contrôle de Akron dans l'Ohio. Ce bogue auparavant inconnu s'est déclaré suite à des évènements rares s'étant produit simultanément. Cette défaillance retarda la réponse des opérateurs aux événements qui ont conduit à la panne généralisée, alors qu'une action rapide aurait pu limiter sa propagation. En effet, les opérateurs ne savaient pas qu'ils travaillaient sans alarmes (visuelles et sonores) et qu'ils observaient depuis environ une heure des informations périmées sur leur partie du réseau. Ils n'ont pas réalisé la menace constituée par le changement de l'état du réseau électrique. Ce changement d'état était dû entre autre à un manque d'élagage des arbres sous les lignes haute tension qui provoqua trois court-circuits sur les lignes. Les images satellites figure I.1 ont été prises vingt heures avant la panne pour la première et sept heures après pour la seconde où l'on peut voir que le système électrique n'a pas encore repris son fonctionnement normal.

28/09/2003 – Italie Lors de la panne généralisée ayant touché toute l'Italie (figure I.2), une quantité de données inattendue a surchargé les moyens d'informations et de communication. Au rythme de dix secondes consacrées par alarme déclenchée, il aurait fallu plusieurs années aux opérateurs pour traiter l'ensemble des alarmes actives lors de l'écroulement du réseau. Ensuite, l'indisponibilité du réseau électrique pendant plusieurs heures a épuisé les alimentations sans interruption locales conduisant à l'indisponibilité des moyens de contrôle et de communication. Ceci a alors fortement rallongé la phase de restauration, car il a fallu commander manuellement des dispositifs qui auraient pu être contrôlés à distance. Cette situation correspond à des défaillances en aggravation.

19/08/2006 – Alabama Une surcharge du réseau de communication a provoqué l'arrêt

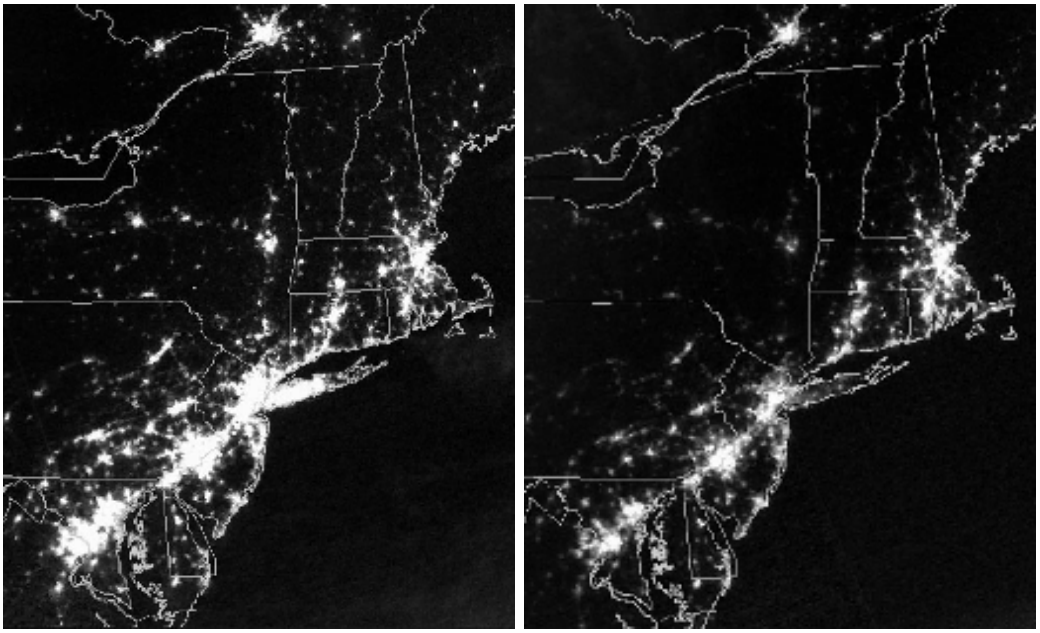

Fig. I.1 – Images satellite de la panne du 14/08/2003 (crédit NOAA/DMSP)

Fig. I.2 – Photomontage d'après *Living Earth*

de la tranche 3 de la centrale nucléaire de Browns Ferry aux États-Unis. L'origine de cet incident est un micro-contrôleur logique programmable (PLC) défectueux qui s'est mis envoyer un flot excessif de données, ce qui a provoqué le blocage de la commande de variation de vitesse de deux pompes de circulation d'eau pour le circuit de refroidissement. Par conséquent, les opérateurs ont dû préventivement arrêter manuellement le réacteur. Ainsi, un petit incident sur un réseau de communication a provoqué, suite à une chaîne d'événements, l'arrêt de production imprévu d'un gros générateur d'électricité, ce qui aurait pu provoquer d'autres conséquences plus graves sur le réseau électrique, si ce problème avait eu lieu lors d'une situation plus critique pour l'équilibre entre la production et la consommation. Cet événement est une défaillance en cascade.

04/11/2006 – Europe Des déclenchements de lignes en cascade lors de la soirée du 4 novembre 2006 ont provoqué la séparation du réseau de transport européen (UCTE) en trois zones asynchrones entre elles, comme représentées figure I.3. Les raisons de ces perturbations sont principalement le non respect du critère N-1 et une coordination entre les opérateurs des réseaux de transport insuffisante [UCT07]. Grâce à l'efficacité des mesures du plan de protection, la panne généralisée a été évitée. Néanmoins, le délestage de 5200 MW en France pendant 30 minutes (5 millions de personnes touchées) a provoqué une saturation des standards d'appels des centres de secours et un arrêt d'une dizaine de TGV en gare et sur voie. Il s'agit d'une défaillance en cascade.

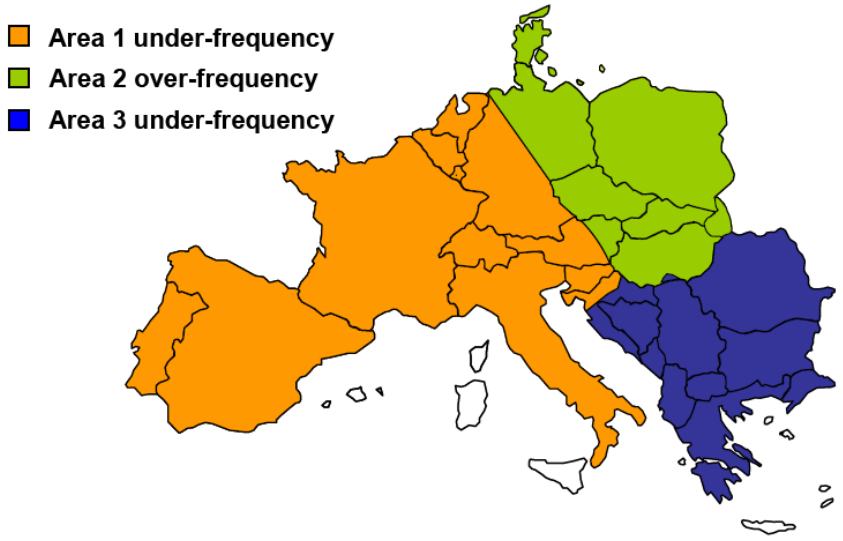

Fig. I.3 – Les trois zones asynchrones du 4 novembre 2006 (crédit UCTE)

I.4 Objectifs de la modélisation des interdépendances

Comme annoncé ci-avant, le but de cette étude est de de proposer des méthodes et outils de modélisation des infrastructures critiques couplées. L'hypothèse principale de ce travail est de se limiter à l'infrastructure électrique et son système de contrôle associé,

basé sur les technologies de l'information et de la communication.

Cette modélisation devra posséder les trois caractéristiques suivantes :

- intégration des infrastructures dans un modèle unifié,
- mise en évidence des modes communs de défaillances et des effets de cascade,
- permettre une caractérisation de la criticité ainsi qu'une recherche des points les plus faibles, qui ne sont pas nécessairement des éléments physiques.

Le premier point est nécessaire parce qu'il est important de mieux comprendre ces interactions avec une vue intégrée et globale. On est tout autant intéressé par les liens logiques, les liaisons fonctionnelles (en terme de service apporté) que par les liaisons physiques.

Au vu de la complexité du problème, différentes approches peuvent être utilisées pour modéliser les systèmes multi-infrastructures et ainsi mener à une meilleure compréhension de ces systèmes. Ainsi, dans le cadre de ce travail, deux outils scientifiques ont été utilisés. Le premier est une approche comportementale avec la réalisation d'un cosimulateur multi-infrastructures qui sera décrit au chapitre 3. Le second est une approche plus théorique avec une modélisation s'inspirant de la théorie des réseaux complexes. Celle-ci sera abordée au chapitre 4 sur un système mono-infrastructure. Puis elle sera étendue aux systèmes multi-infrastructures avec prise en considération des interdépendances et modélisation des modes communs de défaillance et des effets de cascade au chapitre 5.

Chapitre II

État de l'art de la modélisation des infrastructures critiques

Sommaire

Résumé

Différentes approches ont déjà été utilisées pour modéliser les infrastructures critiques en vue de leur sécurisation ainsi que leurs interdépendances. Parmi celles-ci, on peut citer l'utilisation des réseaux de Pétri, les graphes approvisionnement/demande, la modélisation basée sur agents, l'utilisation de bases de données, la dynamique des systèmes, les approches économiques et la simulation comportementale. Ce chapitre présente une courte introduction aux méthodes qui n'ont pas été retenues pour être explorées plus en détail dans ce mémoire de thèse et discute de leurs avantages et inconvénients.

II.1 Introduction

L'état de l'art présenté dans ce chapitre commence par un résumé de quelques rapports sur la sécurisation des infrastructures critiques. Puis, en ce qui concerne les propositions de modélisation des interdépendances, plusieurs voies déjà explorées seront présentées telles que l'utilisation des réseaux de Pétri, les graphes approvisionnement/demande et la modélisation basée sur agents. L'état de l'art concernant les deux approches utilisées dans le cadre de cette thèse sera présenté dans les chapitres correspondants.

Ces modélisations sont confrontées à de nombreuses difficultés à cause de la complexité des systèmes étudiés. Comme noté dans [RPK01], une de ces difficultés est que se contenter d'assembler des modèles existants d'infrastructures ne marche généralement pas. 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 peuvent ne pas être compatibles avec d'autres modèles. De plus, cette approche ne permet pas forcement de rendre compte du comportement émergeant des systèmes comprenant de multiples infrastructures. Une autre difficulté apparaît pour cette modélisation, il s'agit du comportement des humains interagissant avec les infrastructures, comportement que l'on peut considérer comme totalement imprévisible. Il y a également le problème de la faible probabilité d'occurrence des évènements qui nous intéressent. En effet, comme énoncé au chapitre précédent, les infrastructures étudiées marche actuellement globalement bien avec une durée de non fonctionnement ou mauvais fonctionnement très faible par rapport au temps de fonctionnement normal. Or, sécuriser les infrastructures critiques consiste justement à travailler sur ces événements exceptionnels pour les réduire en terme de durée ou d'impact de leurs conséquences. Cet aspect de faible probabilité ne doit pas être négligé. Il se pose aussi le problème de la disponibilité des données concernant les réseaux étudiés ou les incidents. En effet, pour des raisons invoquées de sécurité ou commerciales, ce type de données, quand elles existent, restent bien souvent confidentielles, et il devient alors plus difficile de travailler sur des cas représentant finement les infrastructures réelles.

II.2 Sécurisation des infrastructures critiques

Le rapport de la commission du président (américain) sur la protection des infrastructures critiques américaine [Mea97] présente ses travaux sur le sujet et en particulier la dépendance envers l'infrastructure d'information et de communication et l'exposition de toutes les infrastructure à ces nouvelles vulnérabilités et menaces liées à cette dimension cybernétique.

L'article [Dac04], présente une étude datant de mars 2004 pour le *United States General Accounting Office* présentant une analyse de la vulnérabilité des systèmes de contrôle (SCADA) aux cyber-attaques. Les systèmes de contrôle doivent faire face à un risque plus important pour plusieurs raisons : ils utilisent des technologies standards avec des vulnérabilités connues, ils sont connectés à d'autres réseaux comme le réseau d'entreprise lui-même connecté à Internet, il existe souvent des liens non sécurisés ouverts pour le diagnostic et la maintenance ou des connexions sans fils et des informations sensibles sur les infrastructures et ces systèmes de contrôle sont souvent publiquement disponibles. En particulier par rapport à ce dernier point, il est facile de se procurer le manuel contenant le

mot de passe par défaut de l'équipement et il arrive malheureusement que ce mot de passe ne soit jamais changé. De plus, il existe une menace cybernétique concernant les systèmes de contrôle car ils peuvent être vulnérables aux cyber-attaques. Ainsi plusieurs de ces cyber-attaques sur des systèmes de contrôle ont déjà été rapportées comme par exemple l'infection du réseau informatique privé d'une centrale nucléaire par le ver Slammer décrite dans le chapitre précédent. Ce type d'attaques comprend la perturbation du fonctionnement des systèmes de contrôle en retardant ou bloquant les informations transitant dans les liens de communication, le changement de paramètres non autorisé sur les différents équipements ou l'envoi de fausses informations. Pour finir, la sécurisation de ces systèmes de contrôle pose de nombreux défis. L'un d'eux est le manque de technologies de sécurité spécialisées pour ces systèmes qui sont développés dans une optique de disponibilité temps réel et non dans une optique de cyber-sécurité. Un autre défi est la non perception de la justification économique de cette sécurisation car elle se fait à un coût élevé. Un troisième étant les conflits organisationnels de coordination entre le personnel de la sécurité informatique et les opérateurs de ce système de contrôle qui sont généralement des groupes de travail différents au sein d'une même entreprise.

Dans [RD06], une étude portant sur la modélisation et la simulation des infrastructures critiques interdépendantes décrit différentes méthodes utilisées dans ce domaine comme les graphes approvisionnement/demande, le modèle entrées/sorties généralisé de Leontief, un simulateur temps réel MITS (*Multiple Infrastructures Tokens Simulator*) [MHVJ06], les réseaux de Pétri, la modélisation basée sur agent et la théorie des jeux.

L'article [Mas02] adresse également le problème de la compréhension des interdépendances entre les infrastructures. En particulier, une définition des interdépendances strictement basée sur les défaillances est proposée. Les interdépendances ne sont alors pas associées à tous les types d'interactions qui peuvent exister entre deux systèmes mais seulement associées aux interconnexions qui peuvent provoquer des défaillances. Sont également détaillés la dépendance de l'infrastructure électrique envers les systèmes de télécommunications et les concepts de dépendances, vulnérabilité et d'imprévisibilité.

II.3 Modélisation par réseaux de Petri

Un outil quelquefois utilisé pour modéliser les interdépendances des infrastructures est le réseau de Petri ([DA89]), créés par le mathématicien allemand Carl Adam Petri lors de la seconde moitié du vingtième siècle. Ceux-ci sont des graphes constitués de places et de transitions reliées entre elles par des arcs orientés. Un arc relie une place à une transition ou une transition à une place : il y a toujours une alternance entre les arcs et les places. Chaque place peut contenir des jetons ou marques. La position des jetons dans les places décrit l'état du système modélisé par le réseau de Petri. Les jetons se déplacent de place en place en suivant les arcs lorsque la transition associée est active. L'évolution des jetons décrit donc l'évolution de l'état du système. Un exemple simple de réseau de Petri contenant deux places, deux transitions et un jeton est représenté figure II.1. La matrice d'incidence d'un réseau de Petri est une matrice dont chaque ligne est associée à une place P_i et chaque colonne à une transition T_j. La taille de la matrice d'incidence indique donc le nombre de places et de transition du réseau de Petri auquel elle est associée. L'élément w_{ij} de la matrice d'incidence W vaut $+1$ si T_j est une transition de sortie de P_i, vaut moins -1

si T_j est une transition d'entrée de P_i et vaut 0 si P_i et T_j ne sont pas connectées entre eux par un arc orienté. Les invariants des réseaux de Petri permettent de caractériser certaines de leurs propriétés. Il en existe de différents types comme la composante conservative ou la composante répétitive. La première signifie que le système est dans un seul état à la fois (s'il y a toujours un et un seul jeton) ou que le nombre de jetons se conserve. La seconde indique qu'une succession de franchissement de transition ramène à l'état initial et donc qu'elle peut se répéter.

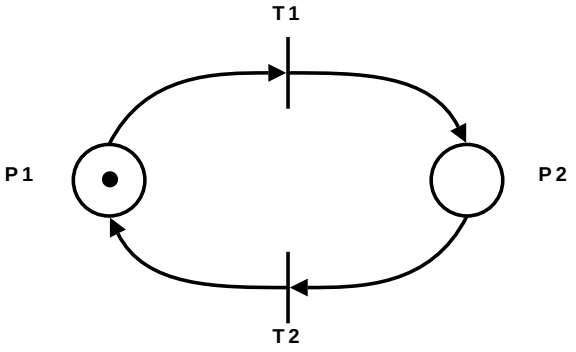

Fig. II.1 – Exemple de réseau de Petri

Une proposition de cette utilisation est présentée dans [GD03]. Les auteurs ont conçu un modèle d'interdépendance des infrastructures par réseau de Petri présenté figure II.2. Ils utilisent ensuite une approche analytique basée sur la matrice d'incidence (de taille 23×33 pour leur modèle) et sur les invariants de place afin d'identifier les relations et les interdépendances entre les infrastructures. Il y a 23 transitions et 33 places pour la modélisation de 6 infrastructures, ce qui donne environ 5 places par infrastructure. Autrement dit, cette approche reste de haut niveau et ne semble pas adaptée à une modélisation plus fine du comportement de chaque réseau.

Dans [KO03], une modélisation est proposée pour identifier et analyser les défauts de mode commun en utilisant les « réseaux de Petri stochastiques généralisés » (GPSN). Ceux-ci sont une extension des réseaux de Petri. Ils ajoutent, entre autre, un type de transition supplémentaire à la transition immédiate : la transition temporisée. Un autre ajout est la multiplicité des arcs qui a comme conséquence de ne pas avoir un nombre de jetons fixes. Ce type de modélisation permet aux auteurs de représenter des défaillances dues aux interdépendances et de les quantifier. Ils reconnaissent que leur modèle possède des limites. Cependant, ils considèrent qu'il dépasse les modèles d'arbres de défaillance traditionnels du fait de la prise en compte explicite des défaillances de mode commun.

Dans [CLDG07], est proposé un cadre de modélisation pour l'analyse des interdépendances dans les systèmes électriques. Deux infrastructures sont considérées : l'infrastructure électrique avec la génération et le transport de l'énergie jusqu'au client final et le système de contrôle basé sur les technologies de l'information dont le but est de contrôler les paramètres physiques de la première infrastructure ainsi que d'effectuer des reconfigurations en situation d'urgence. Ce travail a été réalisé dans le cadre du projet européen CRUTIAL qui entreprend l'analyse et la gestion des interdépendances et du risque opérationnel résultant. Les états de l'infrastructure électrique sont représentés de façon hybride (c'est-à-dire avec des variables continues pour les tensions, fréquences, courants, puissances

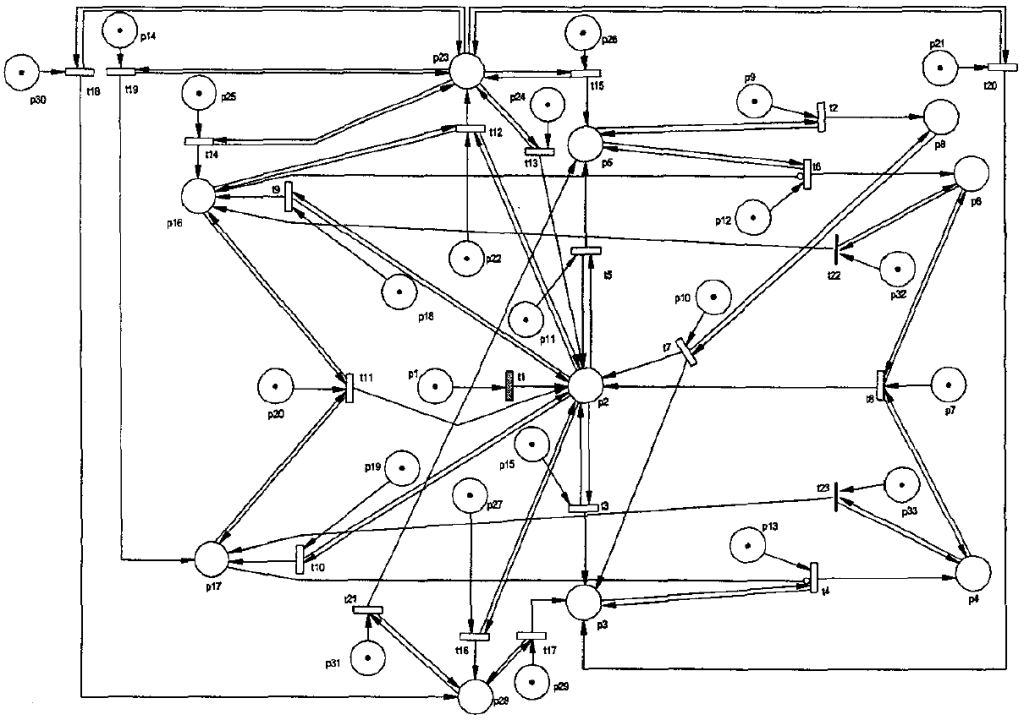

FIG. II.2 – Réseau de Petri des interdépendances entre infrastructures
Reproduite avec l'autorisation des auteurs [GD03]

actives et réactives et des variables discrètes pour sa topologie) et ceux de l'infrastructure de contrôle de façon discrète (fonctionne, en défaut, quelques erreurs ou autres). Une mise en œuvre dans un outil existant multi-formalisme basé sur une généralisation des réseaux de Petri stochastiques a été réalisée afin d'étudier la faisabilité de cette approche. Dans le cadre du même projet européen, l'article [LKK07] s'intéresse aux mêmes infrastructures et propose une modélisation des défaillances en cascade, en aggravation et de mode commun et prenant également en considération les attaques sur l'infrastructure d'information. Cette modélisation est basée sur des automates à état qui sont ensuite transformés en réseau de Petri.

D'une manière générale, l'approche par réseau de Pétri ou dérivés (tels que les réseaux de Pétri stochastiques généralisés) possède l'inconvénient de pouvoir mener à des graphes non triviaux pour des systèmes simples. Ainsi dans l'article [SLP06], où est présentée une méthode basée sur les réseaux de Pétri pour analyser les interactions entre les réseaux électrique et de communication, une simple ligne avec deux organes de coupure et un centre de contrôle est représenté par un réseau de Pétri comprenant 17 places et 23 transitions. Le réseau résultant est représenté figure II.3. Cette approche semble par conséquent difficilement applicable à l'infrastructure électrique dans son ensemble et les moyens de communication et d'information associés à l'échelle nationale ou continentale. Ce type de modélisation parait donc très mal généralisable à des systèmes beaucoup plus complexes.

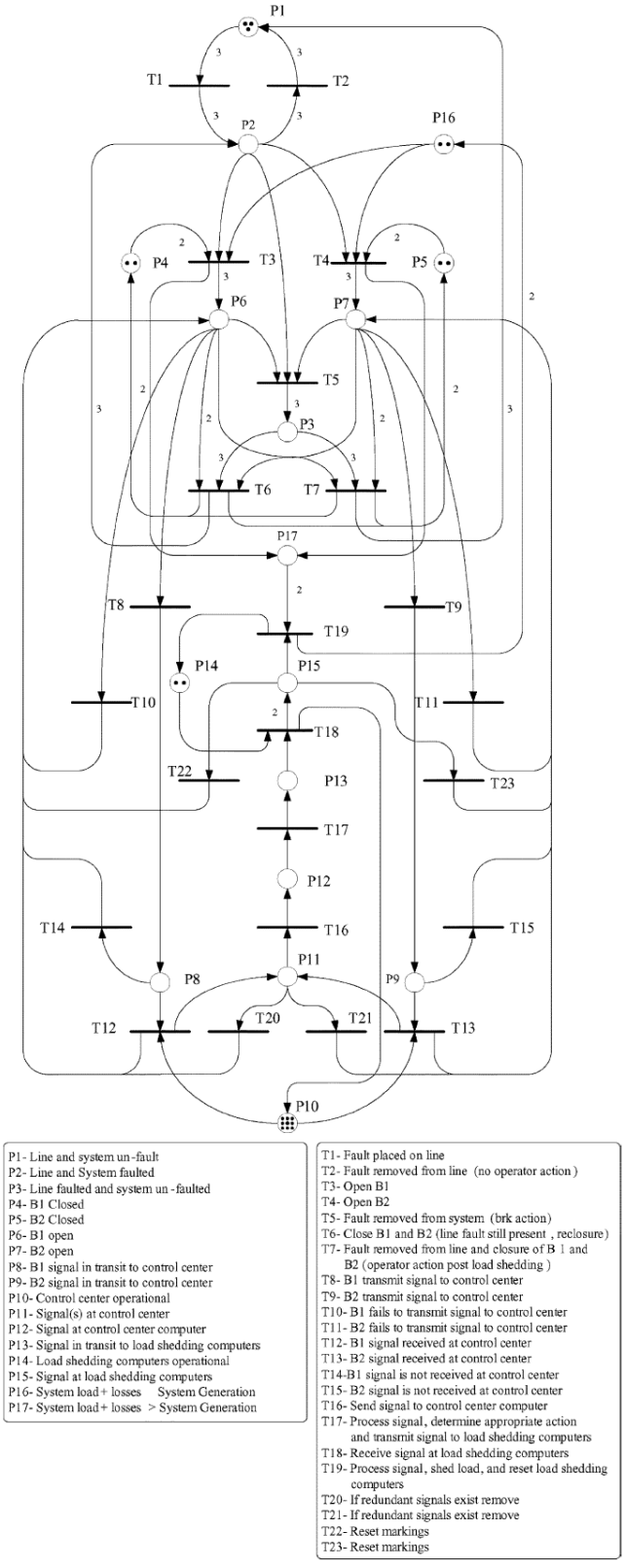

Fig. II.3 – Réseau de Petri d'un système de protection de Hydro-Québec
Reproduite avec l'autorisation des auteurs [SLP06]

II.4 Modélisation par graphes approvisionnement/demande

Une autre voie abordée dans la littérature est celle de la modélisation par graphes approvisionnement/demande (*supply-demand graphs*). Chaque infrastructure est représentée par un ensemble de nœuds et d'arcs et un flux (d'énergie, de communications ou autre) qui circule de nœud en nœud en passant par les arcs. Trois types de nœuds différents sont définis : nœuds d'approvisionnement, nœuds de demande et nœuds de transbordement qui ne produisent, ni ne consomment mais par lesquels le flux passe. Les arcs peuvent être définis avec une capacité limitée, mais pas nécessairement.

Ainsi, on trouve une utilisation de cette approche dans [LMMW03], reprise dans [LMW07]. Les auteurs s'intéressent particulièrement aux interdépendances qualifiés de géographiques et physiques au chapitre précédent. L'objectif est d'améliorer la restauration des services après une panne touchant les infrastructures critiques. L'exemple illustrant ce modèle est l'attaque du *World Trade Center* en 2001 et la phase de restauration de l'état normal. Des algorithmes ont été développés afin d'aider à la décision pendant cette dernière phase.

Dans [LMW04], il y a une identification des vulnérabilités des infrastructures actuelles et une proposition de nouvelles méthodes systématiques de conception prenant en compte les interdépendances. Cette démarche est également basée sur les graphes approvisionnement/demande. Ceci est réalisé afin d'améliorer la fiabilité des infrastructures critiques. Pour illustrer leur méthodologie, les auteurs adressent le problème d'un lien redondant pour une ligne de télécommunication, mais les deux partageant la même source d'alimentation électrique. Si cette source se trouve hors service, alors dans ce cas les deux liens de communication, du fait de leur dépendance en énergie électrique vont être eux aussi hors service malgré la redondance (qui est néanmoins utile envers un défaut ne touchant qu'un des liens). Les figures II.4 montrent cette redondance de lignes de communication (en trait mixte) entre les lieux A et B sans vulnérabilité due à l'infrastructure électrique pour l'image de gauche et avec une vulnérabilité due à l'utilisation d'une même source d'alimentation électrique (triangle) pour l'image de droite. L'algorithme proposé permet d'identifier et d'évaluer ces vulnérabilités dues aux interdépendances physiques, sans proposer de solutions alternatives pour les éviter. Les parades sont du ressort de l'ingénieur.

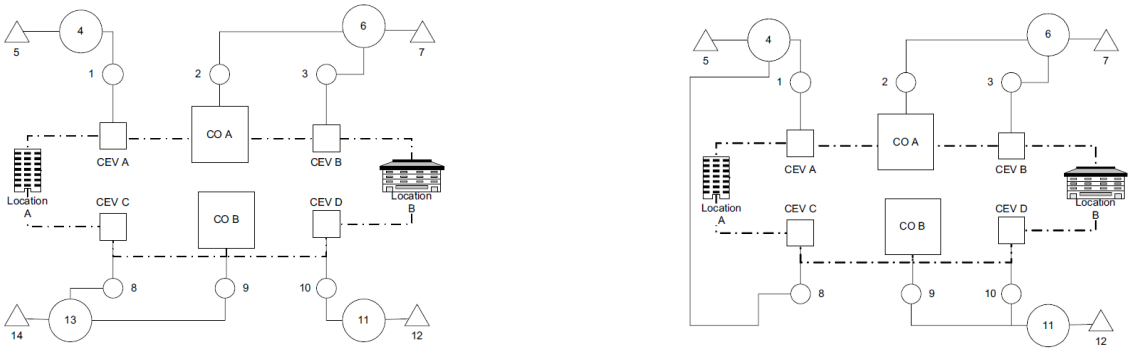

Fig. II.4 – Exemples de graphes approvisionnement/demande sans (à gauche) et avec (à droite) des vulnérabilités dues aux interdépendances
Reproduite avec l'autorisation des auteurs [LMW04]

Le principal problème de ce type de méthode de modélisation est qu'elle est de haut niveau et, par conséquent, généralement peu précise ou, si on rentre plus dans des cas d'utilisation fortement détaillés, la taille devient vite problématique et elle peut donc être applicable que à une zone restreinte.

II.5 Modélisation basée sur agents

Une troisième approche est celle de la modélisation basée sur agents dite ABM (*Agent-Based Modelisation*). C'est une technique de modélisation en vue de la simulation nécessairement informatique dans ce cas [MS99], on parle alors de ABS (*Agent-Based Simulation* ou ABM&S (*Agent-Based Modelisation and Simulation*). Cette approche de modélisation a tout d'abord été très utilisée en sciences sociales [Bon02] et en écologie [Gri99] où elle fut habituellement appelée *Individual-Based Modelisation* (IBM). C'est une approche intrinsèquement distribuée, de bas en haut (*bottom-up*), utilisant une société d'agents intelligents connectés entre eux. La définition d'un agent est variable selon les domaines et les auteurs. Néanmoins, il se dégage des différentes définitions une plus précise. « Un agent est un système autonome (logiciel et/ou matériel) qui est situé dans un environnement (contenant d'autres agents) et qui agit dessus afin de poursuivre ses propres objectifs ». On part d'une approche du bas vers le haut, du comportement relativement simple de différents composants de bas niveau et on les laisse coopérer. Le comportement complexe et de haut niveau émergeant de cette coopération apparaît alors de lui même au cours de la simulation. Cette approche possède différents avantages par rapport aux techniques de modélisation classiques comme explicités dans [BS00] et [MN05]. 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 troisième 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. Pour simplifier, les trois mots clefs de l'ABM sont objet, émergence et complexité.

Cette méthode est très utilisée pour l'étude des systèmes adaptatifs complexes, les CAS (*Complex Adaptative System*). On peut brièvement définir un CAS comme un ensemble où la coopération des différents composants conduit à un ensemble supérieur à la somme de ses parties prises individuellement. C'est ce que l'on appelle « comportement émergeant ». Or, dans [RPK01], les infrastructures critiques sont définies comme des « systèmes adaptatifs complexes ». Dès lors, elles peuvent donc être traitées par la modélisation basée sur agents.

Ainsi, dans [HWG+06] est décrit le développement d'un environnement de simulation distribué des réseaux électriques et de communication fondé sur la simulation basée sur agents. Les articles [PSU04] et [PSU05] décrivent une modélisation et simulation basée sur agent pour les infrastructures critiques interdépendantes. Cette modélisation est illustrée dans la figure II.5. Cette méthode est également proposée dans [RVD06] comme contrôle décentralisé du réseau électrique ainsi que pour la modélisation et la simulation

des interdépendances. Dans [TWR+04], il y a une utilisation d'*Intelligent Software Agents* pour l'intégration, la modélisation et la simulation des infrastructures critiques, tandis que [ZPF03] utilise un modèle de la théorie des jeux et de la simulation basée sur agents pour la modélisation des infrastructures critiques. Une méthodologie pour étudier les interdépendances dans les infrastructures critiques avec une mise en œuvre d'ABM&S est proposée dans [CGT07] sur un exemple simple du système d'information pour la gestion des urgences.

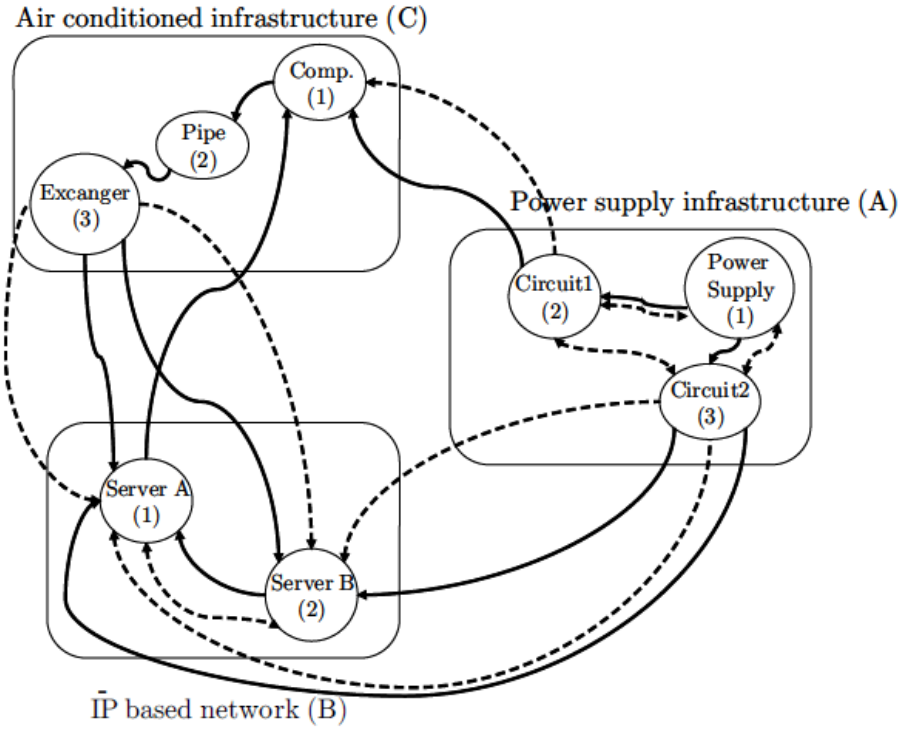

FIG. II.5 – Exemple de modèle basé sur agents d'infrastructures interdépendantes
Reproduite avec l'autorisation des auteurs [PSU05]

Cette méthode semble vraiment très intéressante pour modéliser les infrastructures composées d'acteurs ayant chacun ses objectifs propres. Cependant, on a décidé de restreindre cette étude à l'infrastructure électrique et au système de contrôle associé basé sur les technologies d'information et de communication. Ces infrastructures sont constituées de différents éléments concourant à la réalisation d'un but commun qui est d'alimenter les clients finals en énergie électrique. Il n'y a donc pas d'acteurs indépendants ayant leurs objectifs propres. Par conséquent, quoique prometteuse et initialement étudiée dans le cadre de cette thèse, cette approche n'a finalement pas été retenue pour être présentée plus en détail dans ce mémoire de thèse.

II.6 Autres modélisations utilisées

D'autres concepts apparaissent également dans la littérature tels que l'utilisation de techniques de réseaux sociaux et de modélisation de fiabilité pour la modélisation des

cyber-interdépendances des infrastructures critiques dans le programme de recherche présenté dans [KBB05]. Ce programme de recherche comporte trois objectifs : modéliser les cyber-interdépendances entre les infrastructures critiques, les simuler et concevoir des mécanismes de partage d'information pour leur protection. La modélisation est envisagée sous forme de réseaux en commençant par l'Internet et l'infrastructure financière. La simulation serait l'étude de scénarios de type quoi si comme par exemple « que se passe-t-il lorsqu'un réseau des distributeurs automatiques de billets tombe en panne ? » La conception envisagée est un protocole Internet, non pas pour les basses couches, mais de haut niveau.

Il y a aussi la modélisation et simulation des infrastructures critiques basées sur un Système d'Information Géographique (GIS) présenté dans [Wol05]. Cette approche est également utilisée dans [JW08], mais pour modéliser les interdépendances, une approche bayesienne est utilisée. Ce type de modélisation est intéressant lorsque l'on s'intéresse seulement à une zone bien définie et que l'on dispose de données précises sur l'ensemble des infrastructures présentes. Mais, elle devient difficilement applicable à l'échelle continentale, qui est l'échelle actuelle des réseaux électriques synchrones.

L'article [Zim04] présente l'utilisation d'une base de données sur les incidents affectant les infrastructures critiques pour mettre en valeur leurs vulnérabilités et leurs interdépendances. Cette approche est utile pour identifier les vulnérabilités les plus récurrentes ou dommageables et tâcher de les réduire, mais ne permet pas d'identifier les vulnérabilités, a priori, lors de la conception et l'évolution des infrastructures.

L'utilisation d'un modèle de *system dynamics* (dynamique des systèmes) d'une panne généralisée avec ses effets de cascade sur l'infrastructure de télécommunication qui elle même cascade sur l'infrastructure des services d'urgence est décrite dans [OUCB05] et [ORK07], comme illustré sur la figure II.6. Le premier effet de cascade vient de plusieurs points :

- les téléphones sans fils ont besoin d'alimentation électrique pour pouvoir fonctionner,
- il existe de plus en plus de foyer avec seulement des téléphones cellulaire. Si la panne électrique dure suffisamment longtemps, les antennes peuvent ne plus fonctionner et les batteries des téléphones s'épuisent,
- les services de téléphonie sur IP (VoIP) nécessitent un modem fonctionnel, ce qui peut ne pas être le cas en l'absence d'alimentation sans interruption individuelle.

La deuxième cascade, par ses effets dus à la non intervention des services d'urgences (pompiers, ambulances ou police), peut être à l'origine d'aggravation de blessures ou même de décès.

Fig. II.6 – Cascade à travers les infrastructures

Dans l'article [Per07], une modélisation des infrastructures critiques est couplée avec un algorithme génétique. Cette modélisation est effectuée dans un but de planification d'infrastructure. Les algorithmes génétiques sont des méthodes d'optimisation méta-heuristique,

c'est-à-dire des méthodes pouvant s'appliquer à différents problèmes non-linéaires pouvant donner rapidement une solution approximative (qui n'est pas nécessairement l'optimum global). Ces méthodes sont non-déterministes, c'est-à-dire que deux exécutions de l'algorithme avec les mêmes paramètres ne donneront pas obligatoirement le même résultat du fait de l'utilisation de fonctions aléatoires. Le principe de ces algorithme est inspiré de la théorie de l'évolution de Darwin. Dans le cas de cet article, l'optimum désiré correspond au minimum des conséquences dommageables (en pratique le coût des conséquences directes et indirectes). L'algorithme permet donc de chercher les meilleurs moyens de protéger les infrastructures modélisées.

Une étude de la propagation des défaillances dans les infrastructures critiques est réalisée dans la référence [PS08]. L'approche de modélisation des conséquences des défaillances proposée utilise la théorie des ensembles flous pour quantifier les liaisons de propagation de défaillance entre les infrastructures. Les ensembles flous permettent aux auteurs de prendre en considération l'incertitude des modèles et des données. Ils sont utilisés pour quantifier à la fois l'état de chaque système, mais également la propagation des défaillances. Les auteurs présentent ensuite les résultats de simulations de scénarios comprenant des propagations de défaillances. Cette approche n'a pour l'instant été réalisée que sur un cas d'étude simple.

Il y a également des approches économiques, comme celles basées sur le modèle économique de Leontief évoquées dans [RPK01], [Rin04] et [Hel]. Ce type d'approche donne des résultats de type économiques et ne correspond donc pas à notre démarche de modélisation d'un point de vue technique.

II.7 Simulation comportementale et théorie des réseaux complexes

Deux autres approches seront décrites plus en détail par la suite du mémoire. Il s'agit de la simulation comportementale des infrastructures et l'utilisation de la théorie des réseaux complexes.

Le simulation comportementale consiste en une simulation temporelle des infrastructures étudiées. De nombreuses modélisations et simulateurs existent déjà pour chaque infrastructure. Cependant, effectuer des simulation de chaque infrastructure indépendamment les unes des autres ne correspond pas à une simulation intégrée de multiples infrastructures, en particulier toutes les interdépendances qui peuvent exister et auxquelles on s'intéresse ne sont pas considérées. Par conséquent, il est nécessaire de concevoir des modèles et un simulateur intégrant plusieurs infrastructures. Cette approche sera exposée au chapitre suivant. Une grande attention doit être aussi portée quant à la synchronisation de ces différentes simulations. De plus, suivants la dynamiques des phénomènes qui doivent être mis en évidence et traités, la cohérence des domaines de validité des modèles utilisés doit être rigoureusement choisie. Par exemple, la mise au point de parades afin d'éviter l'écroulement des réseaux (stabilité dynamique long terme, [Kun94]) nécessité une modélisation et une simulation particulière des composants du réseau électrique et des modèles compatibles à ces dynamiques pour les infrastructures de communication et de contrôle associées. Son application à la problématique étudiée sera l'objet du chapitre 3.

Une dernière approche que l'on retrouve régulièrement dans la littérature sur l'étude des grands réseaux est la théorie des réseaux complexes. C'est un domaine nouveau appliqué à de nombreuses infrastructures différentes. Son application à l'infrastructure électrique sera l'objet du chapitre 4. À partir de cette approche, une proposition de modélisation des interdépendances au sein d'un modèle intégré de plusieurs infrastructures sera alors présenté dans le chapitre 5.

Chapitre III

Cosimulateur multi-infrastructures

Sommaire

Résumé

Un outil de simulation pour systèmes multi-infrastructures est d'un grand intérêt pour améliorer la compréhension de ces systèmes et en particulier de leurs interdépendances. Il n'existe, à l'heure actuelle, que peu de simulateurs combinés permettant de les étudier et aucun accessible en dehors de leur laboratoire de conception. Face à ce constat, on a décidé de développer notre propre outil. Celui-ci est basé sur trois logiciels métier distincts ainsi qu'un procédé de communication entre-eux. Il peut fonctionner sur différents systèmes d'exploitation et est évolutif. Son utilisation sur des scénarios d'étude a permis de mettre en évidence un exemple d'interdépendance comportementale entre une infrastructure électrique et son système de conduite.

III.1 Introduction

Un cosimulateur multi-infrastructures ainsi qu'un réseau de *benchmark*, c'est-à-dire destiné à la validation de résultat a été développé, dans le cadre du stage de Master 2 Recherche de Maria Viziteu effectué de février à juin 2007 [Viz07]. Cette approche est complémentaire et transversale à l'approche théorique décrite dans les chapitres suivants. En effet, cet outil de simulation permet de confronter à l'approche théorique une approche numérique à défaut de pouvoir être réellement expérimentale. En effet, il n'est pas acceptable de provoquer une interruption de fonctionnement des infrastructures dans un objectif de compréhension et d'analyse, même dans le but louable, à terme, de leur sécurisation.

Il existe déjà quelques simulateurs multi-infrastructures utilisés dans le cadre de la recherche. Nombre d'entre eux sont développés aux États-Unis. L'étude présentée dans [PDHP06] récapitule quasiment l'ensemble des produits finis ou à l'état de projet relatifs à la simulation couplée de différentes infrastructures avant l'année 2006. Le lecteur intéressé par un état de l'art détaillé des simulateurs multi-infrastructures pourra s'y référer. Comme autre simulateur non présent dans cette étude, on peut citer également le MITS (*Multiple Infrastructures Tokens Simulator*) [MHVJ06] évoqué au chapitre précédent. L'objectif de ce simulateur est de modéliser de manière intégrée l'ensemble des réseaux de différentes infrastructures le tout dans un but de minimisation de l'ensemble des coûts de ces systèmes tout en maximisant leur efficacité à sauver des vies humaines en cas de grandes catastrophes. Chaque système est décrit à l'aide de jetons, de cellules, de nœuds et de canaux de transports.

Malheureusement, aucun des simulateurs présentés prenant en considération le réseau électrique et les infrastructures de communication et d'information n'est disponible. On a donc décidé d'en réaliser un. Le but n'étant pas non plus de refaire entièrement les modèles des différents composants de chaque infrastructure et pour des contraintes de temps et de validation des outils, ce simulateur est basé sur des outils déjà existant pour chaque infrastructure. Il s'agit donc d'un *cosimulateur* car il y a une simulation couplée (ou combinée) de plusieurs infrastructures. Dans notre cas, comme énoncé dans le premier chapitre, on ne considère que l'infrastructure électrique et le réseau de communication et le système d'information (du centre de conduite associé).

Le travail présenté dans ce chapitre a fait l'objet d'une publication au *IEEE Power and Energy Society General Meeting* en 2008 [RVC+08].

III.2 Structure du simulateur

III.2.a Infrastructure électrique

Modélisation

Le cosimulateur est conçu afin de pouvoir étudier des événements tels que les récentes pannes généralisées et, plus particulièrement, les problèmes de stabilité long terme [Kun94]. Au niveau de la simulation électrique, on s'intéresse donc plutôt à des phénomènes dont la durée caractéristique est supérieure à la seconde, mais inférieure à une journée. On ne va donc pas s'intéresser aux phénomènes électromagnétiques de l'ordre de la miliseconde ni à de la planification sur plusieurs décennies, mais à de la simulation en temps continu. Cette

simulation est basée sur l'intégration d'équations algébro-différentielles représentant les modes caractéristiques de divers composants du réseau ainsi que des automates associés. Cette résolution est typiquement réalisée grâce à la méthode des trapèzes ou une de ses variantes. Ce type de simulation est nommé *simulation à temps continu*. En effet, malgré l'échantillonnage du pas de temps de l'intégration, les variables varient de manière continue.

Logiciel

Le logiciel retenu pour la simulation de l'infrastructure électrique, compte tenu des remarques du paragraphe précédent, est PSAT, acronyme de *Power System Analysis Toolbox*[1] [Mil05b]. C'est une boite à outils Matlab fonctionnant aussi sur GNU Octave[2] [Eat02]. Il permet, entre autre, d'effectuer des simulations temporelles (*time domain simulation*), mais aussi des calculs de répartition de charge (*load-flow*), des calculs de répartition de charges optimaux (*optimal power flow*), des analyses de stabilité petits signaux (*small signal stability analysis*) et du placement optimal des synchro-phaseurs (*phasor measurement unit placement*). Des modèles existent pour, entre autres, les nœuds, les lignes, les transformateurs à deux et trois enroulements, les régleurs en charge, les générateurs, les interrupteurs, les défauts, les mesures de fréquence, les synchro-phaseurs, différents types de charge, les machines synchrones, asynchrones et à double alimentation, les régulateurs de puissance et de tension, les transformateurs déphaseurs, les admittances parallèles, les piles à combustible et le vent. Il est possible de compléter les modèles existant par de nouveaux modèles définis par l'utilisateur ou modifier les modèles existants pour les adapter à ses besoins. PSAT est multi-plateforme dans le sens où il peut fonctionner sur tous les environnements supportées par Matlab ou GNU Octave. Il est relativement facile à utiliser et surtout c'est un logiciel libre (sous licence GPL). Outre le fait que l'on peut le télécharger facilement, cela offre également la possibilité d'accéder et de modifier son code source afin d'adapter cet outil à nos besoins. Cela a été justement réalisé afin de permettre la communication inter-processus mais de la manière la moins intrusive possible. Cette réalisation n'aurait pas été possible avec un logiciel tel que Eurostag [RTEb] (développé conjointement par EDF et Tractebel) ou PSS/Netomac [Sie] (développé par Siemens). On pourra également distribuer ensuite les versions modifiées. Par contre PSAT possède l'inconvénient d'être plus lent à l'exécution que ses équivalents commerciaux écrits en C ou en Fortran, la principale raison étant qu'il est interprété sur la plate-forme Matlab et non pas compilé. Une capture d'écran de PSAT est présentée figure III.1.

Le cosimulateur fut basé d'abord sur la version 1.3.4c qui était la dernière version stable lorsque le simulateur fut construit, puis sur la version 2.1.2 lorsqu'elle est sortie, c'est-à-dire en juin 2008. Le code fut enrichi par de nouvelles fonctions telles que des courbes de de charges, des protections ampèremétriques des lignes, le délestage fréquencemétrique à plusieurs seuils et l'arrêt de générateurs à des instants donnés pour simuler une perte d'une unité de production. L'ajout de ces nouvelles fonctionnalités a été facilité par un mécanisme de PSAT permettant d'insérer des fonctions de perturbations lors des simulations temporelles, perturbations étant ici entendue au sens large.

[1] `http://www.power.uwaterloo.ca/~fmilano/psat.htm`
[2] `http://www.octave.org`

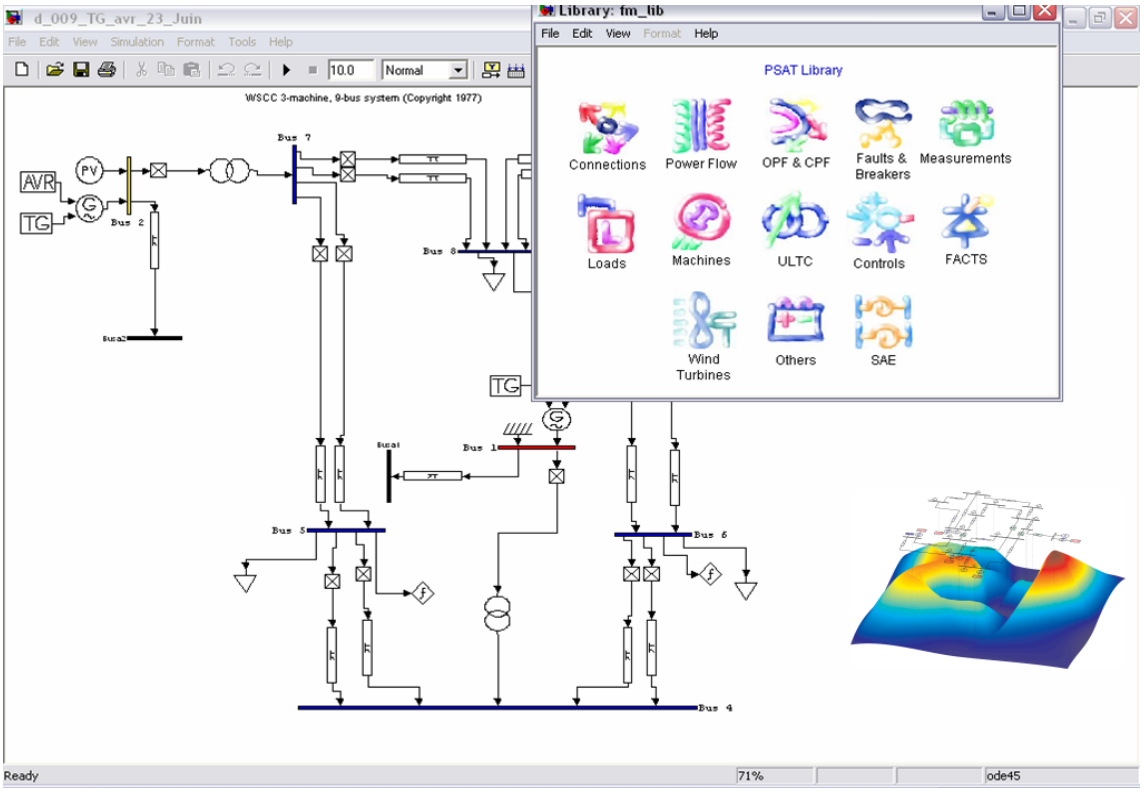

Fig. III.1 – Capture d'écran de PSAT

III.2.b Infrastructure de télécommunication

Modélisation

En ce qui concerne la simulation de l'infrastructure de télécommunication, le but est de simuler son comportement externe compatible avec les études de la stabilité long terme des réseaux, autrement dit on adopte une approche de type « boite noire ». On n'a pas pour but d'étudier le détail des différentes couches de protocoles ou de dimensionner un nouveau réseau, mais plutôt de savoir qualifier l'intégrité et le retard dans les communications. Dans ce type de simulation, il n'y a donc pas d'équations différentielles à intégrer. Les variables sont discrètes et non plus continues et les phénomènes sont décrits par des évènements, c'est ce que l'on appelle *simulation à temps discret*. On a modélisé donc les routeurs, les liens entre eux, les centrales de mesure et la partie contrôle des RTU (interrupteurs et régulateurs de puissances et de tension). Les routeurs ont comme paramètres caractéristiques la taille de leur file d'entrée (*buffer*), leur débit de sortie et ils possèdent une table de routage fixée manuellement pour aiguiller les paquets sur les liens adéquats. Les liens sont modélisés par leur latence et leur taux d'erreur. Il n'y a pas de bande passante associée spécifiquement aux liens, à la place, on fixe le débit de sortie du routeur qui limite le débit du lien de sortie correspondant. Par exemple, si un interrupteur est ouvert dans le réseau électrique à l'instant de simulation t, l'information arrive au centre de conduite comme un « événement » δ secondes plus tard en étant passée par plusieurs routeurs et liens de communication. Bien sûr, tous les appareils du réseau de communication peuvent être forcés en état de marche ou d'arrêt afin de simuler des défauts ou leur maintenance.

Il est également possible de définir des liens de secours qui sont d'autres routes utilisées lorsque le lien normal ou le routeur suivant ne fonctionne pas.

Logiciel

Les logiciels classiques de simulation des réseaux de télécommunications utilisés par les chercheurs et les ingénieurs qui les étudient en détail ont pour objectif d'effectuer des investigations sur les performances de divers protocoles ou encore de dimensionner un réseau. Étant donné qu'ils sont en général assez spécialisés et que notre besoin est en comparaison très basique, notre principal critère de choix fut la facilité d'emploi. Pour cette raison, on s'est appuyé sur un simulateur à temps discret général sur lequel on a créé des modèles de composants de télécommunication simples.

Ce logiciel est SimPy[3] qui est l'abréviation de *Simulation in Python*. La programmation se fait en langage Python[4] et en orienté-objet. C'est aussi un logiciel libre (sous licence LGPL), donc comportant les avantages cités précédemment pour le logiciel de l'infrastructure électrique. SimPy est utilisé dans des domaines aussi variés que la modélisation de propagation d'épidémies, la simulation de trafic, la planification de surveillance de l'espace aérien, les études de performance de matériel informatique, l'optimisation de processus industriels ou l'enseignement des méthodologie de simulation. SimPy possède des fonctionnalités pour effectuer des statistiques, une interface utilisateur graphique (*GUI*) et de tracés de courbes. On n'a pas utilisé ces fonctionnalités car le cosimulateur a été conçu pour que l'interaction avec l'utilisateur se fasse entièrement à partir du Matlab sous lequel tourne la simulation électrique.

SimPy est un logiciel de simulation temps discret générique. Il ne possède donc pas de modèles tout fait pour les différents composants du réseaux de communication. Ces composants ont donc dû être développés. La liste suivante les récapitule et donne aussi une brève description de leurs caractéristiques propres :

Message qui contient l'expéditeur, le destinataire, un numéro et le contenu qui peut être une **Alarme** ou une **Mesure**.

Alarme contenu d'un **Message** qui contient le composant ayant émis l'alarme, la grandeur hors limite, l'instant et le problème.

Mesure contenu d'un **Message** qui contient le **Capteur** ayant effectué la mesure, l'instant, la grandeur, sa valeur et l'unité.

Lien qui contient un nom, le composant d'arrivée, une latence et le taux d'erreur associé.

Capteur qui contient un nom, les valeurs minimales et maximales, l'écart type de son erreur de mesure et le type. Ce dernier peut être un nœud simple (mesure de la tension et de l'angle), générateur (mesure de tension, angle, puissances actives et réactives et vitesse de rotation), charge (mesure de tension, angle, puissances active et réactive et fréquence) et lignes (mesure du courant).

Centrale de mesure qui contient la liste de ses **Capteur**s, la liste des interrupteurs qu'elle gère, le nom du **Centre de conduite** auquel elle envoie les mesures collectés

[3] `http://simpy.sourceforge.net/`

[4] `http://www.python.org/`

des capteurs et les informations des interrupteurs, la période d'envoi des alarmes et la période d'envoi des mesures.

Router qui contient une file avec une taille fixée, un débit, des **Lien**s associés et une table de routage.

Centre de conduite qui contient un nom, un **Lien** de sortie pour ses messages et éventuellement un (ou des) **Lien**(s) de secours.

RTU qui contient les dispositifs pour fixer les consignes de couple et de tension du générateur associé ou commander les interrupteurs associés.

Une capture d'écran de SimPy est présentée figure III.2.

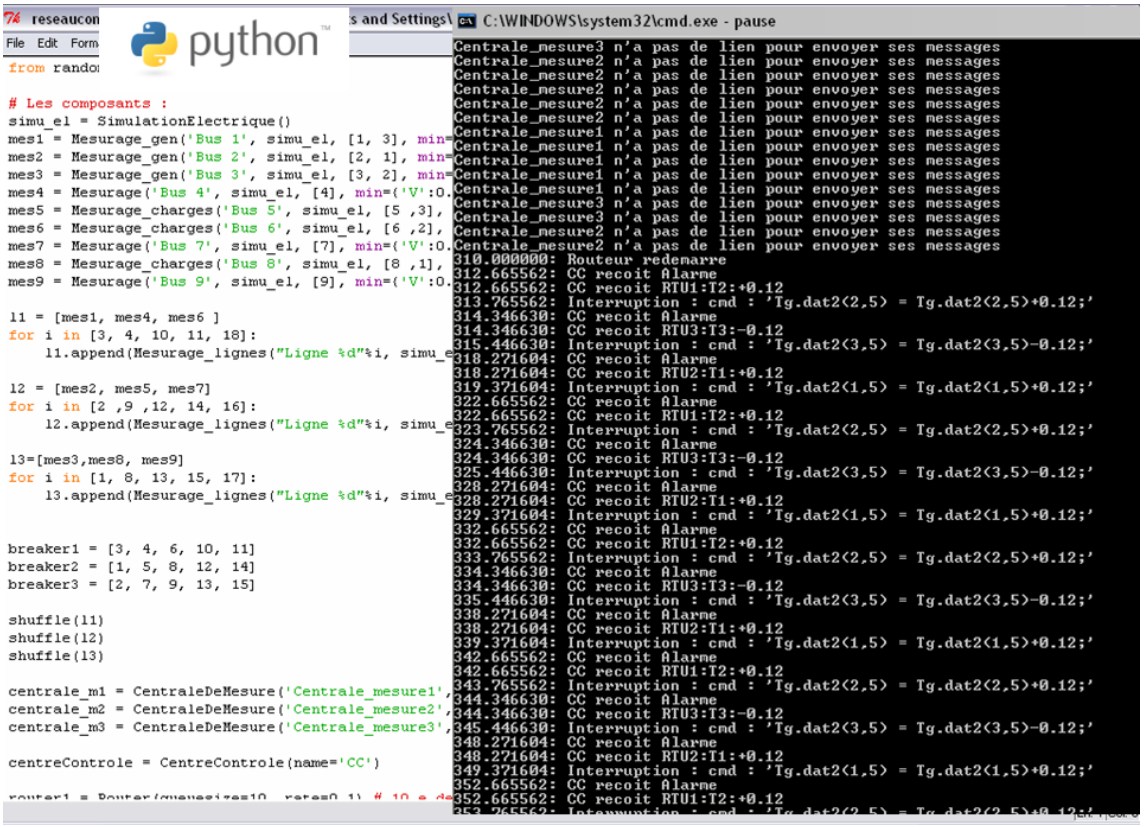

Fig. III.2 – Capture d'écran de SimPy

III.2.c Infrastructure informatique

Modélisation

En ce qui concerne le système d'information, c'est-à-dire le centre de conduite du réseau électrique, il a tout d'abord été modélisé par un système simple qui ne fait que seulement répondre par des ordres vers les RTU aux alarmes qui lui sont transmises à partir des centrales de mesures. Mais il est ensuite possible de l'améliorer en lui incorporant des fonctions plus complexes présentes dans les systèmes de gestion de l'énergie (*EMS*) telles qu'un estimateur d'état, un *optimal power flow* ou bien d'autres fonctions encore.

Logiciel

En terme de choix logiciel, la principale spécification était d'utiliser un logiciel où l'on pouvait facilement étendre les fonctionnalités en ajoutant des modules déjà développés ou en en développant de nouveaux. On a choisi le logiciel de calcul numérique Matlab. Il est important de noter que ce Matlab, bien que tournant sur le même ordinateur, est un processus différent du premier dans lequel s'exécute la simulation du réseau électrique. Cette séparation logicielle assure qu'aucune information ne pourra transiter du réseau électrique vers le centre de contrôle sans passer par l'intermédiaire du réseau de communication. Le logiciel GNU Octave peut, ici aussi, remplacer Matlab.

La mise en œuvre actuelle du centre de conduite est vraiment très simple. Elle consiste en un acquittement des mesures et une réponse aux alarmes par des actions prédéfinies pour chaque type d'alarme en fonction de sa provenance comme représenté sur le synoptique de la figure III.3.

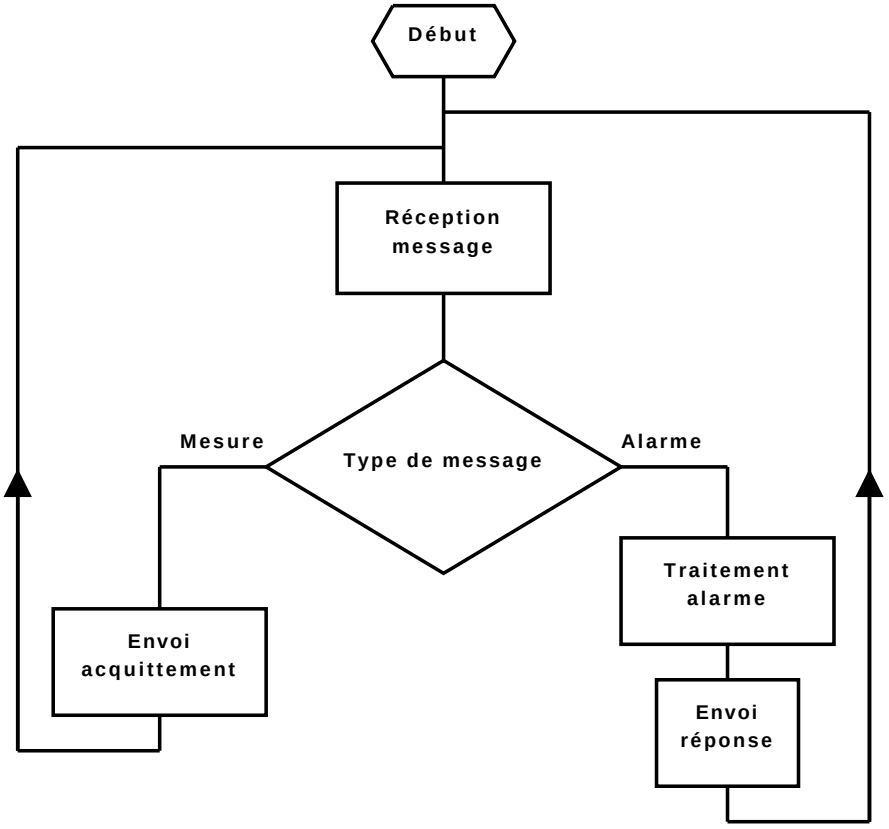

Fig. III.3 – Synoptique du centre de conduite

Une capture d'écran du centre de conduite sous Matlab est présentée figure III.4.

III.2.d Communication inter-processus

Objectifs

Dans les sections précédentes, différents outils logiciels pour la simulation de chaque infrastructure ont été présentés. Il s'agit maintenant de les faire fonctionner ensemble comme

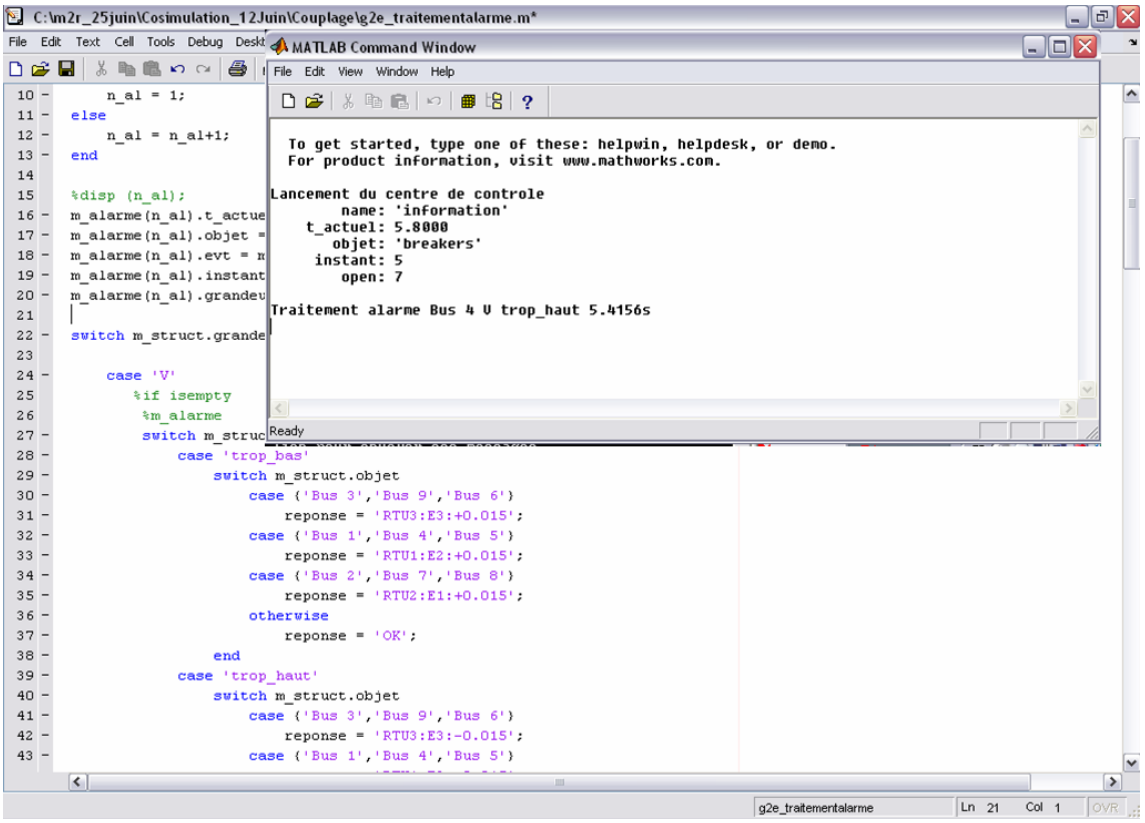

Fig. III.4 – Capture d'écran du centre de conduite sous Matlab

un seul et unique logiciel. Cette tâche est le rôle de la communication inter-processus (*IPC*). Pour construire ce logiciel intégré, une IPC basique était suffisante. Une IPC plus complexe telle que COM (*Component Object Model*) ou CORBA (*Common Object Request Broker Architecture*), qui sont présentes dans Matlab, n'était pas nécessaire. De plus, on souhaitait une mise en œuvre qui n'était pas spécifique à un système d'exploitation afin d'être indépendant de la plate-forme. Bien entendu, la mise en œuvre de l'IPC en tant que telle dépend fortement du système d'exploitation, mais il est possible de choisir un type d'IPC ayant un concept identique sur toute les plates-formes. Ainsi, le cœur de l'IPC sera très différent, mais les interfaces seront presque les mêmes pour chaque système d'exploitation.

Mise en œuvre

Le concept de « tube nommé » (*named pipe*) a été utilisé. Cette IPC est fournie par le système d'exploitation. C'est une connexion entre la sortie d'un processus et l'entrée d'un autre. Cette connexion peut aussi se faire de manière anonyme, c'est-à-dire qu'elle n'a pas de nom associé et n'existe que le temps d'existence des processus. Dans notre cas, elle est nommée et peut donc exister indépendamment des processus qui s'y connectent (sauf que sous Windows, elle est supprimée automatiquement lorsque le dernier processus la quitte). La mise en œuvre possède quelques différences en fonction du système d'exploitation : les tubes nommés sont bidirectionnels sous Windows et unidirectionnels sous système POSIX (*Portable Operating System Interface*), il en faut donc deux pour avoir un canal de communication duplex. Sur ces derniers, les tubes nommés sont également appelés

FIFO (*First In, First Out*) et sont également plus faciles à créer et à utiliser du fait qu'ils sont vus comme un fichier (suivant la philosophie d'UNIX : tout est fichier). Matlab peut gérer directement ces derniers (parce qu'ils sont considérés comme des fichiers classiques), mais pas les tubes nommés sous Windows. Néanmoins, Matlab peut exécuter des scripts Perl[5] (l'interpréteur Perl est inclus avec Matlab) qui peut gérer les tubes nommés sous Windows[6]. Pour Python, il n'y a aucune difficulté parce que les tubes sous UNIX sont accessibles en standard et ceux sous Windows avec une extension spécifique[7] [SDK+95].

Cette communication inter-processus peut avoir lieu aussi à travers un réseau informatique, en natif sous Windows ou via un système de fichier en réseau sous système compatible Unix (par exemple NFS). Les processus n'ont alors pas besoin de tourner sur la même machine. Cela permet de séparer physiquement les simulations de chaque infrastructure. Néanmoins l'intérêt est relativement réduit, car du fait de l'instruction bloquante de lecture (phénomène explicité juste après), on n'obtient pas de réduction du temps total de la simulation, mais au contraire un allongement car la communication se fait entre plusieurs machines avec des temps de latence associés et non plus sur un même ordinateur.

Fonctionnement

La communication utilisant les tubes nommés est très basique. Cela consiste juste à écrire une chaîne de caractère à une extrémité du tube pour un processus et à l'autre extrémité du tube un second processus qui attendait cette chaîne de caractère peut la lire. Un aspect important à noter est que l'action de lecture est une instruction bloquante. Cela signifie que lorsqu'un processus souhaite lire le contenu du tube, il reste bloqué sur cette instruction jusqu'à ce que un autre processus écrit dedans. Ce mécanisme a été utilisé afin de réaliser la synchronisation entre les processus. Deux liens de communications bidirectionnels sont nécessaires, un entre les réseaux électrique et de télécommunication et l'autre entre les infrastructures d'information et de télécommunication. Par conséquent, deux tubes nommés bidirectionnels sont créés sous Windows comme présenté en haut de la figure III.5 et quatre FIFO unidirectionnelles sur les systèmes POSIX (en bas de cette figure).

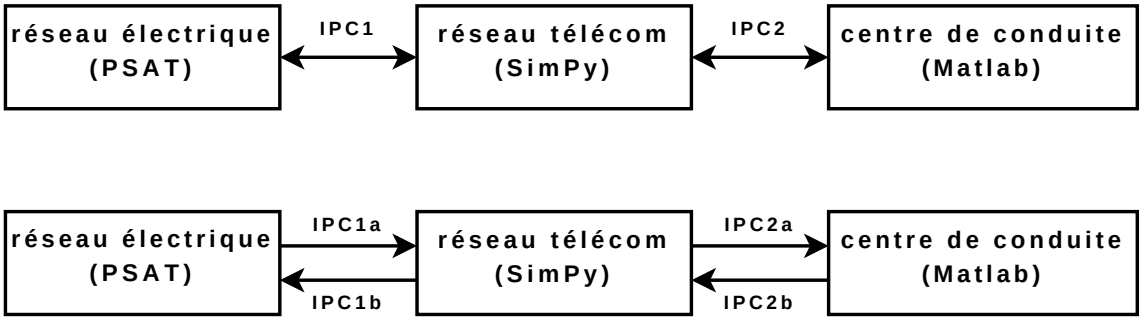

Fig. III.5 – Architecture du cosimulateur

Un médium de communication n'est pas suffisant afin d'accomplir une communication

[5] `http://www.perl.org/`
[6] `http://www.roth.net/perl/pipe/`
[7] `http://sourceforge.net/projects/pywin32/`

duplex. Il faut également définir une syntaxe des messages et un protocole de communication. La syntaxe choisie est la suivante :

- les champs sont séparés avec une virgule (,) ;
- un champ possède une clef et une donnée (qui est généralement une valeur numérique) ;
- la clef et la donnée sont séparées par un deux points (:) ;
- si une virgule est inclue dans une chaîne entre apostrophes doubles, alors ce n'est pas un symbole de séparation de champs. Ceci permet d'éviter qu'un envoi d'une virgule dans une donnée ne soit mal interprété ;
- un message se termine avec un dollar ($).

Un autre problème a été résolu. C'est celui de la synchronisation temporelle entre les logiciels et la coordination entre la simulation à temps continu et celle à temps discret.

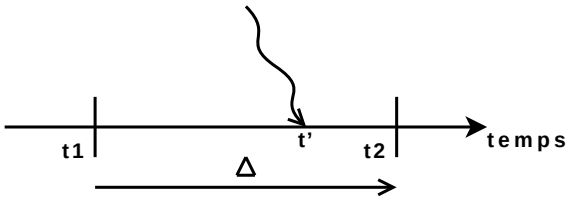

Fig. III.6 – Synchronisation temporelle

Lorsque PSAT est à l'instant t_1, il fixe le pas de temps Δ (voir figure III.6). Puis il calcule l'état du système électrique à l'instant $t_2 = t_1 + \Delta$. Afin de vérifier si Δ n'a pas été choisi trop grand, PSAT effectue une estimation de l'erreur réalisée. Si le calcul converge, alors PSAT envoie à SimPy l'ordre de simuler entre t_1 et t_2. Si rien ne s'est passé pour le réseau électrique pendant cette simulation, SimPy s'arrête à l'instant t_2 et le fait savoir à la simulation électrique. Connaissant cela, PSAT peut alors continuer en calculant un nouveau pas de temps Δ' (ou le même Δ) et ainsi de suite. Mais si SimPy a une information à transmettre au réseau électrique à l'instant t' compris entre t_1 et t_2 qui amène à une modification de ce dernier, alors il arrête sa simulation à t' et transmet cet instant à la simulation électrique. PSAT réduit alors son pas de temps Δ, effectue les changements requis (s'il y en a) et calcule l'état du système électrique à l'instant t'. Ce cycle est répété jusque atteindre l'instant final de simulation. Lorsqu'une mesure ou une alarme arrive au centre de conduite, cette donnée est transmise au simulateur correspondant et il peut ensuite transmettre des ordres de commande pour le réseau électrique. L'algorithme correspondant à cette synchronisation temporelle est présenté figure III.7.

Au final, la communication inter-processus permet d'assembler les différents logiciels afin qu'ils puissent travailler ensemble. La liaison entre PSAT, SimPy et Matlab (ou GNU Octave) a pu être réalisée avec succès. L'architecture schématisée de l'ensemble du cosimulateur multi-infrastructures est présentée figure III.5.

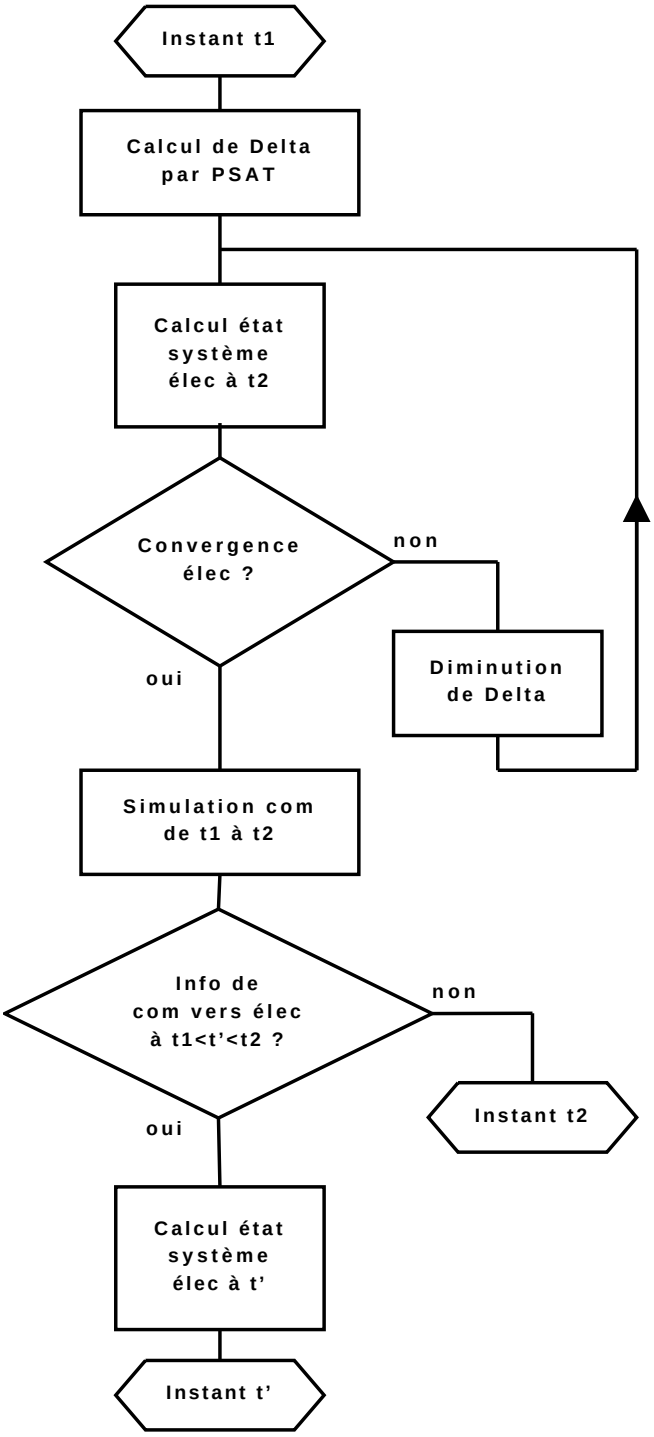

FIG. III.7 – Algorithme de la synchronisation temporelle

III.2.e Modifications ultérieures

Depuis la première version achevée après le stage de Master [Viz07], de nombreuses améliorations ont été régulièrement amenées.

Il est ainsi maintenant possible d'ajouter un bruit gaussien dont on peut régler l'écart type aux mesures effectuées par les centrales de mesures. Cela est utile si on souhaite ajouter, par exemple, un estimateur d'état au centre de contrôle.

Les logiciels composant le cosimulateur évoluant eux aussi, nous l'avons adapté à la dernière version de PSAT, c'est-à-dire à la série 2.1.X [Mil08]. Ceci est un changement majeur (le cosimulateur ayant été initialement conçu avec la version 1.3.4) car PSAT passe d'une programmation de type fonctionnel en une programmation orientée objet. Quelques fonctionnalités mineures ont été perdues. Par contre, cela permet d'être en phase avec la version maintenue de PSAT et donc de bénéficier des corrections de bogues ainsi que des dernières fonctionnalités.

III.3 Résultats

III.3.a Infrastructure d'étude

Le réseau de *benchmark* est constitué d'un réseau électrique ainsi que d'une infrastructure de télécommunication associée raccordée au centre de contrôle.

Choix du réseau électrique

La base de départ pour le réseau électrique est le réseau 9 nœuds et 3 générateurs du WSCC (*Copyright 1977*) tel que décrit dans la documentation de PSAT [Mil05a] et dont la mise en œuvre se trouve dans le répertoire `tests` de PSAT sous le nom de `d_009`. Ce réseau est représenté figure III.8.

Modifications apportées au réseau électrique

Le choix des paramètres dynamiques des machines synchrones et de leurs régulateurs primaires de vitesse et de tension (TG et AVR) ont été choisis de sorte de modéliser des générateurs thermiques aux nœuds 2 et 3 et un générateur hydraulique au nœud 1. Les lignes ont été transformées en lignes bi-ternes. Par conséquent, les paramètres individuels de chaque ligne ont été modifiés : la résistance et la réactance séries ont été multipliés par deux et la susceptance parallèle divisée par deux afin de conserver les mêmes caractéristiques globales du réseau. Chaque nœud générateur a été pourvu d'une ligne purement résistive de valeur 0.001 p.u (voir référence [Wee87] pour les p.u) connectée à un autre nœud afin de modéliser les auxiliaires sur lesquels se replie la machine synchrone lorsqu'elle se trouve îlotée du reste du réseau. Chaque ligne de transmission (donc hors transformateurs et hors lignes de modélisation des auxiliaires) a été équipée de disjoncteur la protégeant en cas de surcharge. La valeur de réglage pour l'ouverture de ces disjoncteurs est réglée à un courant $I_{\max} = 1,75$ p.u. Un disjoncteur équipe également tous les transformateurs associés aux générateurs ce qui permet de les isoler du reste du réseau. De plus, est effectuée au niveau de chaque charge une variation temporelle de la puissance apparente consommée par celle-ci selon des courbes définies par des profils différents (domestiques, industriels

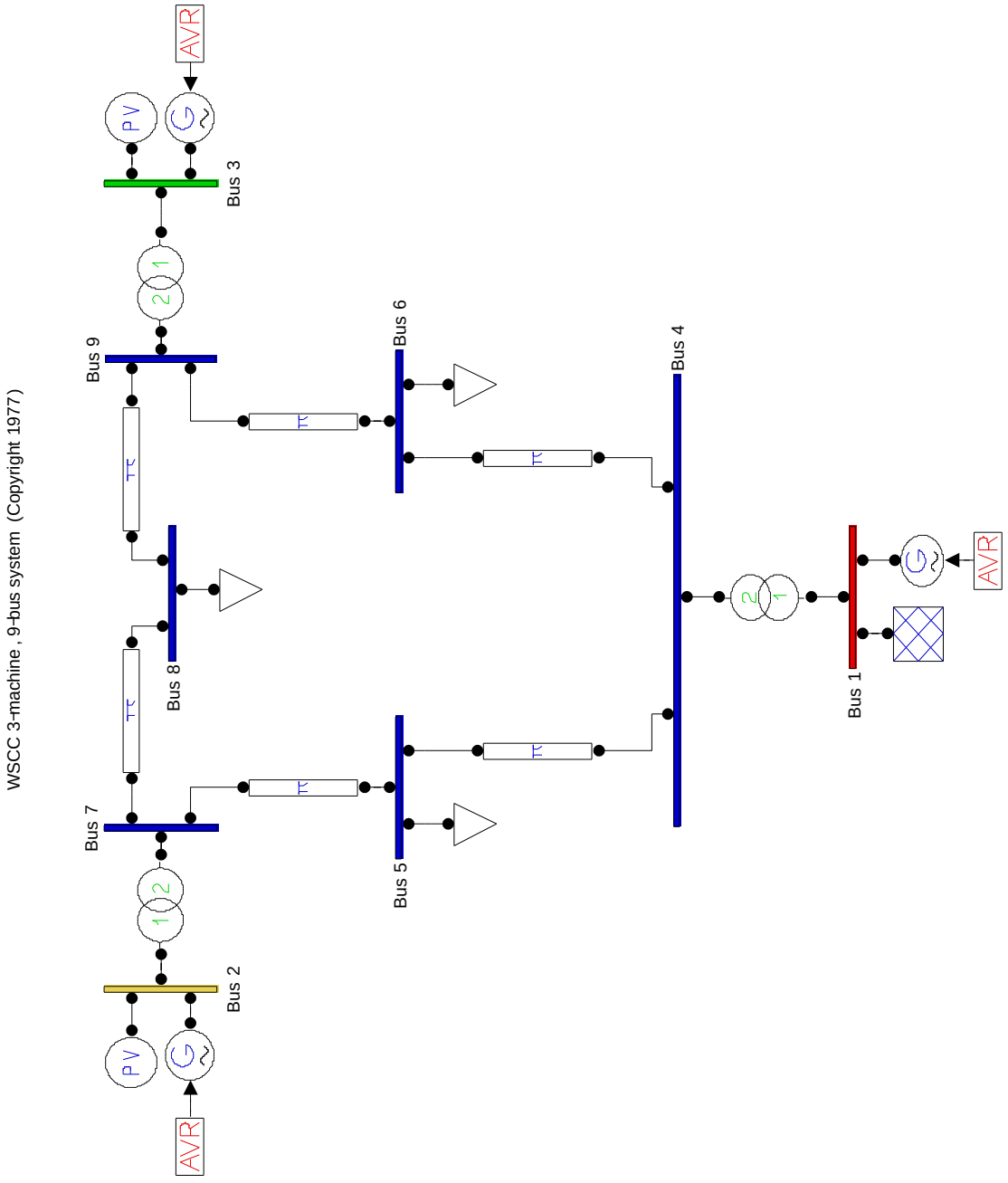

FIG. III.8 – Réseau 9 nœuds initial

et commerciales). Ces courbes de charges sont données à la figure III.10. On a également intégré un délestage des charges en cas de sous-fréquence avec un délestage de 20% pour une fréquence inférieure à 48 Hz et de 50% lorsque la fréquence devient inférieure à 47 Hz. Le réseau électrique final après ces modifications est présenté figure III.9.

Réseau de communication

Le réseau de communication est composé de quatre routeurs, trois centrales de mesures auxquels sont associés neuf capteurs. Il y a un capteur par nœud électrique, et chaque centrale de mesure en gère trois. Il y a trois capteurs de type nœud simple, trois de type nœud générateur et trois de type nœud charge. Il y a également trois RTU pour commander les interrupteurs et les générateurs. Au total, il y a dix liens de communications pour connecter ces composants entre eux. Ce réseau de communication seul est représenté figure III.11.

III.3.b Scénarios et résultats

Maintenant que le simulateur est entièrement conçu et développé, il est possible d'effectuer différentes études. Le but est de mettre en évidence des interdépendances entre les infrastructures. Les trois scénarios de simulation présentés dans cette partie ont été réalisés en utilisant le cosimulateur présenté dans les sections précédentes [Viz07].

Premier scénario

Dans ce premier scénario, tous les composants des infrastructures fonctionnent normalement. La courbe de charge totale correspond à celle de la France le 4 novembre 2006 entre 15h et 20h interpolée et ramenée à une échelle de 400 secondes. Cette compression du temps est possible si l'on s'assure que les différentes variables d'état ont atteint leur régime permanent avant toute nouvelle variation. Les vitesses de rotation ainsi que la puissance mécanique des générateurs synchrones sont représentés figure III.12. Comme tous les générateurs sont synchrones, leur vitesse de rotation est identique.

Second scénario

L'infrastructure électrique précédente fonctionne dans un état N-1 : un des trois générateurs est déconnecté du réseau au temps de simulation cinq secondes. Ce générateur se désynchronise (ω_{Syn2} est différent des autres vitesses de rotation) et accélère brutalement car il se retrouve sans charge. Son réglage primaire réagit en diminuant le couple et donc la puissance mécanique. Le centre de conduite reçoit des alarmes de sur-vitesse et diminue encore la consigne de couple afin de faire baisser la vitesse de rotation. La fréquence de ce générateur se stabilise à 51 Hz après 35 secondes. Il est alors possible de ramener cette fréquence à celle du reste du réseau pour une reconnexion ultérieure. Les deux autres générateurs compensent cette perte de production en augmentant la leur et commencent à fonctionner proches de leurs limites de puissance mécanique respectivement à 2 et 1,6 p.u. Le centre de conduite est totalement informé de l'état du système et peut traiter les alarmes en changeant les références de tension et de puissance pour les générateurs (réglage secondaire). Ainsi, il y a un ajustement de la consigne de couple des générateurs par

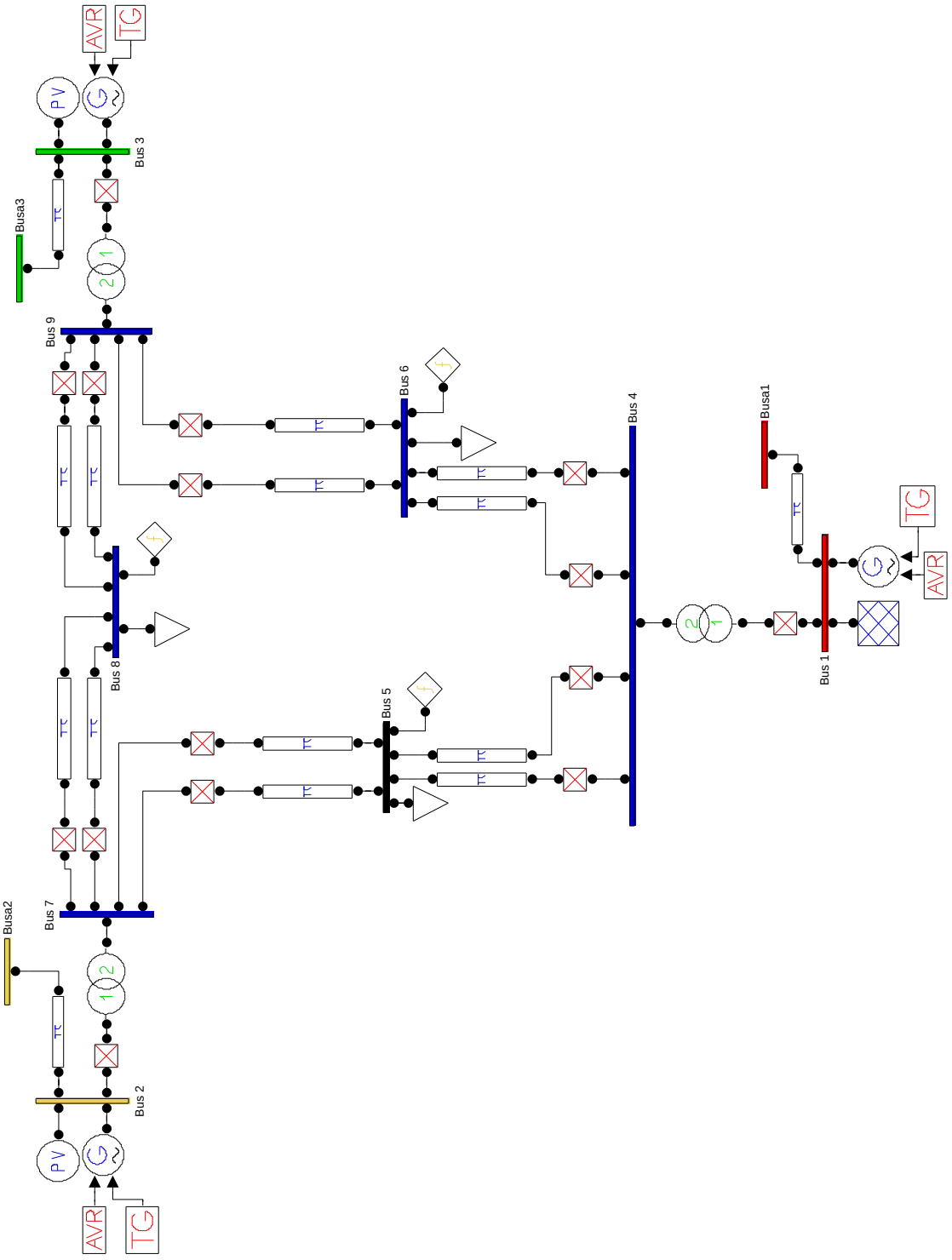

FIG. III.9 – Réseau 9 nœuds final

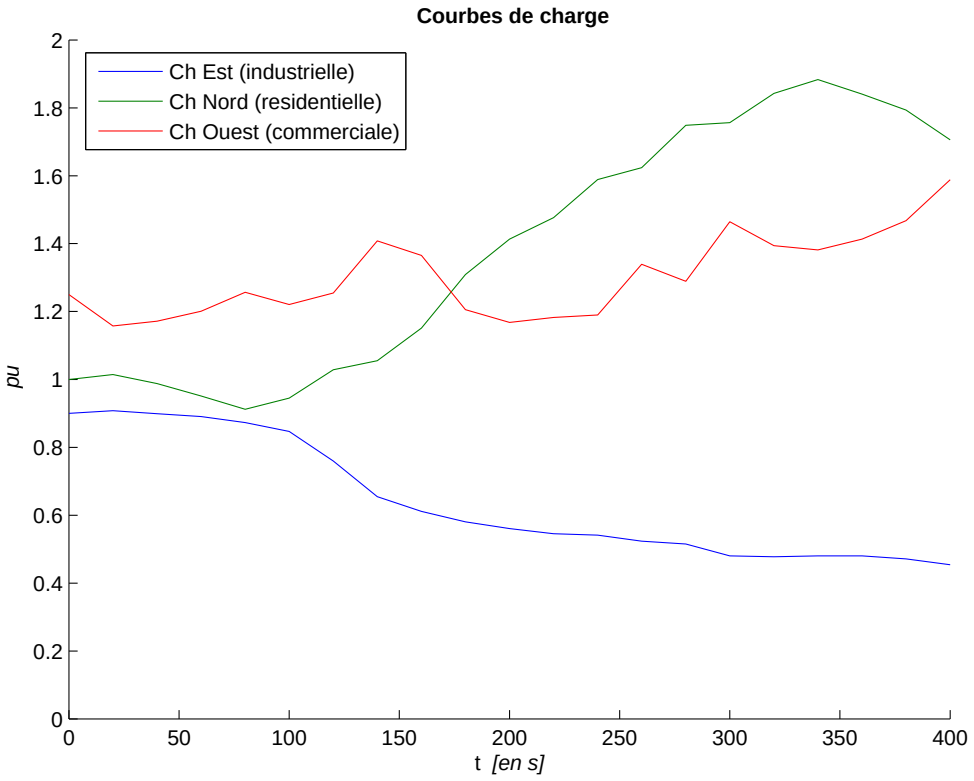

Fig. III.10 – Profil des courbes de charges

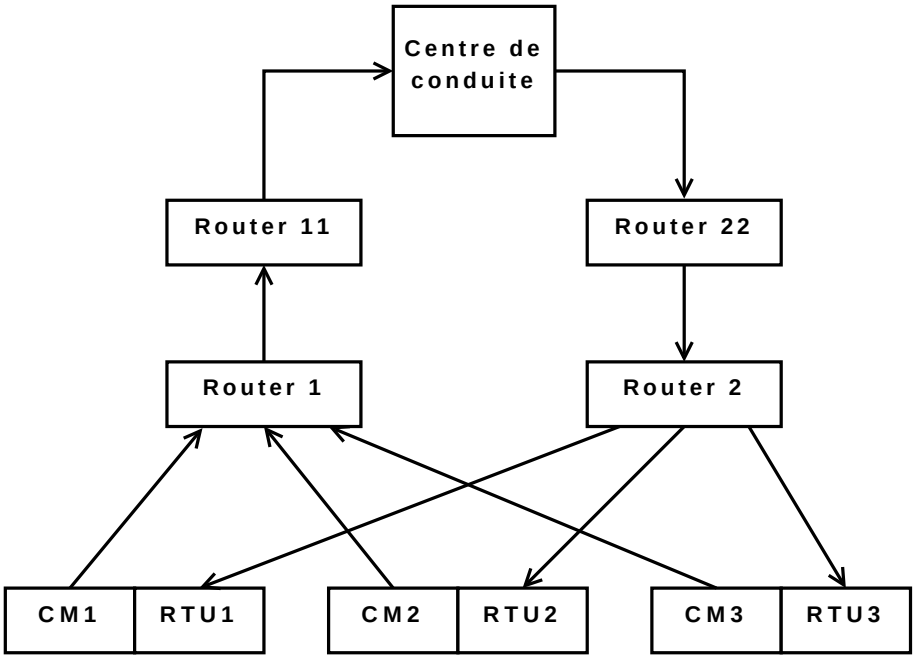

Fig. III.11 – Réseau de communication

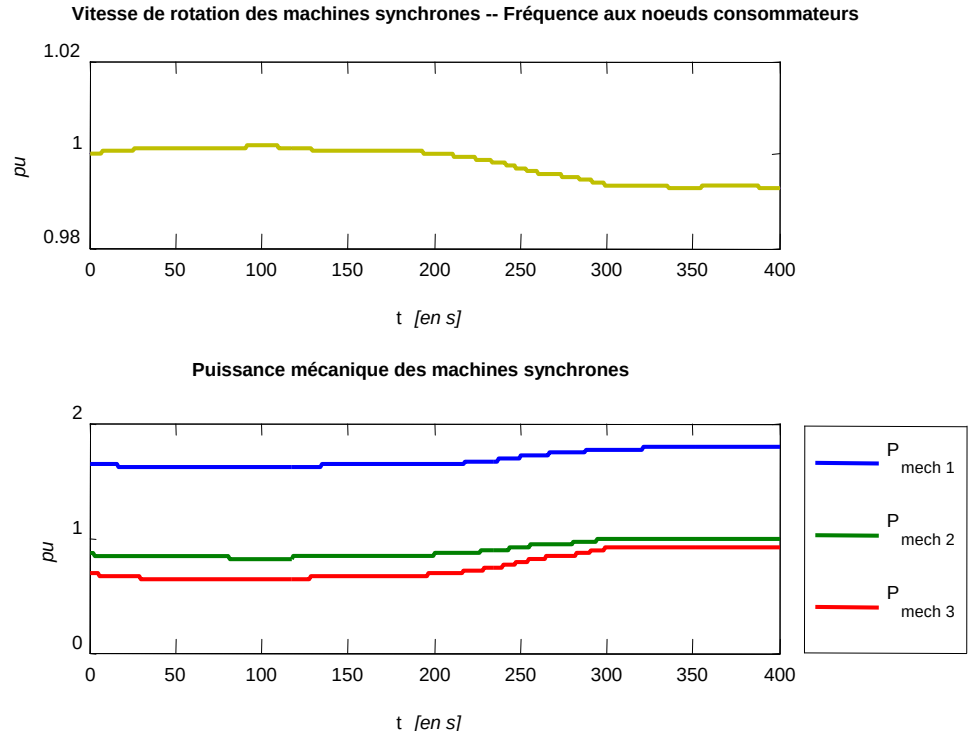

FIG. III.12 – Résultats pour le scénario 1

le centre de conduite aux instants 265s et 285s. La fréquence reste dans les limites grâce au réglage secondaire de fréquence [RTEa] [RTE04] coordonné par le centre de conduite (système d'information) et il n'y a pas eu de délestage fréquencemétrique. Les résultats obtenus dans ce cas sont illustrés figure III.13.

Le centre de conduite a reçu et traité 38 alarmes lors de ce scénario.

Troisième scénario

La contingence N-1 dans le réseau électrique précédent est associée avec une défaillance dans un des composants du réseau de télécommunication : le routeur connectant les stations de mesures avec le centre de conduite est mis hors service à l'instant de simulation dix secondes puis redémarré à l'instant de simulation trois cent dix secondes. Les liens de secours du réseau de télécommunication ne sont pas activés. Pendant trois cents secondes, le centre de conduite n'a aucune information actualisée sur l'état du système. Les réglages secondaires de tension ([PLT87], [RTEa] et [RTE04]) et de fréquence ne peuvent pas fonctionner. Lorsque le routeur de communication est redémarré, le centre de conduite reçoit les alarmes et peut finalement réagir. Néanmoins, la fréquence est déjà inférieure à la première limite basse (48 Hz) et un délestage de charge est effectué : 20% de la consommation est effacée à partir de l'instant 311s comme on peut le voir figure III.14. La réaction du centre de conduite arrive trop tard.

Le nombre total d'alarme traitées par le centre de conduite n'est plus que de 11.

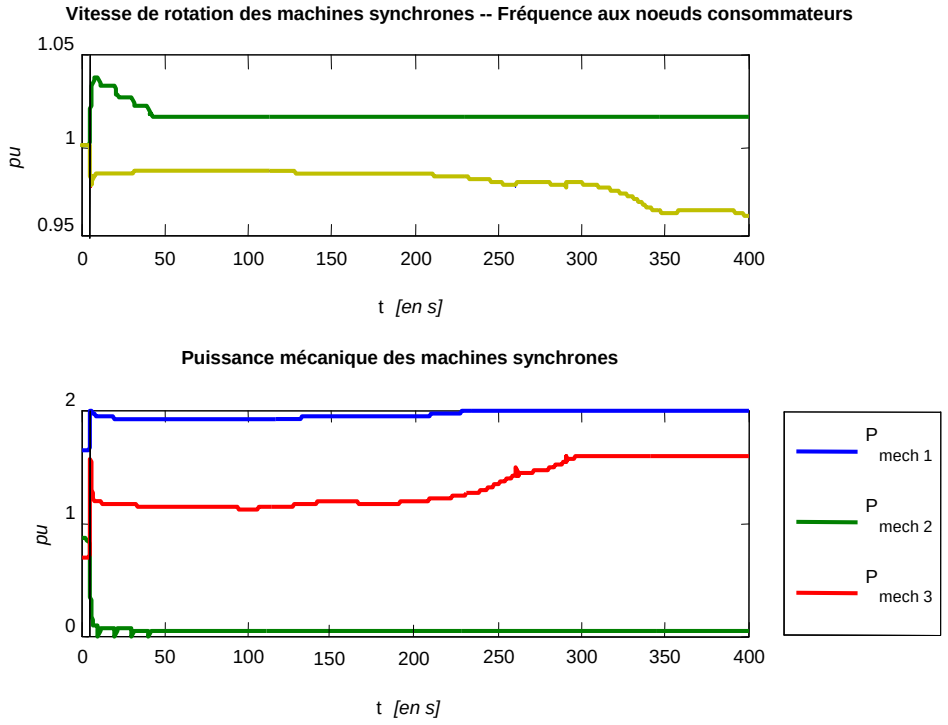

Fig. III.13 – Résultats pour le scénario 2

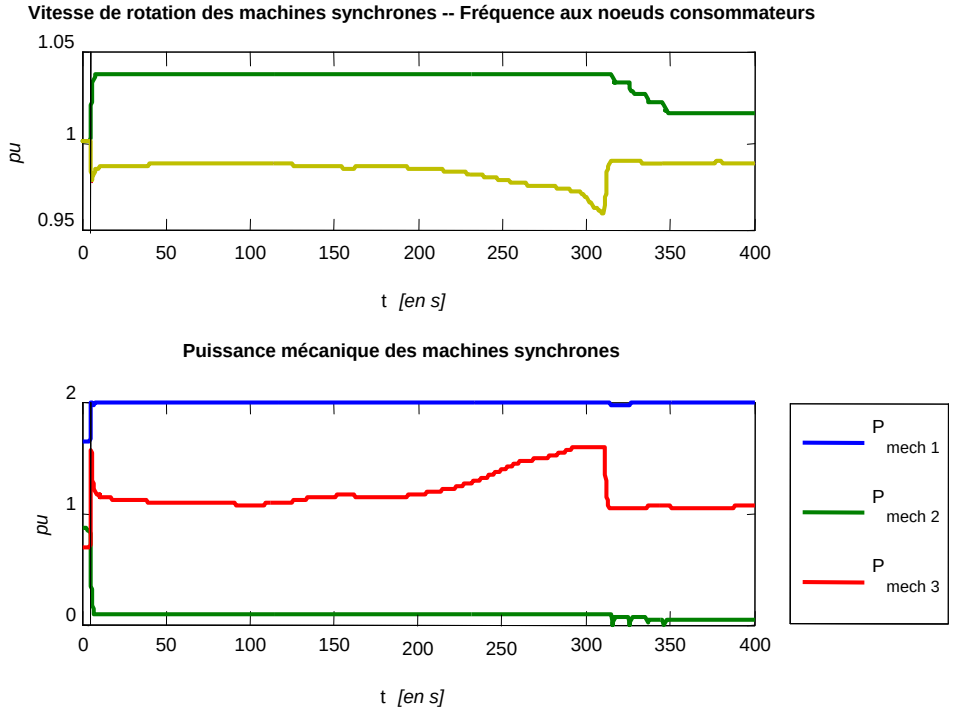

Fig. III.14 – Résultats pour le scénario 3

III.3.c Performances du cosimulateur

Les performances de calcul du simulateur (en terme de temps d'exécution) ne sont pas exceptionnelles, mais néanmoins acceptables. Les principales raisons sont l'utilisation de langages interprétés et surtout la communication inter-processus qui allonge les temps de simulation, surtout sous le système d'exploitation Windows où Matlab lance l'exécutable Perl à chaque pas de simulation. Sur un ordinateur de bureau actuel « classique » (PC Pentium 4, processeur cadencé à 3 GHz avec 1 Go de RAM), la durée de simulation est équivalente au temps simulé (temps réel), une simulation de 300 secondes prenant un peu moins de 5 minutes de calcul. Néanmoins, le rapport temps simulé sur temps réel de simulation n'est pas constant. En effet, la simulation est vraiment plus rapide lorsque tout se passe bien et plus de calculs sont nécessaires lorsque des grandes perturbations se produisent ou que des interrupteurs commutent. La simulation de l'infrastructure de communication nécessite relativement beaucoup moins de temps que celle de l'infrastructure électrique. L'utilisation d'un processeur multi-cœur ne conduit pas à des améliorations de la vitesse de calcul car les différentes simulations ne s'exécutent pas en parallèle mais elles sont exécutées de manière séquentielle. Cela est dû à notre procédé de synchronisation (voir section III.2.d). Chaque simulation, après avoir écrit ses données calculées dans un tube de communication (et permet ainsi au processus situé à l'extrémité de ce tube qui attendait dans un état bloquant, de continuer ses calculs) attend en retour des données à lire et donc arrête de calculer.

Au final, le noyau de cosimulation est pleinement fonctionnel, très flexible, multi-plateforme et modulaire.

III.4 Conclusion partielle

Il est nécessaire de développer des outils permettant une meilleure compréhension du comportement des systèmes multi-infrastructures. Dans cet objectif, un cosimulateur multi-plateforme a été réalisé intégrant trois infrastructures différentes. Il fonctionne et est très modulaire ce qui permet de facilement l'adapter à des besoins futurs. L'infrastructure d'étude, qui représente seulement un réseau régional avec son centre de conduite, a été choisie simple avec un nombre réduit de composants. Mais, il est possible d'étudier des réseaux avec un nombre d'éléments beaucoup plus élevé, comme le permet PSAT qui est le principal élément contraignant de cet outil.

Les simulations effectuées à travers les trois scénarios fournissent des résultats montrant qu'un réseau de télécommunication pleinement opérationnel est vraiment critique pour l'infrastructure électrique. Ces résultats mettent également en valeur l'effet des interdépendances d'un point de vue comportemental.

Il a été envisagé de mettre en place un préprocesseur et un traitement des résultats en vue d'effectuer des études statistiques qui auraient pu permettre d'identifier certaines vulnérabilités. Mais ce travail n'a pu être réalisé dans la cadre de cette thèse, faute de moyens humains. Une autre évolution envisagée est la possibilité d'insérer plusieurs centres de conduite, chacun gérant sa propre région électrique.

Chapitre IV

Réseaux complexes : Théorie et application sur l'infrastructure électrique

Sommaire

Résumé

Après un état de l'art, ce chapitre présente les méthodes classiques de la théorie des réseaux complexes appliquées à l'infrastructure électrique : différentes méthodes de partitionnement, une étude de robustesse et un modèle de cascade sont traités. Le réseau de référence choisi pour l'application de ces méthodes est un modèle approché de l'UCTE première zone.

IV.1 Introduction

L'approche présentée dans le chapitre précédent, basée sur de la simulation comportementale, est intéressante pour appréhender une partie des phénomènes d'interdépendances dans les systèmes multi-infrastructures, mais cette approche n'est pas suffisante pour en saisir la totalité. La principale raison est la limitation en terme de complexité et de temps de calcul. En effet, la simulation de phénomènes sur une durée d'une heure prendra une durée équivalent sur un petit réseau (d'une dizaine de nœuds électrique et de télécommunication avec un centre de contrôle) et ce pour une seule simulation. Pour une étude $N-1$ systématique, on peut être amené à effectuer plusieurs milliers de simulations de ce type. Une approche plus théorique et analytique est alors nécessaire. Il ne s'agit pas de décréter qu'elle est meilleure (ou moins bonne) que la précédente, mais plutôt de les considérer comme complémentaire et c'est cette vision double qui devrait permettre de mieux progresser dans l'analyse et la compréhension de ces systèmes complexes.

Comme les infrastructures étudiées sont des grands réseaux, une idée, en plus de celles exposées au chapitre 2, est de se servir de concepts issus des graphes ou plus précisément de réseaux complexes (*complex networks*). La théorie des réseaux complexes est une extension de la théorie des graphes [Die00], initiée en 1736 par Leonhard Euler. Pendant deux siècles, les mathématiciens n'ont pu étudier seulement que des graphes basés sur des modèles simples. En 1960, Paul Erdös et Alfréd Rényi ont fondé une nouvelle approche basée sur les méthodes probabilistes appelée théorie des graphes aléatoires. Dans leur modèle, les nœuds sont liés ensembles aléatoirement. Néanmoins, ces graphes sont homogènes c'est-à-dire que le nombre de voisins de chaque nœud n'a que de petites variations autour de sa valeur moyenne. Par exemple, si on considère le réseau électrique comme un graphe où les sous-stations sont les nœuds et les lignes les liens, alors l'homogénéité implique que chaque sous-station dans le réseau a à peu près le même nombre de lignes connectées. Depuis une dizaine d'année, grâce à l'explosion de la puissance de calcul des nouveaux moyens informatiques et l'existence de grandes bases de données, les comparaisons entre les modèles précédents et les réseaux réels ont montré que les premiers sont inadéquats pour étudier les infrastructures réelles. En effet, les réseaux réels de la sociologie, l'informatique, la biologie, l'électronique, l'électricité, les télécommunications et les transports sont fortement hétérogènes. Par exemple, dans les réseaux sociaux, il y a des individus ayant une forte vie sociale connaissant de nombreuses autres personnes et d'autres plus isolés étant en relation avec un nombre plus restreint de personnes. De même, si l'on considère le transport aérien, il existe des aéroports comme l'aéroport international JFK de New-York reliant de très nombreuses destinations de par le monde et d'autres tels que l'aéroport de Grenoble ayant un nombre de connexions beaucoup plus limité. L'émergence de nouveaux modèles pour mieux décrire ces graphes a conduit à la création de la théorie des réseaux complexes. Ce champ d'étude est relativement récent, mais en pleine croissance du fait de ses applications pluridisciplinaires. Dans la littérature, les ouvrages suivants présentent une synthèse détaillée de ce domaine : [AB02], [BLM$^+$06], [DM01] et [New03].

Un graphe ou un réseau (complexe) est composé d'arêtes – ou autrement appelées connexions, liens, arcs, lignes – reliant entre eux des sommets – ou sites, nœuds –, les arcs pouvant être orientés ou non. Selon les graphes considérés, les boucles – qui sont des arcs dont les deux extrémités sont rattachées au même sommet – et les arcs multiples

peuvent exister, ou non. De plus, on peut associer des poids aux arcs et/ou aux nœuds. La généralité de cette définition permet à la théorie des réseaux complexes de s'appliquer à des domaines aussi variés que les mathématiques, la physique, la biologie, l'informatique et la sociologie.

L'Internet, le *World-Wide Web*, les réseaux de collaboration scientifiques et filmographiques pour les acteurs sont les réseaux les plus classiquement étudiés par cette théorie, en particulier du fait de l'existence des bases de données associées. Néanmoins, l'infrastructure électrique en tant que réseau complexe a également été analysée dans [Hol06] où est décrite l'utilisation de modèles de graphes pour analyser la vulnérabilité de ces réseaux envers des attaques intentionnelles ou aléatoire consistant en la suppression de nœuds. Dans [CLDN02] et [KCAL05], sont proposées des modélisations de défaillances en cascade sur le réseau électrique de transport nord-américain. Cette approche est également proposée dans [Sun05] comme nouvelle méthode pour modéliser les défaillances en cascade dans les réseaux électriques. Dans [SH05], il y a une analyse et une comparaison de différents types de modèles de défauts en cascade, de nouveau dans les réseaux électriques. En outre, l'article [CSCW07] propose une identification des lignes vulnérables dans les réseaux électriques basée sur la théorie des réseaux complexes. Néanmoins, l'ensemble de ces études ne s'appliquent que à une seule infrastructure à la fois. Il y a également des descriptions de modèles pour l'étude des interactions des infrastructures critiques en tant que systèmes complexes dans [NNC+05] ainsi qu'une analyse des risques afférents dans [CNG+07]. Pour finir cet état de l'art, deux projets européens ont basé une partie de leur étude sur cette théorie pour l'étude des infrastructures critiques : IRRIIS et Manmade.

Le projet IRRIIS (*Integrated Risk Reduction of Information-based Infrastructure Systems*) financé par la commission européenne dans le cadre du FP6 s'intéresse aux *Large Complex Critical Infrastructures (LCCI)*, c'est-à-dire aux infrastructures critiques, et plus spécifiquement à la réalisation d'outils d'évaluation et de conception. Dans son livrable D.2.1.1 [IRR06], une étude est réalisée sur la topologie des *LCCI*, étude fondée sur la théorie des réseaux complexes. En particulier, une étude du partitionnement du réseau électrique (de transport) italien et des études topologiques sur ce même réseau sur Internet au niveau des routeurs des systèmes autonomes *(AS)* sont effectuées.

Le projet Manmade [Arr08] a pour but d'identifier les vulnérabilités et les phénomènes émergeant dans les réseaux construits par les humains (*manmade*) en développant des méthodes mathématiques. De par sa définition, il s'adresse donc à l'ensemble des infrastructures critiques. Dans le cadre de ce projet, il a été effectué une étude de robustesse sur les réseaux électriques scandinaves (NORDEL) et européens (UCTE) ainsi que sur les réseaux de gaz d'Allemagne et du Royaume-Uni.

Généralement, les études utilisant la théorie des réseaux complexes commencent par une caractérisation statique ou statistique des réseaux. C'est à dire aux calculs de certaines grandeurs caractérisant la topologie de ces graphes tels que entre autres, le degrés des nœuds, la distribution de ces degrés, les corrélations, le diamètre, la longueur caractéristique du graphe, le degré moyen et le coefficient de *clustering* entres autres. Cette étude sera présentée dans la section IV.3. Il peut également être intéressant d'appliquer des méthodes de partitionnement de graphe aux infrastructures critiques. Celui-ci consiste à séparer un graphe en deux ou N parties distinctes avec un minimum de coupures de lignes. Cette étude qui peut permettre d'identifier les zones de faiblesses d'un réseau sera

effectuée dans la section IV.4. En plus de cette caractérisation purement statique, une modélisation des phénomènes dynamiques pouvant intervenir dans les réseaux peut être réalisée. La question de la résistance aux pannes et aux attaques est présentée dans la section IV.5. Un autre phénomène dynamique étudié est le problème de la vulnérabilité des réseaux complexes vis à vis des attaques basées sur les défaillances en cascade détaillée dans la section IV.6.

Le but de ce chapitre est de présenter un panorama, et non pas une étude exhaustive, des méthodes classiquement utilisées sur un système mono-infrastructure afin de pouvoir s'en inspirer dans la proposition de modélisation pour les systèmes multi-infrastructures couplés présentée au chapitre suivant. Pour cette raison, des extensions possibles de ces différentes méthodes seront exposées dans leur bilan.

Pour compléter cette introduction, voici les définitions de quelques termes relatifs à la théorie des graphes fréquemment utilisés par la suite. Celles-ci seront illustrées sur un exemple simple qui est le graphe maison présenté figure IV.1.

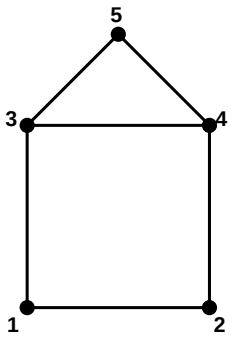

Fig. IV.1 – Graphe maison

Graphe : ensemble V de N nœuds (ou sommets ou points ou vertex) et E de L liaisons (ou liens ou arcs ou edge) entre ces points. Une liaison est un couple de nœuds $(i, j) \in V^2$. Un graphe G est donc un couple de deux ensembles :

$$G = (V, E) \tag{IV.1}$$

Le graphe maison comporte cinq nœuds et six liaisons.

Degré : le degré k_i du nœud i est le nombre de nœuds j tels que $(i, j) \in E$, autrement dit le nombre de voisins de i sur le graphe ou encore le nombre de liens connectés au nœuds i. Les degrés du graphe maison sont 2, 2, 3, 3 et 2 (donnés dans l'ordre des nœuds).

Degré moyen : moyenne des degrés de tous les nœuds :

$$\sum_{i \in V} \frac{k_i}{N} \tag{IV.2}$$

Le degré moyen du graphe maison est $2,4$.

Densité :

$$\frac{L}{\frac{N*(N-1)}{2}} \tag{IV.3}$$

La densité montre la connectivité globale entre les nœuds du graphe. Un graphe sans liaison aura une densité nulle et un graphe ayant toute les liaisons possibles aura une densité égale à 1. La densité du graphe maison vaut $0,6$.

Chemin géodésique : le plus court chemin existant entre deux nœuds du graphe. Le chemin géodésique entre 1 et 5 est 1 – 3 – 5.

Diamètre : le plus long de tous les chemins géodésique d'un graphe entre chaque paire de nœuds. Le diamètre du graphe maison vaut 2. Il est atteint par exemple entre 1 et 5.

Distance moyenne :

$$L_{moy} = \frac{1}{N(N-1)} \sum_{i \neq j \in V} d_{ij} \tag{IV.4}$$

avec d_{ij} la longueur du chemin géodésique entre i et j. L_{moy} est fini pour un graphe connecté, mais son calcul pose problème pour un graphe non connecté. Deux solutions sont alors adoptées, soit le calcul de L_{moy} pour le plus grand sous graphe connecté soit le calcul de l'efficacité globale E_{glob}. Pour le graphe maison, la somme des distances vaut 28, soit une distance moyenne de $1,4$.

Efficacité globale :

$$E_{glob} = \frac{1}{N(N-1)} \sum_{i \neq j \in V} \frac{1}{d_{ij}} \tag{IV.5}$$

cette grandeur peut être normalisée [LM01] [LM04] [Sun05]. L'efficacité entre deux nœuds correspond à l'inverse de sa distance géodésique, l'efficacité globale en est sa valeur moyenne pour le graphe. Lorsque un nœud i est isolé alors $d_{ij} = \infty$ et $\frac{1}{d_{ij}} = 0$. Elle vaut $0,8$ pour le graphe maison.

Coefficient de clustering : c_i fraction de voisins de i qui sont connectés entre eux. Il mesure donc la densité locale de liaisons. Pour les nœuds du graphe maison, il vaut 0, 0, 1/3, 1/3 et 1. En effet, le nœud 1 est connecté à 2 et 3 qui ne sont pas connectés entre eux et le nœud 5 est connecté à 3 et 4 qui sont connectés entre eux.

Coefficient de clustering moyen :

$$C = \frac{1}{N} \sum_{i} c_i \tag{IV.6}$$

Il mesure la densité moyenne de triangles présents. Il vaut 5/3 pour le graphe maison.

Coefficient de centralité d'intermédiarité : (*betweenness centrality*) b peut être défini pour les nœuds et pour les liaisons. Si n est le nombre total de chemins géodésiques et $n(i)$ le nombre de chemins géodésiques passant par l'élément i, alors

$$b_i = \frac{n(i)}{n} \tag{IV.7}$$

Pour le calcul, on ne considère pas les extrémités. Ainsi, un nœud présent sur beaucoup de chemins géodésiques entre d'autres nœuds aura un coefficient de centralité d'intermédiarité beaucoup plus grand. On peut aussi ne pas diviser par n. Pour les nœuds du graphe maison, il vaut 1, 1, 3, 3 et 0. En effet, le nœud 1 est sur la moitié des chemins les plus courts entre 2 et 3 et sur la moitié entre 3 et 2 donc son coefficient vaut 1. Pour le nœud 3, il est sur le seul chemin le plus court entre 1 et 5

et entre 5 et 1 et sur la moitié des chemins géodésiques entre 1 et 4 et 4 et 1, son coefficient vaut donc 3.

Distribution des degrés ou densité de probabilité des degrés :

$$p_k = \frac{N_k}{N} \tag{IV.8}$$

où N_k est le nombre de nœuds de degré k. Pour le graphe maison, $p_2 = \frac{3}{5}$, $p_3 = \frac{2}{5}$ et $p_j = \frac{0}{5}$ pour j différent de 2 et 3. L'histogramme correspondant est présenté figure IV.2.

Moment d'ordre n :

$$< k^n >= \sum_k k^n p_k \tag{IV.9}$$

Le premier moment est égal au degré moyen du graphe. Le second moment est une indication des fluctuations de la distribution des degrés.

Connexité : un graphe est dit connexe s'il existe un chemin entre tous les nœuds qui le composent. Le graphe maison est connexe.

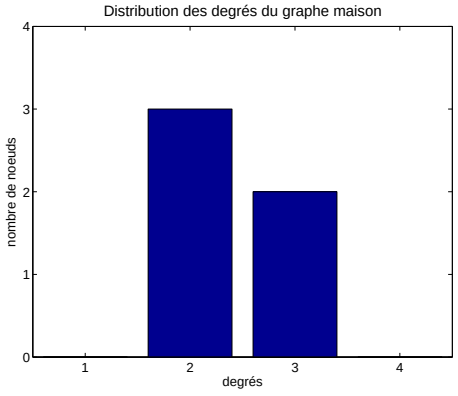

Fig. IV.2 – Histogramme de la distribution des degrés du graphe maison

IV.2 Outils

IV.2.a Description du réseau d'étude

Le graphe de référence utilisé dans ce chapitre (et le suivant) pour étudier les méthodes classiques de la théorie des réseaux complexes est issu d'un réseau électrique réel. Ce réseau correspond à une partie du réseau de transport européen, plus particulièrement le réseau UCTE (Union pour la Coordination du Transport de l'Electricité) première zone. Celui-ci comprend 18 pays : Portugal, Espagne, France, Belgique, Luxembourg, Allemagne, Pays-Bas, Suisse, Italie, Danemark (partie continentale), République Tchèque, Autriche, Slovénie, Pologne, Slovaquie, Hongrie, Croatie et une partie de la Bosnie-Herzégovine. C'est un modèle établi par Qiong Zhou et Janusz Bialek comprenant 1254 nœuds, 1944 lignes et 378 générateurs [ZB05][1]. Ce modèle est approché du fait de l'indisponibilité des données

[1]Les données résultantes sont disponibles à l'adresse `http://www.see.ed.ac.uk/~jbialek/Europe_load_flow/`

exactes. En effet, les compagnies de transports de l'électricité ne publient pas ces informations pour des raisons commerciales ou de sécurité. Pour l'établissement du modèle, seules les données publiquement disponibles ont été utilisées. Les hypothèses servant à son établissement sont :

- seules les lignes à un niveau de tension supérieur ou égal à 220 kV sont prises en compte ;
- la résistance, l'admittance parallèle et les capacités séries, lorsqu'il y en a, sont ignorées. Seule la réactance série est considérée ;
- la réactance est calculée à partir de la longueur des lignes en considérant une impédance de $0.31\Omega/km$ pour les lignes 220 kV et $0.28\Omega/km$ pour les lignes 380 kV à 50 Hz ;
- tous les interrupteurs sont considérés fermés à l'état normal ;
- certains nœuds différents géographiquement proches ont été fusionnés en un nœud équivalent.

Pour ce chapitre, l'établissement du graphe a été effectué à partir de ce réseau en considérant en plus deux hypothèses. La première est que les lignes bi-ternes, c'est-à-dire les liaisons multiples entre une même paire de nœud, ont été considérées comme une liaison simple. La seconde est que les liaisons ne sont pas pondérées. Une représentation graphique du graphe est présentée figure IV.3.

IV.2.b Logiciels utilisés

Les différents calculs sur les graphes ont été majoritairement réalisés à l'aide du logiciel NetworkX ([HSS05]). NetworkX est un logiciel développé dans l'équipe *Mathematical Modeling and Analysis* du *Los Alamos National Laboratory*. Il est dédié à la création et la manipulation et donc l'étude des réseaux complexes qu'ils soient de nature technologique, biologique ou bien sociale. Par conséquent, les champs d'applications de ce logiciel couvrent aussi bien les mathématiques, l'informatique, la physique, la biologie que la sociologie. Il inclue déjà des fonctions de création et de mesures des grandeurs usuelles des graphes tel que par exemple le calcul du chemin le plus court entre deux nœuds. NetworkX est écrit en langage Python et par conséquent est multi-plateforme. C'est un logiciel libre distribué sous les termes de la LGPL (GNU Lesser General Public License).

Pour le tracé des figures et une partie de l'étude du partitionnement, le logiciel Matlab, qui a déjà été présenté au chapitre précédent, a été utilisé.

Pour le tracé des graphes, outre Matlab, il a également été fait usage de neato de la suite Graphviz (*Graph Visualisation Software*) développé par *AT&R Research*. Ce logiciel dispose d'un algorithme permettant de disposer les nœuds dans le plan afin de minimiser les croisement de lignes, ce qui est fort utile lorsque l'on ne dispose pas des données géographiques de ces points.

IV.3 Caractéristiques topologiques

Dans cette section sont présentées les caractéristiques statiques, purement topologiques du graphe étudié.

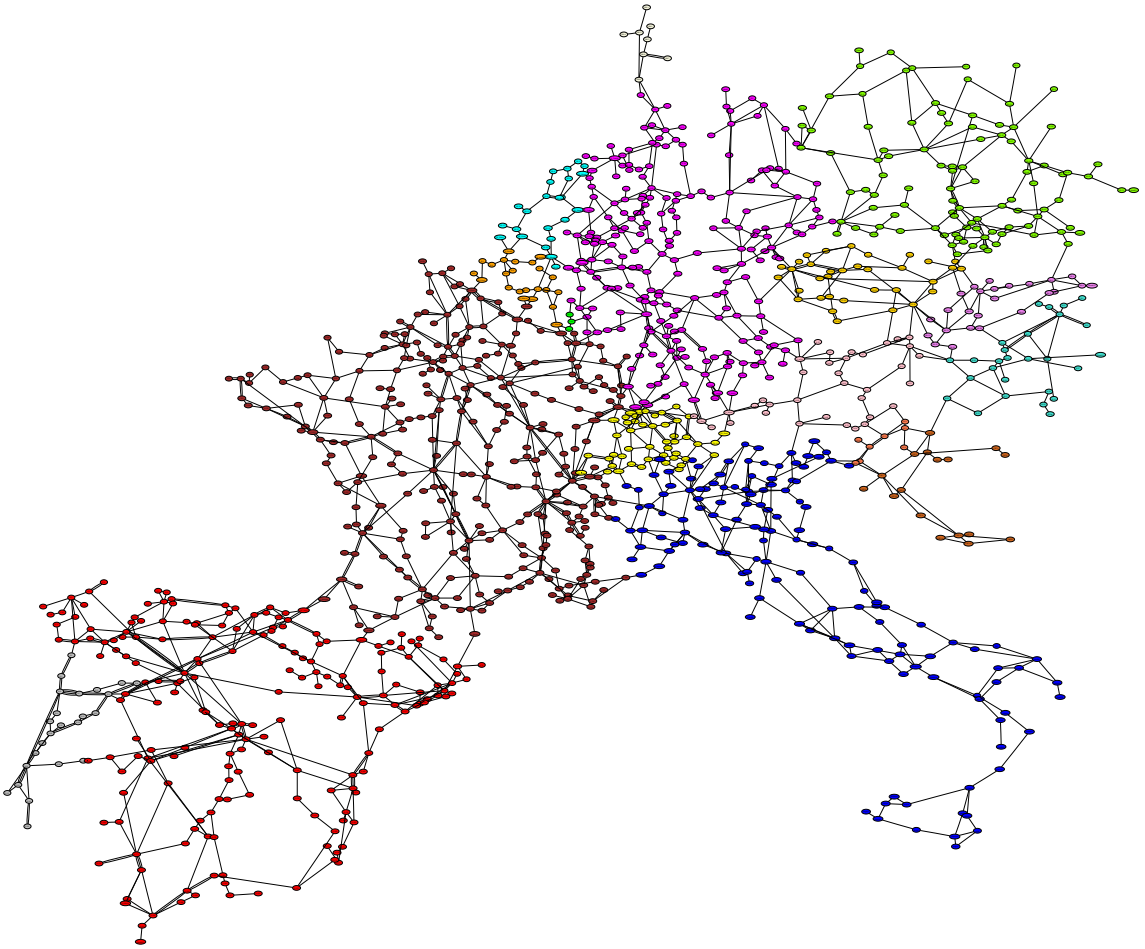

Fig. IV.3 – Réseau UCTE première zone

IV.3.a Caractéristiques générales

Pour commencer, on peut calculer quelques caractéristiques du graphe précédemment définies :

- nombre de nœuds : 1254 ;
- nombre de liens : 1812 ;
- densité : $0,0023$;
- degré moyen : $2,8900$;
- moment d'ordre 2 des degrés : $11,4402$;
- degré maximum : 13 ;
- diamètre : 48 ;
- coefficient de clustering moyen : $0,1063$;
- distance moyenne : $17,2728$;
- histogramme des degrés : voir table IV.1.

Tab. IV.1 – Histogramme des degrés du graphe représentatif de l'UCTE

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13
N_k	0	204	490	229	129	90	57	31	10	4	5	1	1	3

IV.3.b Distribution des degrés

L'histogramme des degrés permet, grâce à une simple division par le nombre total de nœuds dans le graphe, de calculer la distribution des degrés. Celle-ci est tracée pour l'UCTE sur une échelle linéaire figure IV.4. Le trait discontinu vertical correspond au degré moyen pour le graphe. On peut remarquer qu'il existe une grande différence d'ordre de grandeur entre le nombre de sommets de chaque degré. Afin de permettre une meilleure visualisation, le tracé a également été effectué sur la même figure avec une échelle semi-logarithmique pour l'axe des ordonnées. Cette fonction correspond aussi à la densité de probabilité qu'un nœud choisi au hasard dans le graphe possède k voisins. On la note p_k.

Il est intéressant de savoir comment décroît la fonction de distribution des degrés au fur et à mesure que le degré augmente. Cependant, cette fonction est en générale « bruitée », et ne permet donc pas une identification aisée de la forme de sa loi de décroissance. Pour contourner ce problème, deux méthodes ont été proposées [New03]. La première consiste à tracer l'histogramme avec une taille de la classe augmentant exponentiellement avec le degré. Par exemple, les premières classes peuvent être : 1, 2–3, 4–7, 8–15 et ainsi de suite. La valeur pour chaque classe étant divisée par le nombre de degré qu'elle comprend. Ainsi est réalisé une sorte de moyenne adaptative où les valeurs les plus faibles, c'est-à-dire appartenant aux degrés les plus élevés sont moyennés sur un plus grand intervalle. L'inconvénient majeur de cette méthode est la perte d'information due à l'agglomération dans une même classe des degrés différents. Elle est cependant bien adaptée, lorsque l'on trace l'histogramme sur une échelle logarithmique pour les abscisses. La seconde méthode consiste à, non pas tracer directement la fonction de densité de probabilité, mais plutôt la fonction de distribution cumulée ou pour reprendre le terme de statistique, « la fonction de répartition ». Cette fonction est calculée en sommant cumulativement les termes de la

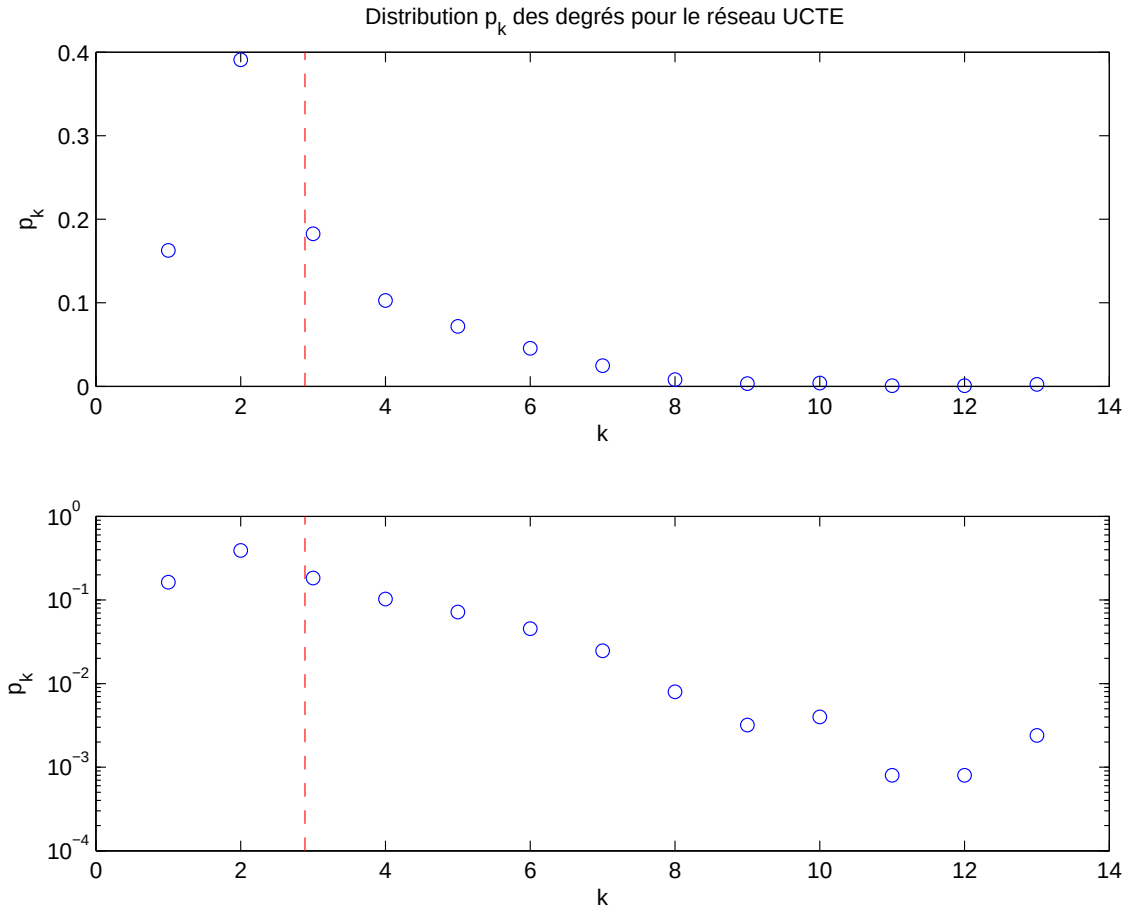

Fig. IV.4 – Densité de probabilité d'avoir un nœud de degré k

fonction de densité de probabilité des degrés :

$$P_k = \sum_{j \geq k} p_j \tag{IV.10}$$

Ainsi, P_k correspond à la probabilité qu'un nœud choisi au hasard possède au moins k voisins. Il n'y a pas de perte d'informations car la densité de probabilité peut être retrouvée à partir de la fonction de répartition grâce à des différences [New03]. La fonction de répartition est tracée figure IV.5 avec une échelle semi-logarithmique et une échelle log-log.

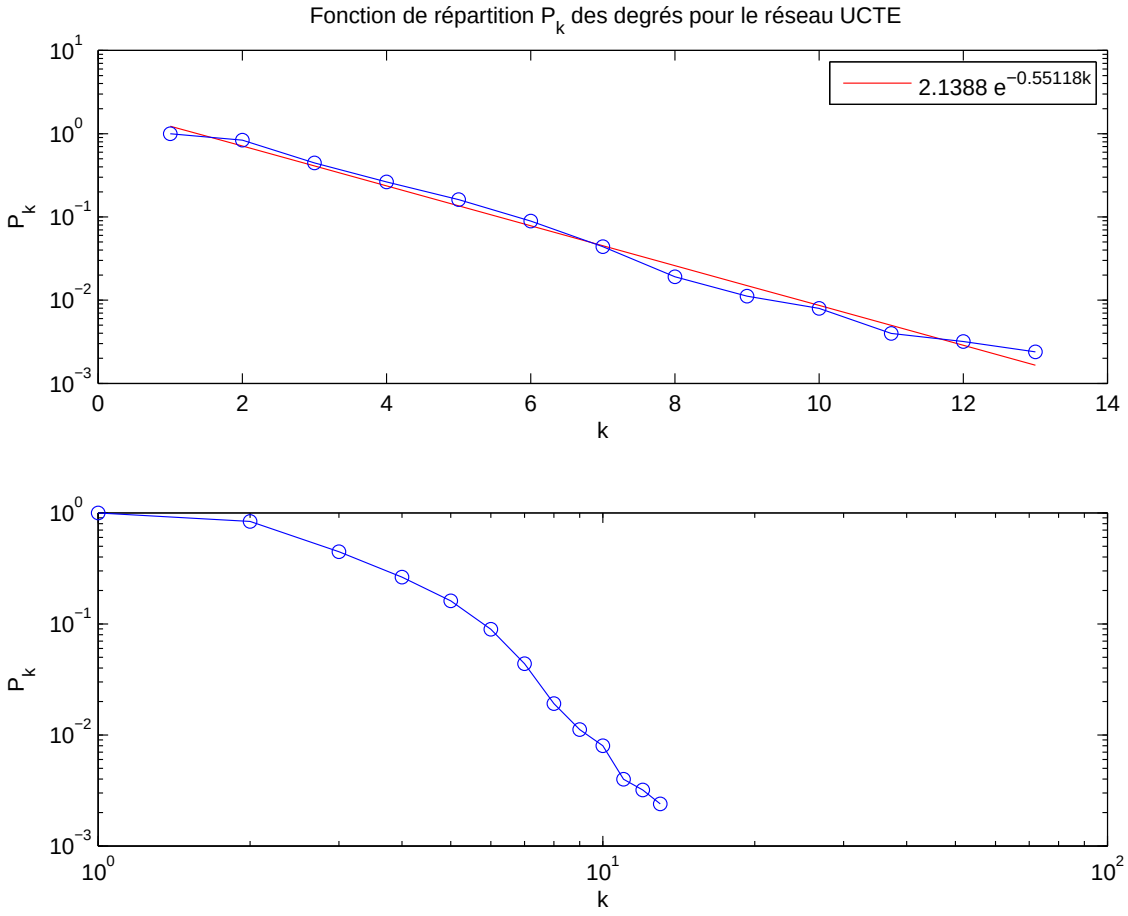

FIG. IV.5 – Fonction de répartition pour le graphe de l'UCTE

Pour un graphe aléatoire tel que défini en 1960 dans le modèle des mathématiciens Paul Erdös et Alfréd Rényi, la densité de probabilité des degrés suit une loi de Poisson définie pleinement avec un degré moyen $< k >$.

Les réseaux réels ne correspondent que très rarement à un graphe aléatoire. La décroissance de leur densité de probabilité peut suivre une loi de puissance, c'est-à-dire de la forme $k^{-\alpha}$ pour la densité de probabilité soit, $k^{-(\alpha-1)}$ pour la fonction de répartition avec α généralement compris entre 2 et 3. Cette décroissance correspond à une droite sur une échelle log-log. Une autre possibilité est que la décroissance suive une loi exponentielle, c'est-à-dire de la forme $c \cdot e^{-\beta k}$ aussi bien pour la densité de probabilité que pour la

fonction de répartition. Cette décroissance correspond à une droite sur une échelle semi-logarithmique (linéaire en abscisse et logarithmique en ordonnée). La figure IV.5 montre simplement que la loi de distribution des degrés pour le graphe étudié ne suit pas une loi de puissance, mais une loi exponentielle. Cette loi correspond à $P_k = 2,14e^{-0,551k}$.

Les graphes dits sans-échelle (*scale-free*) ont une loi de distribution des degrés en puissance. Ce n'est pas le cas du graphe d'étude qui n'est donc pas sans-échelle. On retrouve cette constatation sur d'autres réseaux électriques dans le monde par exemple le réseau de l'ouest des États-Unis [Sun05], le réseau italien [CLM04b], et les réseaux ferroviaire qui ont la même loi. Dans le cas du réseau italien, la fonction de répartition suit la loi $P_k = 2,5e^{-0,55k}$, loi très proche du réseau UCTE dans lequel il est inclus. Pour le réseau de l'ouest des États-Unis, le coefficient β vaut 0,5. Par contre, la densité de probabilité des degrés suit une loi de puissance pour les réseaux sociaux (par exemple citations), liens sur le Web, graphes d'appels téléphoniques). On peut remarquer que la première catégorie correspond à des réseaux physiques ayant une implantation géographique, contrairement à la deuxième catégorie.

IV.3.c Petits-mondes

Les graphes « petits-mondes » (*small-world*) sont des graphes ayant une petite valeur de distance moyenne comme les graphes aléatoires et une grande valeur de coefficient de clustering comme les maillages réguliers (treillis). Cet effet a été découvert par le sociologue Stanley Milgram, qui observa empiriquement en 1967, que seul un nombre réduit d'étapes étaient nécessaires pour envoyer des paquets (lettres) entre deux personnes préalablement sélectionnées aléatoirement, chaque personne ne faisant suivre ces paquets qu'a des personnes qu'elle connaît. Pour un graphe aléatoire, on a :

$$L_{rand} \sim \frac{ln(N)}{ln(< k > -1)} \tag{IV.11}$$

et

$$C_{rand} \sim \frac{< k >}{N} \tag{IV.12}$$

tandis que pour un maillage régulier :

$$L_{reg} \sim \frac{N}{2 < k >} \tag{IV.13}$$

et

$$C_{reg} \sim \frac{3(< k > -2)}{4(< k > -1)} \tag{IV.14}$$

[LM01].

Tab. IV.2 – Comparaison de la distance moyenne et du coefficient de clustering entre le graphe UCTE et deux graphes classiques

	graphe UCTE étudié	graphe aléatoire	maillage régulier
L	$L_{UCTE} = 17,273$	$L_{rand} = 11,207$	$L_{reg} = 216,96$
C	$C_{UCTE} = 0,1063$	$C_{rand} = 0,0023$	$C_{reg} = 0,3532$

Comme on peut le voir table IV.2, le graphe d'étude a une petite valeur de L comme un graphe aléatoire avec un nombre de nœuds et de liens équivalents et une grande valeur de C comme un maillage régulier avec un nombre de nœuds et de liens équivalents. Ce graphe possède donc la propriété « petits-mondes ». Cela signifie donc qu'il est efficace pour transporter de l'énergie à la fois globalement (faible distance moyenne) et localement (coefficient de clustering élevé) [LM04]. Cette propriété a également été observée sur le réseau de l'ouest des États-Unis, les réseaux du Nord et du Centre de la Chine [Sun05] et le réseau de transport Nordique [Hol06].

IV.4 Partitionnement

IV.4.a Objectifs

L'étude du partitionnement de graphe permet de déterminer quels sont ses points de faiblesse. Par conséquent, si le graphe étudié modélise un réseau réel, on peut évaluer les lignes de fracture possible de l'infrastructure considérée. En particulier, lorsque l'infrastructure est un réseau électrique, la connaissance de ces lignes de coupure peut permettre de prévoir, en cas de fort déséquilibre de charge entre les régions du réseau, les lignes où peuvent se produire une cascade de surcharge et le découpage en zones résultant. Ce type d'étude peut ainsi permettre, grâce à la connaissance de cette vulnérabilité topologique du réseau actuel, de :

- soit planifier la construction de nouvelles lignes qui renforcera le réseau,
- soit prévoir des mesures permettant aux sous-réseaux indépendants pouvant se former de fonctionner de manière autonome si la première option n'est pas possible pour une quelconque raison (environnementale, économique, politique ou autre).

La connaissance de la séparation minimale à effectuer pour séparer le graphe peut également être utile afin d'éviter la propagation de perturbation telle que le phénomène de cascade. Dans ce cas, cette étude permet de découper préventivement des zones et de faire en sorte qu'elles puissent fonctionner de manière autonome. Cette situation est semblable au cas précédent mais, dans ce cas, la partition (ou îlotage) est intentionnelle.

D'un point de vue social, ce genre de méthode est utilisé pour déterminer les communautés (ou groupes fortement connectés). Il est ensuite possible de caractériser un individu donné selon qu'il se situe pleinement dans un sous groupe social ou si au contraire il agit comme un pont à la frontière de différents sous groupes. Cette méthode est également utilisée pour faire de la répartition de charge pour des calculs parallèles ou pour concevoir des réseaux téléphoniques [BLM+06].

Le travail présenté dans cette section a fait l'objet d'une publication au *IEEE PowerTech* en 2009 [RCH+09].

Trois méthodes différentes de partitionnement de graphe ont été étudiées et vont être présentées : la bissection spectrale, l'algorithme de Girvan et Newman et un partitionnement spectral étendu. Les deux partitionnements spectraux ont été testés sous Python avec NetworkX et sous Matlab pour vérification tandis que l'algorithme de Girvan et Newman n'a été testé que avec NetworkX. En effet, contrairement à Matlab, NetworkX possède une fonction permettant de calculer directement le coefficient de centralité d'intermédiarité pour les liaisons du graphe.

IV.4.b Bissection spectrale

Principe

Le problème du bi-partitionnement de graphe est considéré comme classique en informatique. Il consiste à trouver la division du graphe en deux sous graphes de taille (c'est-à-dire de nombre de nœuds) à peu près égale avec un minimum de liaisons entre ces deux sous parties. Ce problème est connu pour être de type NP-complet [BLM+06]. Différentes méthodes ont été développées pour résoudre ce problème.

La méthode spectrale donne généralement de meilleures solutions que les méthodes heuristiques qui cherchent au voisinage d'un partitionnement initial et ont tendance à rester bloquer dans un minimum local [BLM+06]. Cette méthode fonctionne bien pour couper le graphe en deux parties. Par contre, elle n'est pas la mieux adaptée pour le couper en un nombre quelconque (différent de deux) de sous graphes. Les vecteurs propres de différentes matrices peuvent être utilisés : ceux de la matrice adjacente A, la matrice laplacienne L ou la matrice normale N. Dans ce mémoire sera présentée la méthode avec la matrice laplacienne qui est bien décrite dans [BLM+06].

Description de la méthode

Cette méthode, autrement appelée théorème de la coupure minimale, a été proposée au début des années 1970 et popularisée dans les années 1990 [BLM+06].

Soit un graphe G composé de n nœuds. Sa matrice adjacente A est définie telle que $A_{ij} = 1$ si les nœuds i et j sont connectés et $A_{ij} = 0$ sinon. Sa matrice diagonale D est constituée des éléments $D_{ii} = k_i$ avec k_i le degré du nœud i. On peut alors calculer la matrice laplacienne du graphe [RBT07] :

$$L = D - A \tag{IV.15}$$

Cette matrice L de taille $n * n$, possède n valeurs propres w_i auxquelles sont associées n vecteurs propres v_i. Ces valeurs propres ont comme propriété d'être toutes réelles et positives :

$$\forall i \in 0 \dots n-1, w_i \geq 0 \tag{IV.16}$$

La plus petite des valeurs propres est nulle ($w_0 = 0$) et a comme vecteur propre $v_0 = (1, 1, \dots, 1)$. Dans l'hypothèse considérée où le graphe est entièrement connecté, cette valeur propre nulle est unique, sinon, la multiplicité de cette valeur propre nulle est égale au nombre de sous graphes. Classons les valeurs propres par ordre croissant, et choisissons le vecteur propre associé à la première strictement positive w_1 (donc la seconde ou la plus petite des valeurs propres non nulles). La partition se fait selon le signe de la composante de ce vecteur propre associée à chaque nœud qui n'est jamais nulle : tous les nœuds correspondant à une composante positive d'un côté, tous ceux correspondant à une composante négative de l'autre. Si la taille du réseau est très grande, il peut être avantageux de ne pas calculer tous les vecteurs propres, car on en a besoin que d'un seul, et il existe des méthode permettant de ne calculer que ce deuxième vecteur propre, par exemple l'algorithme de Lanczos qui s'applique aux matrices creuses (ce qui est généralement le cas).

L'algorithme de partitionnement est donc le suivant :

1. Calcul de L matrice laplacienne du graphe G

2. Calcul des paires (w, v), respectivement valeurs propres et vecteurs propres de L
3. Rangement des paires (w_i, v_i) selon l'ordre des w_i croissants
4. Sélection de v_1 le second élément de v
5. Détermination de iv_{1p}, l'indice des composantes de $v_1 > 0$ et de iv_{1n}, l'indice des composantes de $v_1 < 0$
6. Construction de G_p, le sous graphe de G composé de ses nœuds iv_{1p} et de G_n, le sous graphe de G composé de ses nœuds iv_{1n}

Le temps de calcul pour cette méthode varie en $O(n^3)$, n étant le nombre de nœuds du graphe.

Résultats

L'algorithme du partitionnement spectral précédemment présenté a été appliqué sur le graphe représentant le réseau de l'UCTE première zone.

Lorsque l'on coupe le graphe UCTE première zone juste en deux parties, la coupure proposée suit à gros traits les frontières orientales de la France avec ses pays voisins. Elle commence le long de la frontière franco-belge puis continue vers le sud jusqu'aux frontières franco-suisse et franco-italienne comme on peut le voir sur la figure IV.6.

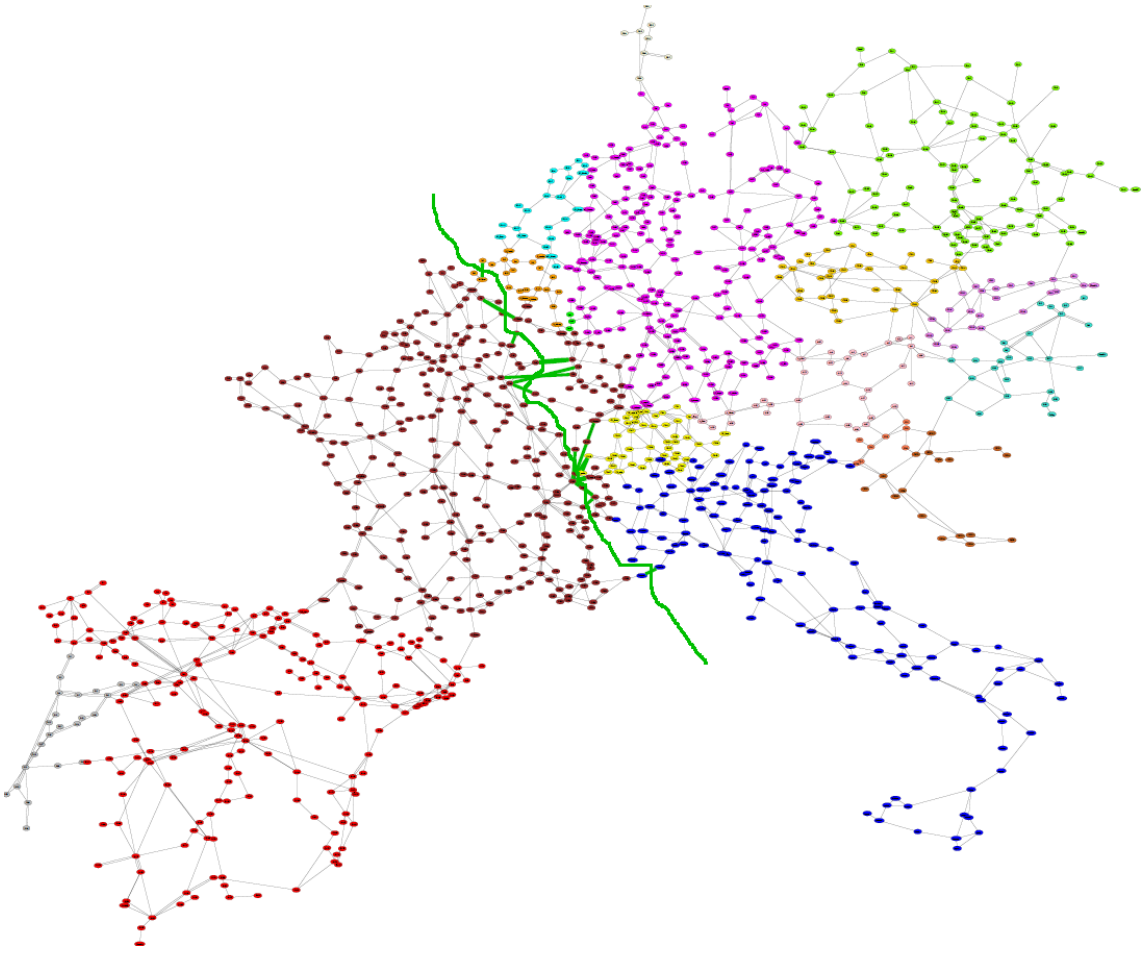

Fig. IV.6 – Coupure 1 du réseau de l'UCTE

Il a également été tenté d'utiliser la troisième valeur propre, autrement dit la seconde non nulle. Le graphe est alors coupé en trois parties. La première coupure se situe le long des Pyrénées, point de faiblesse bien connue du réseau UCTE pour les nombreuses congestions qui y ont lieu. La seconde commence au Nord à la frontière entre les Pays-Bas et l'Allemagne, continue direction sud-est pour traverser l'Autriche, passe entre la Hongrie et la Slovénie et traverse finalement la Croatie. Les coupures obtenues sont présentées par les traits verts sur la figure IV.7. Il se trouve que cette coupure correspond grossièrement à celle ayant effectivement lieu lors de la soirée du 4 novembre 2006 comme représenté figure I.3. L'utilisation de cette valeur propre est absolument non classique, mais il se trouve qu'elle propose des résultats intéressants.

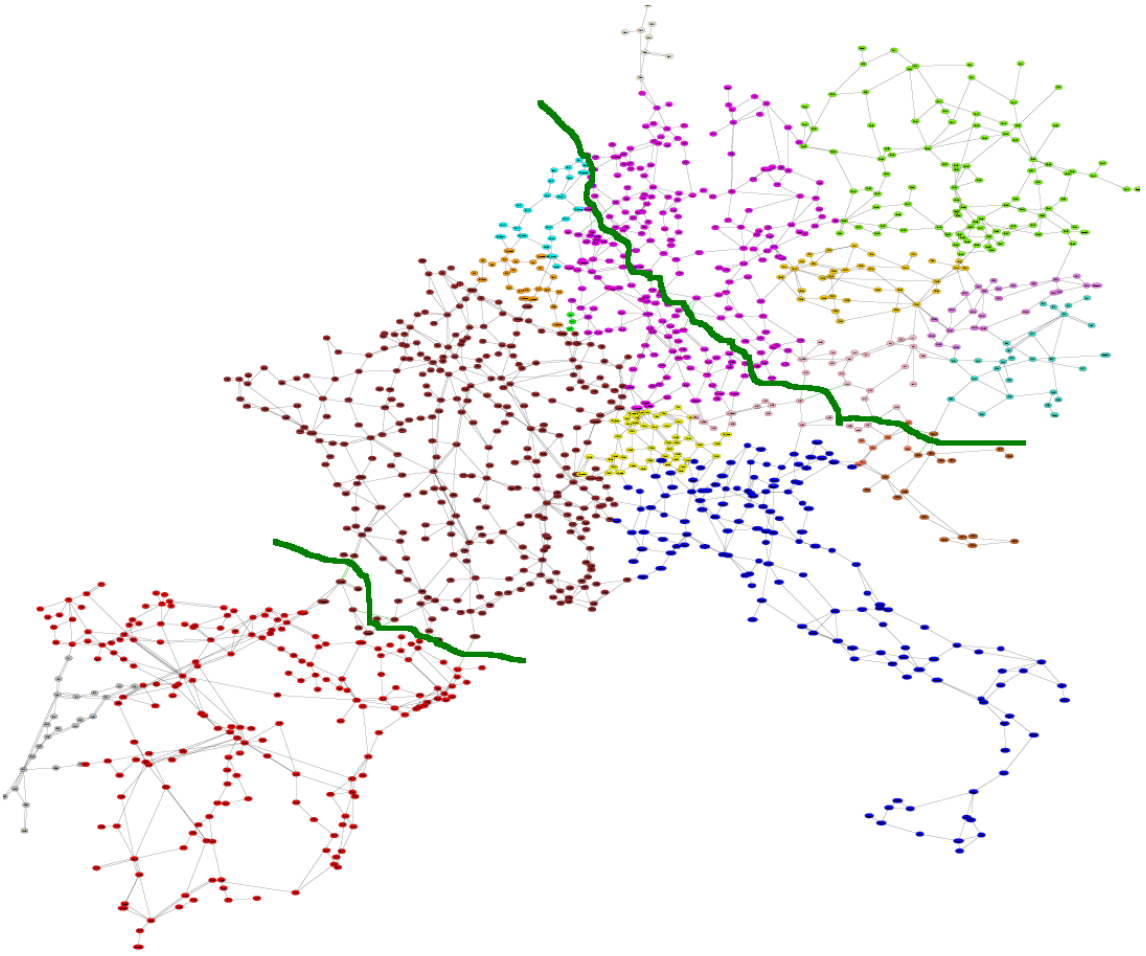

Fig. IV.7 – Coupure 2 du réseau de l'UCTE

Limites

Il existe plusieurs limites à cette méthode de partitionnement. La première vient de la définition même du réseau (UCTE) qui s'arrête à la première zone alors que l'infrastructure réelle est en fait bien plus grande. Comme la méthode consiste en la séparation du graphe en parties de tailles comparables, le choix des limites du réseau contraint le résultat.

Normalement, seule la première valeur propre non nulle est utilisée. Pour un parti-

tionnement en plus de deux parties, on applique la méthode de manière itérative sur les sous graphes. De fait, on obtient au final 2^n zones, n étant le nombre de fois où la méthode a été appliquée. En effet, toute structure un peu complexe ne se coupe pas en plus de deux parties distinctes à la fois (exemple de la feuille de papier soumises à n forces, elle ne se coupera d'abord qu'en deux parties distinctes). Mais si on ne connaît pas par avance le nombre de zones que l'on souhaite obtenir au final, cette méthode ne permet pas de déterminer le nombre d'étapes du processus itératif à effectuer. De plus, même si le partitionnement est à chaque étape effectué de façon optimal, rien ne garantit que le partitionnement final obtenu est lui globalement optimal.

IV.4.c Méthode de Girvan et Newman

Généralités sur le partitionnement hiérarchique

Le partitionnement hiérarchique peut être basé sur deux méthodes que sont la méthode par agglomération et la méthode par division. La méthode par agglomération consiste à partir des N nœuds et appliquer une série de fusion pour aboutir au graphe complet. À l'opposée, la méthode par division consiste à partir du graphe complet et à le séparer en groupes vers N parties. Le résultat peut être représenté sous forme d'arbre hiérarchique montrant les sous graphes à chaque étape de l'agglomération ou de la division selon la méthode employée. Un exemple d'arbre hiérarchique est présenté figure IV.8. Chaque trait horizontal représente une partie du graphe, les traits verticaux symbolisent une séparation en deux d'un sous graphe (ou une fusion) et les cercles à droite représentent les nœuds individuels. Toute section verticale comme celle avec le trait discontinu rouge permet de connaître le nombre de sous graphes actuels lors du processus ainsi que leurs composants. Cette figure représente un arbre pour une méthode par division, mais elle conviendrait aussi pour une méthode par agglomération en la lisant de droite à gauche.

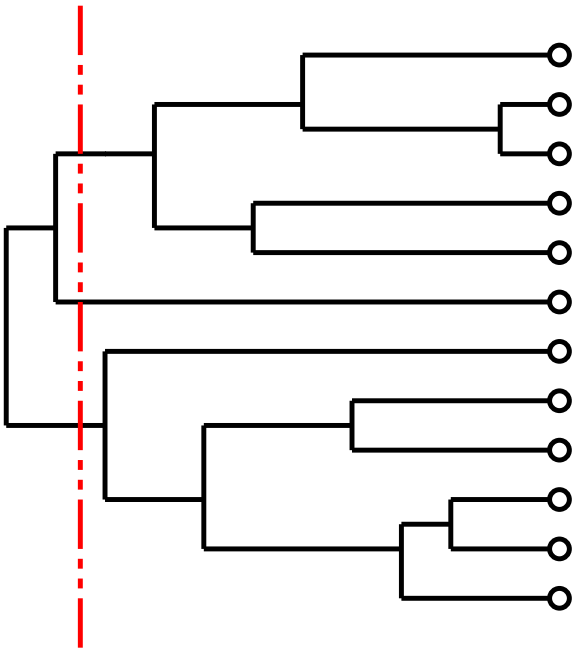

FIG. IV.8 – Exemple d'arbre hiérarchique

Les méthodes par agglomération sont plus traditionnellement utilisées, mais en général, elles posent le problème de laisser des nœuds seuls qui ne fusionnent que vers la fin du processus, phénomène n'ayant pas lieu avec les méthodes par division. En effet, il convient de noter que ces deux méthodes opposées par leur approche ne donnent généralement pas le même résultat lorsqu'elles sont appliquées à un même graphe [BLM+06].

Algorithme de Girvan et Newman

Cet algorithme a initialement été décrit dans l'article [GJ02] et approfondi dans [NG04]. Il est basé sur une méthode par division afin d'éviter le phénomène d'isolation des nœuds exposé dans la partie précédente. C'est une méthode itérative basée sur la suppression progressive des liaisons ayant la plus forte valeur de centralité d'intermédiarité jusque ce que le graphe se découpe en différents sous graphes. C'est-à-dire que le processus de suppression touche avant tout les liaisons rejoignant entre elles différentes communautés.

L'algorithme de Girvan et Newman est donc le suivant :

1. Calculer les coefficients de centralité d'intermédiarité pour toutes les liaisons du graphe ;
2. Supprimer la liaison ayant le coefficient le plus grand ;
3. Recalculer les coefficients pour toutes les liaisons restantes ;
4. Recommencer à l'étape 2 jusque ce que toutes les liaisons soient supprimées.

Recalculer les coefficients de centralité d'intermédiarité de toutes les liaisons affectées par la suppression à chaque pas est très gourmand en temps de calcul, d'autant plus que le graphe étudié est grand. Cela vient du fait qu'il est nécessaire de recalculer tous les chemins géodésiques à chaque étape. Néanmoins il apparaît que cette étape est vraiment très importante pour effectuer un bon partitionnement. Dans le pire des cas, le calcul des coefficients de centralité d'intermédiarité se fait en $O(ln)$ donc l'exécution de algorithme prend un temps $O(l^2n)$ ce qui donne $O(n^3)$ sur des graphes peu denses. Avec les moyens actuels de calculs, cette complexité conduit à se limiter à des graphes jusque maximum 10 000 nœuds. C'est la méthode la plus exigeante en terme de temps de calcul de toutes celles présentées dans ce mémoire.

Au final, on peut tracer un arbre hiérarchique pour représenter les résultats du processus de coupure. Pour ensuite choisir la meilleure division, un indice nommé modularité est calculé à chaque étape.

Modularité

L'indice de modularité est calculé à partir d'une matrice symétrique E de taille k, k étant le nombre de sous graphes réalisés. L'élément e_{ij} est la fraction de toutes les liaisons du graphe qui relient un nœud dans le sous graphe i à un autre nœud dans le sous graphe j. Pour ce calcul, on considère toutes les liaisons du graphe initial, même celles qui ont été supprimées lors du partitionnement. Ainsi :

e_{ii} est la fraction des liens internes à la communautés i ;

$\sum_i e_{ii} = Tr(E)$ est la fraction de liens internes à un sous graphe ($Tr(E)$ étant la trace de la matrice E) ;

$a_i = \sum_j e_{ij}$ est la fraction de liens connectés à la communauté i.
L'indice de modularité est alors défini tel que

$$Q = \sum_i (e_{ii} - a_i^2) = Tr(E) - \|E^2\| \tag{IV.17}$$

avec $\|E^2\|$ la somme des éléments de la matrice E^2. Q à pour valeur minimale 0 pour un partitionnement ne correspondant à aucune structure particulière et pour valeur maximale 1, mais cette borne maximale n'est pas accessible [NG04]. Une valeur élevée de la modularité indique que le partitionnement réalisé a détecté correctement les différentes communautés.

Il existe d'autres fonctions de quantification de qualité de partitionnement, mais celle-ci est actuellement la plus utilisée.

Résultats

L'algorithme a été appliqué sur le graphe de l'UCTE jusqu'à obtenir 182 sous graphes. En effet, la modularité étant globalement décroissante après une vingtaine de coupures, il est inutile d'effectuer les calculs jusqu'à la désintégration complète du graphe en 1254 parties de taille unitaire. Il est cependant utile de ne pas s'arrêter au premier maximum, car il peut arriver que celui-ci ne soit que local et suivi par un deuxième pic qui est le maximum global.

La variation de l'indice de modularité en fonction du nombre de coupures est présenté figure IV.9. Le maximum de la modularité est obtenu pour 21 coupures et vaut $Q_{max} = 0,8692$. Il est représenté par un trait vertical discontinu sur la figure.

Le partitionnement du graphe pour ce maximum est présenté sur la figure IV.10.

IV.4.d Partitionnement spectral étendu

Principe

Une possible extension à la bissection spectrale présentée précédemment dans la partie IV.4.b a été introduite dans l'article [DM04]. L'idée est d'utiliser non seulement la première valeur propre non nulle mais les D premières valeurs propres et leurs vecteurs propres associés. Contrairement à ce qui a été effectué dans la bissection spectrale, ici on utilise ces valeurs propres ensemble et non pas séparément. Ainsi, chaque nœud du graphe est représenté par un point dans un espace à D-dimensions. Les coordonnées de ce point correspondent aux composantes de ce nœud pour chaque vecteur propre. Une mesure de distance permet ensuite de dissocier les points. Plutôt que d'utiliser la distance euclidienne, il a été trouvé dans [DM04] qu'une distance angulaire, formée par l'angle entre deux vecteurs allant de l'origine aux points considérés, semble donner de meilleurs résultats. Ensuite, lorsque les distances entre chaque point sont calculées, il est procédé à un regroupement des points. Là encore, diverses possibilités sont envisageables pour définir la distance entre deux groupes de points. Elle peut être définie comme la valeur minimale de l'ensemble des distances entre deux points appartenant à chacun des groupes (*single linkage clustering*), la valeur maximale (*complete linkage clustering*) ou la moyenne (*group average clustering*). Pour l'instant, selon la littérature, aucune de ces méthodes

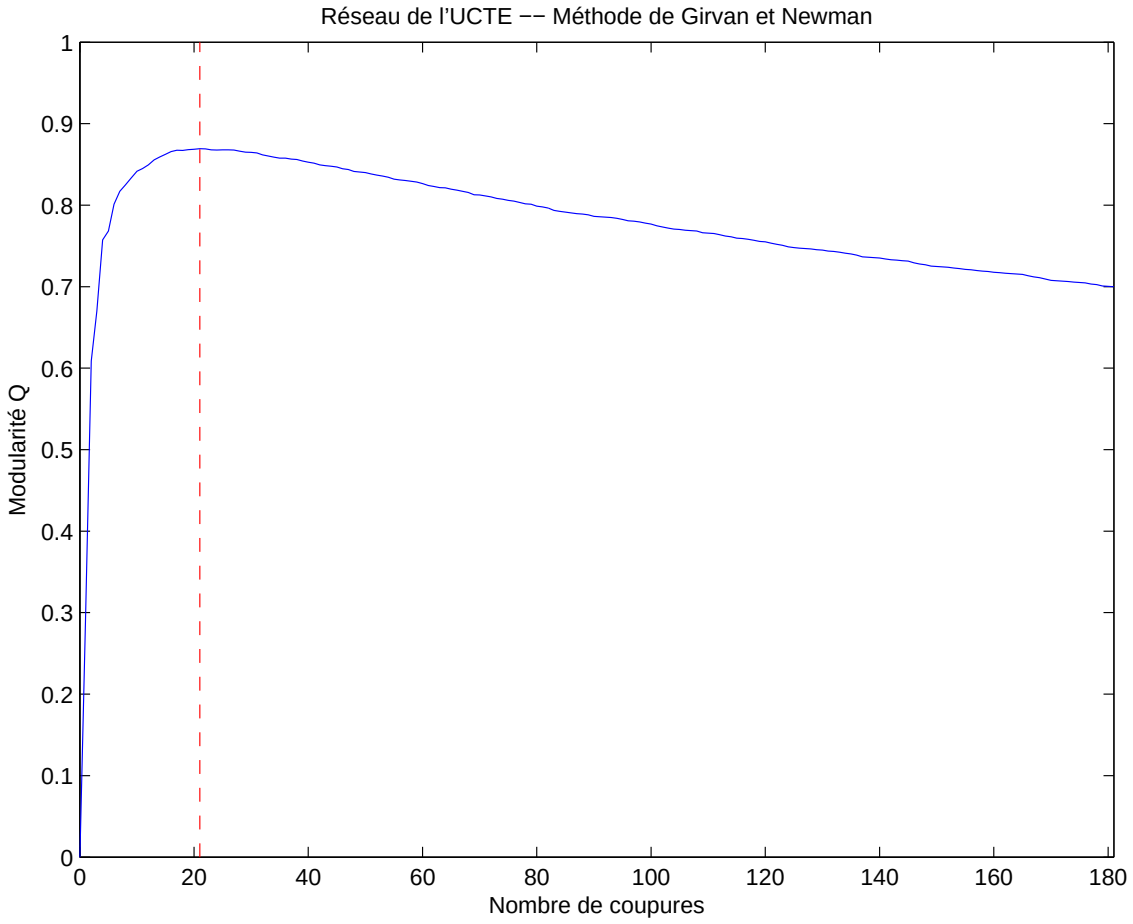

Fig. IV.9 – Courbe de variation de l'indice de qualité de la partition

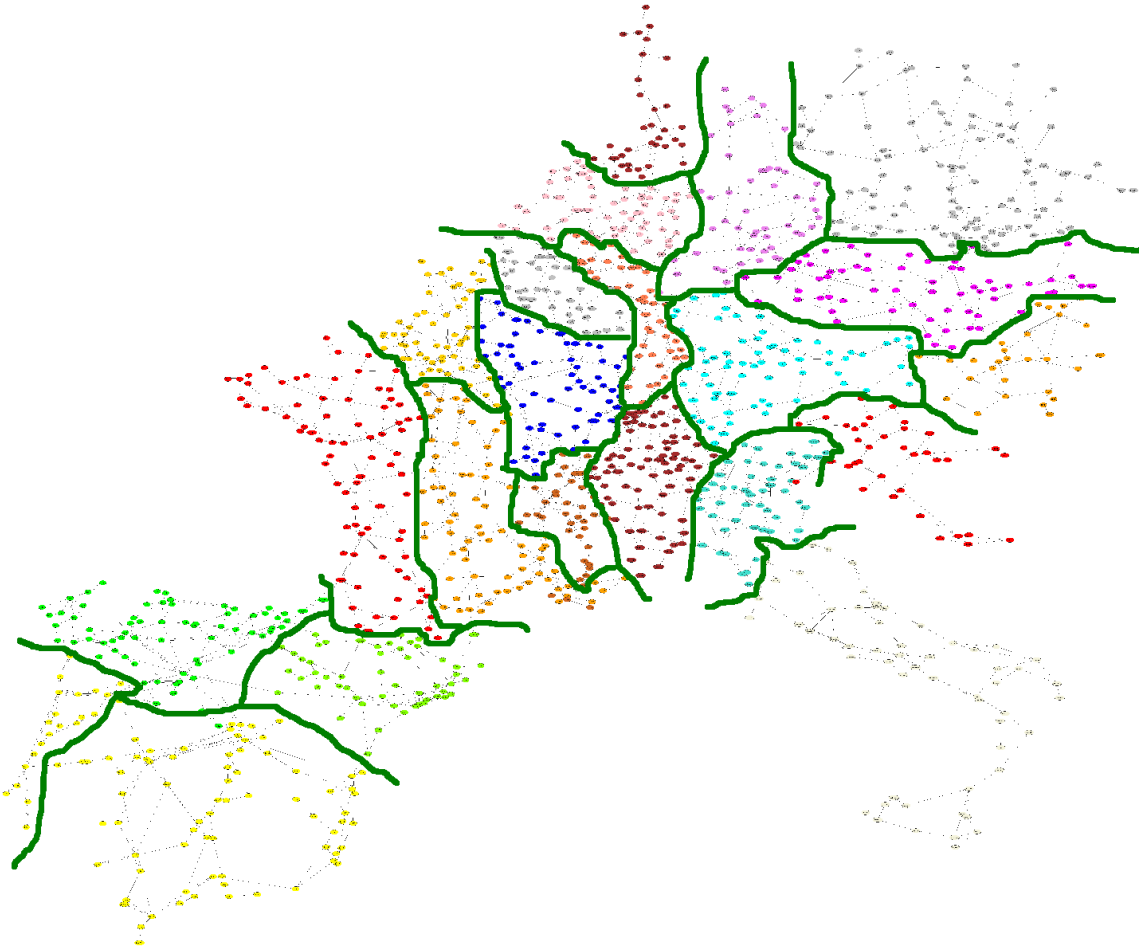

FIG. IV.10 – Partition du réseau de l'UCTE avec l'algorithme de Girvan et Newman

n'a été prouvée plus efficace que les autres. Cependant, la première possède l'inconvénient d'amener le regroupement de points éloignés entre eux, mais reliés par une chaîne d'intermédiaires. Le principe de regroupement consiste à joindre, petit à petit, les groupes de points ayant la distance la plus faible jusque aboutir à un seul groupe comprenant l'ensemble du graphe. Tout au long de ce processus, l'indice de modularité tel que défini pour la méthode précédente est utilisé pour quantifier la qualité du partitionnement et ainsi choisir la meilleure valeur pour la dimension D et le nombre optimal de groupes. Dans l'étude présentée, les trois méthodes de regroupement de points ont été testées.

De plus, il semblerait que l'utilisation du laplacien normalisé plutôt que le laplacien classique conduise à obtenir de meilleurs résultats en terme de coefficient de modularité sans que l'on sache pour l'instant en expliquer la raison [DM05].

Résultats

Tous les cas d'études ont été effectués avec le laplacien classique. La distance euclidienne a été testée jusqu'à la prise en compte de 20 vecteurs propres et la distance angulaire avec 2 vecteurs propres, car le calcul matriciel de la distance angulaire devient plus compliqué pour une dimension supérieure à deux. Pour chaque cas, l'ensemble des méthodes de regroupement présentées précédemment ont été testées.

Afin de visualiser la représentation des nœuds du graphe projetée dans l'espace des vecteurs propres, le tracé des points correspondant aux composantes des vecteurs propres pour le graphe de l'UCTE a été effectué. Chaque pays est représenté par une couleur distincte. La figure IV.11 représente le plan avec le deuxième vecteur propre en abscisse et le troisième en ordonnée et la figure IV.12 l'espace de dimension trois avec les vecteurs propres associés aux trois premières valeurs propres non nulles.

Les résultats obtenus pour tous les cas étudiés sont présentés dans le tableau IV.3.

Lorsque l'on prend en compte seulement 2 vecteurs propres, la distance euclidienne permet d'obtenir de meilleurs résultats (au sens coefficient de modularité) que la distance angulaire. D'une manière générale, le regroupement des groupes de points par minimum de distance est moins bon que les deux autres. Le meilleur résultat pour le regroupement par maximum de distance est obtenu avec 8 vecteurs propres, le graphe obtenu étant composé de 29 sous graphes et le coefficient de modularité valant $Q_{max} = 0,8521$. Mais le meilleur résultat pour le partitionnement spectral étendu a été obtenu avec le regroupement utilisant la moyenne des distances et la prise en considération de 14 valeurs propres. On obtient alors 25 sous graphes et $Q_{max} = 0,8656$. Le partitionnement correspondant est représenté figure IV.13. Chaque sous-graphe est représenté par un couple symbole/couleur différent (les couleurs ne correspondent plus aux différents pays comme précédemment).

Dans tous les cas, cette méthode a donné de moins bons résultats que l'algorithme de Girvan et Newman (rappel $Q_{max} = 0,8692$, figure IV.9).

IV.4.e Limites générales au partitionnement de graphe

Trois méthodes différentes permettant d'effectuer le partitionnement d'un graphe, chacune avec ses avantages et ses limites ont été présentées. D'une manière générale, on peut s'interroger sur les limites du partitionnement en tant que tel, c'est-à-dire indépendamment de la méthode utilisée pour l'effectuer.

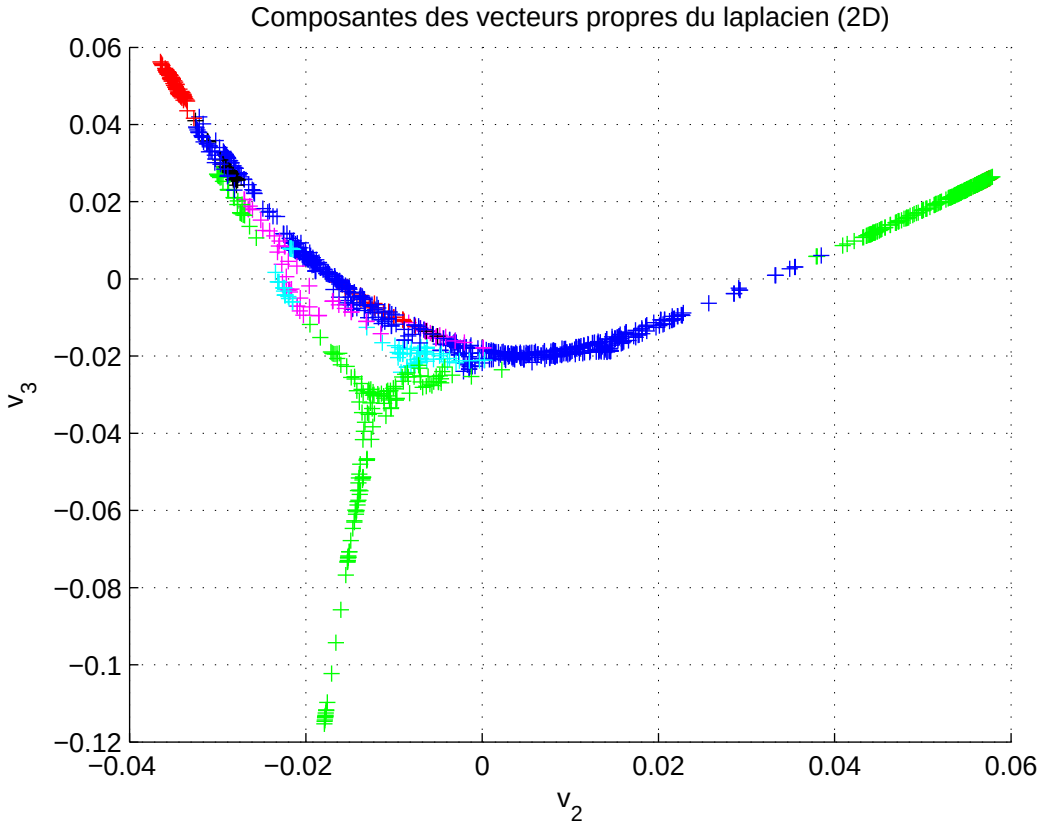

FIG. IV.11 – Projection dans le plan v2/v3

Tab. IV.3 – Valeur de la modularité Q et nombre de zones final en fonction du nombre de vecteurs propres utilisés et du mode de calcul de distance pour différentes méthodes d'agglomération des points

nombre de vecteurs propres	*single linkage clustering*	*complete linkage clustering*	*group average clustering*
2 angulaire	0,67398 ; 20	0,80963 ; 42	0,799282 ; 23
2 euclidien	0,70124 ; 135	0,8275 ; 29	0,83064 ; 28
3 euclidien	0,69747 ; 116	0,84102 ; 27	0,84909 ; 27
4 euclidien	0,71774 ; 127	0,83879 ; 31	0,84538 ; 28
5 euclidien	**0,72935 ; 84**	0,84409 ; 29	0,84796 ; 41
6 euclidien	0,70761 ; 126	0,83841 ; 21	0,84548 ; 44
7 euclidien	0,68136 ; 126	0,85075 ; 29	0,85702 ; 39
8 euclidien	0,69223 ; 120	**0,85205 ; 29**	0,84955 ; 44
9 euclidien	0,56685 ; 105	0,84821 ; 36	0,84926 ; 31
10 euclidien	0,46805 ; 76	0,85087 ; 24	0,85737 ; 23
11 euclidien	0,45163 ; 105	0,85038 ; 37	0,85805 ; 31
12 euclidien	0,62103 ; 126	0,84621 ; 22	0,86244 ; 25
13 euclidien	0,61041 ; 119	0,84509 ; 27	0,86159 ; 26
14 euclidien	0,48208 ; 121	0,84182 ; 28	**0,86563 ; 25**
15 euclidien	0,45831 ; 96	0,85034 ; 35	0,86192 ; 30
16 euclidien	0,44793 ; 112	0,84871 ; 36	0,85766 ; 23
20 euclidien	0,6057 ; 126	0,85788 ; 33	0,86165 ; 31

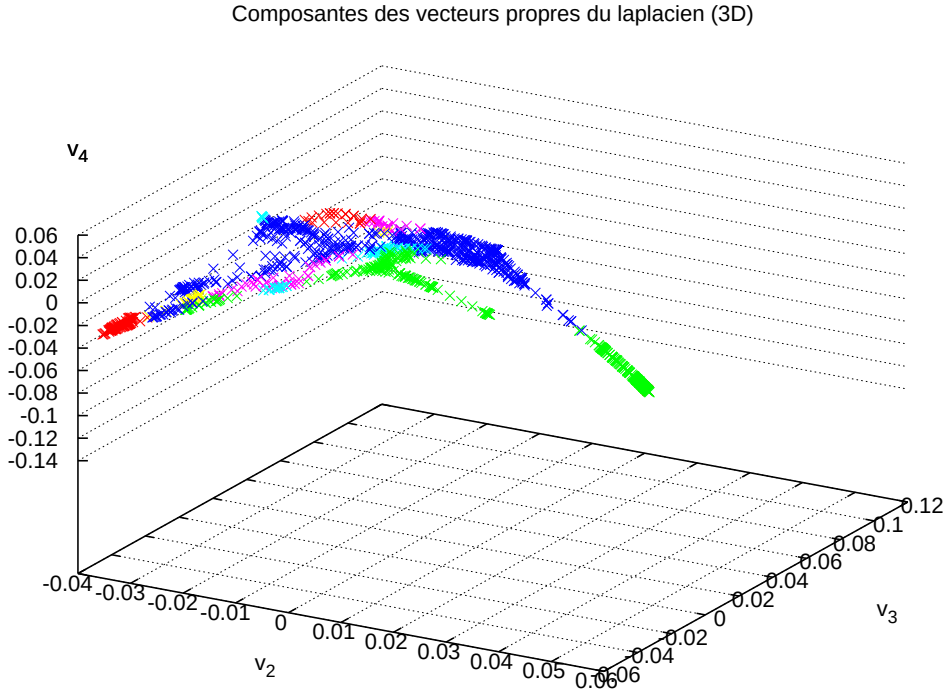

FIG. IV.12 – Projection dans l'espace v2/v3/v4

Une des limites de l'étude réalisée provient de la définition du réseau auquel les méthodes ont été appliquées. En effet, seule une partie du réseau de l'UCTE a été étudiée. Comme le partitionnement consiste à couper le graphe en sous graphes de taille équivalente, le choix des limites du cas d'étude provoque le résultat obtenu.

Lorsque l'on prend la plus grande valeur de l'indice de modularité, les deux dernières méthodes présentées découpent le graphe en de très nombreuses parties, ce qui est l'effet recherché dans des études de partitionnement de certains domaines tels que la sociologie ou la biologie. Mais lorsque le graphe étudié est, comme ici, un réseau électrique, l'intérêt est plus limité. En effet, les séparations observées suites à des perturbations comme celle du 4 novembre 2006 ne produisent que quelques zones distinctes viables (trois pour celle de 2006). On peut donc s'interroger sur l'utilisation possible de ces méthode dans une visée de prévision des lignes de faiblesse.

Par essence, celui-ci ne se fonde que sur des critères purement topologiques. Par contre, il est possible de quantifier les dégâts sur le réseau électrique en calculant les capacités de production et les demandes de consommation sur les sous graphes connectés restant et ainsi voir si l'équilibre peut être réalisé. De plus, ce partitionnement est purement statique, c'est-à-dire que les phénomènes dynamiques ne sont pas pris en considération [Fon08] [Pha06]. Une autre limite, importante par rapport à la problématique de modélisation des interdépendances des infrastructures critiques, est que cette méthode est bien applicable à une infrastructure seule. Cependant, son utilisation sur un graphe modélisant plusieurs infrastructures peut poser problème si le couplage entre les infrastructures est faible, car alors, les coupures se situeront a priori aux frontières. Ce problème ne se pose pas, si la

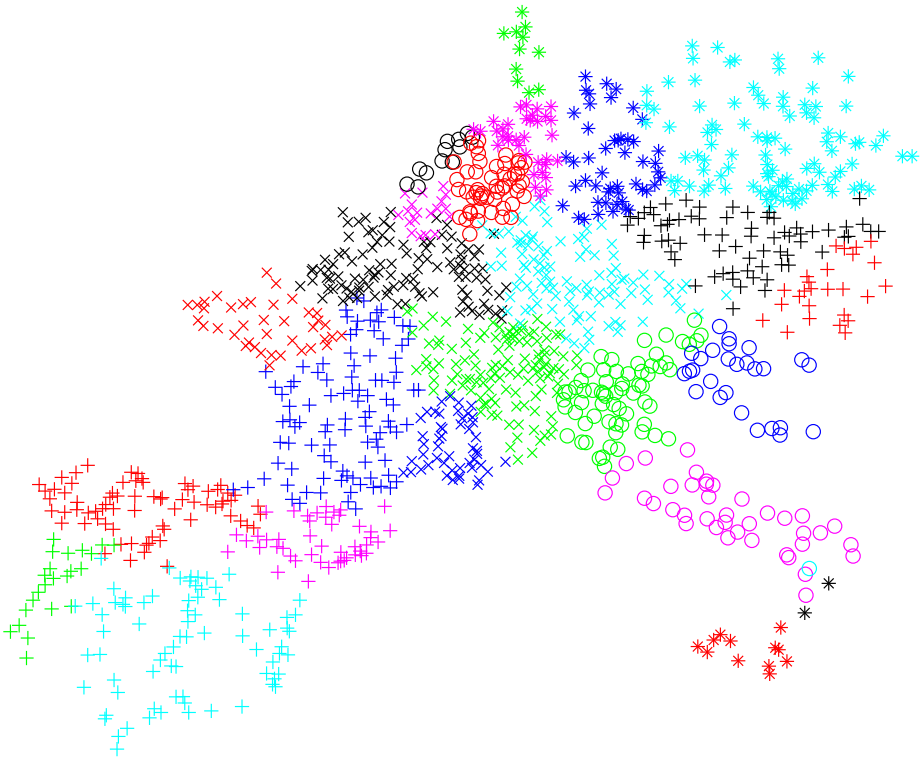

Fig. IV.13 – Partitionnement spectral étendu à 14 vecteurs propres du réseau de l'UCTE avec regroupement par moyenne des distances

modélisation aboutit à un graphe où les réseaux sont entremêlés ou imbriqués fortement l'un dans l'autre.

IV.5 Robustesse statique

IV.5.a Objectif

La robustesse statique du graphe à la suppression d'éléments permet une quantification de la résistance (et par conséquent de la vulnérabilité) de l'infrastructure étudiée par rapport aux pannes, qu'elles soient d'origine accidentelle ou intentionnelle (autrement appelées attaques). Cette étude peut également permettre d'identifier les composants les plus vulnérables du réseau et donc de mieux les protéger. Par exemple, pour certaines topologies de graphes, il a été observé que les nœuds de plus fort degrés sont les plus vulnérables. Partant de ce constat, on peut renforcer prioritairement la protection des sites correspondant à ces nœuds comparativement au reste du réseau.

IV.5.b Méthode

La méthode consiste simplement à supprimer un à un les différents nœuds du graphe et à observer au fur et à mesure de ce processus l'évolution d'une grandeur caractéristique telle que le nombre de nœuds du plus grand élément connexe, son diamètre ou sa distance moyenne.

Dans le cas de l'évaluation de la vulnérabilité aux pannes accidentelles, le choix des nœuds à supprimer se fait de manière aléatoire. Tandis que pour la vulnérabilité vis à vis des attaques ciblées, la suppression des nœuds est faite en utilisant une stratégie déterministe. Dans la littérature, plusieurs méthodes pour la sélection de l'ordre de suppression des nœuds sont adoptées. Celle-ci peut se faire par ordre décroissant de degré ou de charge. La méthode de calcul de la charge aux nœuds utilisée est celle de Brandes (décrite dans [Bra01]), mais on pourrait également utiliser celle de Newman (décrite dans [New01]). Ces algorithmes calculent la fraction du nombre de chemins les plus courts qui passe à travers le nœud considéré. Ce classement peut être réalisé une seule fois sur le graphe initial pour tout le processus ou être réactualisé après chaque suppression. Dans ce cas, seul le premier élément à chaque pas est considéré pour être supprimé.

IV.5.c Choix de l'indicateur

La taille du plus grand élément connexe du graphe est directement représentative de la taille de l'infrastructure qu'il modélise. Si cette taille est strictement inférieure au nombre de nœuds restant dans le graphe, cela signifie qu'il existe des nœuds non connectés à l'élément principal. L'impact de la panne est d'autant plus important que la différence entre le nombre de nœuds restant et la taille du plus grand élément connexe est grande. Pour un réseau électrique, en prenant comme hypothèse que tous les nœuds sont consommateurs, la taille du réseau permet de quantifier le nombre d'utilisateurs affectés qui serait alors proportionnel au nombre de nœuds déconnectés.

Le diamètre et la distance moyenne peuvent être interprétés comme un des paramètres de l'efficacité du réseau. Un faible diamètre ou une faible distance moyenne relativement

à la taille du graphe signifie que le réseau est topologiquement efficace pour transmettre d'un point à un autre de l'information ou de l'énergie selon l'infrastructure considérée. À l'inverse, un diamètre proche du nombre de nœud du graphe indique une plus mauvaise efficacité dans la transmission. Ainsi, comme montré sur la figure IV.14 un graphe de 4 nœuds complet, c'est-à-dire dont les nœuds sont tous connectés avec tous les autres, aura un diamètre de 1 et sera topologiquement plus efficace qu'un graphe de 4 nœuds en ligne ayant un diamètre de 3 et qui aura donc une robustesse moindre. En effet, une plus longue distance à parcourir pour le transport de l'énergie signifie plus de pertes tandis que pour le transport de l'information cela est synonyme de latence plus élevée. Cependant, ces mesures sont fortement dépendantes de la taille du graphe, autrement dit lorsque la taille du graphe décroît du fait de la suppression de nœuds, il est normal que le diamètre et la distance moyenne diminuent, sans pour autant impliquer une meilleure efficacité du réseau.

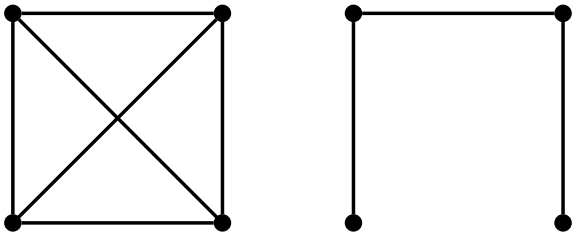

Fig. IV.14 – Deux graphes de 4 nœuds

IV.5.d Résultats déjà connus

Il a été montré (entre autre [BBV06]) (empiriquement, par simulation et aussi analytiquement) que les réseaux sans-échelle (c'est-à-dire dont la loi de distribution des degrés suit une loi de puissance) ont, par nature, une grande résistance aux pannes, c'est-à-dire retrait aléatoire de nœuds du graphe mais également une grande fragilité envers les attaques ciblées sur les nœuds les mieux connectés. Ceci est dû au fait que les pannes aléatoires touchent plutôt les nœuds faiblement connectés car ils sont en plus grand nombre alors que la suppression des quelques nœuds les plus connectés, donc les plus centraux, conduit rapidement à une désintégration du graphe.

Analytiquement, il a été démontré qu'il existe une valeur critique f_c telle que le graphe est considéré détruit lorsque $f > f_c$, f étant la fraction de nœuds du graphe ayant été retiré. En considérant certaines hypothèses non détaillées ici (se référer à [BBV06]), cette valeur est :

$$f_c = 1 - \frac{< k >}{< k^2 > - < k >} \tag{IV.18}$$

$< k^2 >$ étant le moment d'ordre 2 de la densité de probabilité des degrés : $< k^2 >= \sum_k k^2 p_k$. Dans les réseaux sans échelle, cette valeur est très grande et donc f_c est proche de 1 ce qui donne une excellente robustesse aux pannes aléatoires. Dans le cas étudié, $f_c = 0.6620$, c'est-à-dire il faudrait théoriquement supprimer 830 nœuds pour désintégrer ce graphe s'il était sans-échelle.

Une comparaison de la robustesse aux pannes et aux attaques pour les graphes à distribution de degré exponentielle et les graphes sans échelles est effectuée dans [DM01]. On

peut observer que les deux graphes possèdent des propriétés de résistance bien différentes. Une fraction critique existe pour les graphes à distribution de degré exponentielle et est identique pour les pannes et pour les attaques. En fait, les effet de ces deux types de dommages sont très similaires pour ces graphes. En ce qui concerne les graphes sans-échelles, la fraction critique est plus basse pour les attaques mais n'existe pas pour les pannes aléatoires. Ce type de graphe est donc plus vulnérable aux attaques mais possède une résistance bien accrue aux pannes. Le graphe que l'on étudie étant inclus dans la première catégorie, on s'attend par conséquent à avoir des résultats proches pour les pannes et les attaques, c'est à dire une taille décroissante vers 0 jusque la fraction critique et y restant ensuite et une distance moyenne croissante jusqu'à la fraction critique.

IV.5.e Résultats obtenus pour le graphe d'étude

La figure IV.15 présente les résultats obtenus pour une suppression d'éléments type pannes aléatoires. Trois grandeurs caractéristiques sont tracées : la taille du plus grand élément, son diamètre ainsi que la distance moyenne. Ces grandeurs sont les moyennes obtenues pour dix réalisations. L'abscisse correspond au nombre de nœuds supprimés. On peut observer qu'il suffit d'enlever entre 200 et 450 nœuds pour complètement désintégrer le graphe. La fraction critique théorique donnait 830 nœuds, on observe donc en pratique une valeur plus faible.

La figure IV.16 présente une comparaison des résultats entre pannes aléatoires et attaques ciblées appliquées au graphe d'étude. Les méthodes utilisées pour les attaques ciblées sont le classement des nœuds par charge et par degré décroissant à partir de la répartition initiale (sans la recalculer) et en refaisant ce classement après chaque suppression.

La taille du plus grand élément est par nature toujours inférieure ou égale au nombre de nœuds initiaux soustrait du nombre de nœuds supprimés. Cette grandeur est strictement inférieure lorsque les nœuds du graphe ne sont plus tous connectés entre eux mais que le graphe s'est scindé en sous graphes. La modélisation des attaques détruisant le plus rapidement le graphe est celle basée sur la charge des nœuds recalculée après chaque suppression (charge signifiant ici coefficient de centralité d'intermédiarité), suivie par celle éliminant les nœuds par ordre de degrés. La mise à jour des degrés après suppression n'apporte qu'une faible amélioration de l'efficacité de l'attaque, contrairement à l'attaque basée sur les charges qui devient moins destructrice si on se base seulement sur l'ordre initial. Toutes les attaques détruisent plus rapidement le graphe que les pannes aléatoires. Il a également été étudié les attaques inverses, c'est-à-dire basées sur la suppression des nœuds ayant la plus faible charge ou le plus petit degré. Ce type d'attaque est bien moins destructeur que les pannes aléatoires. Ces résultats confirme l'importance des nœuds ayant le plus fort degré ou la plus forte charge pour la cohésion du graphe et à l'inverse la moindre importance de ceux ayant la charge la plus faible ou le degré le plus petit.

Les évolutions du diamètre et de la distance moyenne montrent les mêmes résultats que la taille avec le pic apparaissant en premier pour l'attaque sur les charges recalculées et en dernier pour les pannes aléatoires. De plus, la courbe représentant les pannes aléatoires est située au dessus de toutes les autres, preuve de sa moins grande capacité destructrice.

D'un point de vue temps de calcul, seuls les calculs de la charge (dans le cas d'attaques

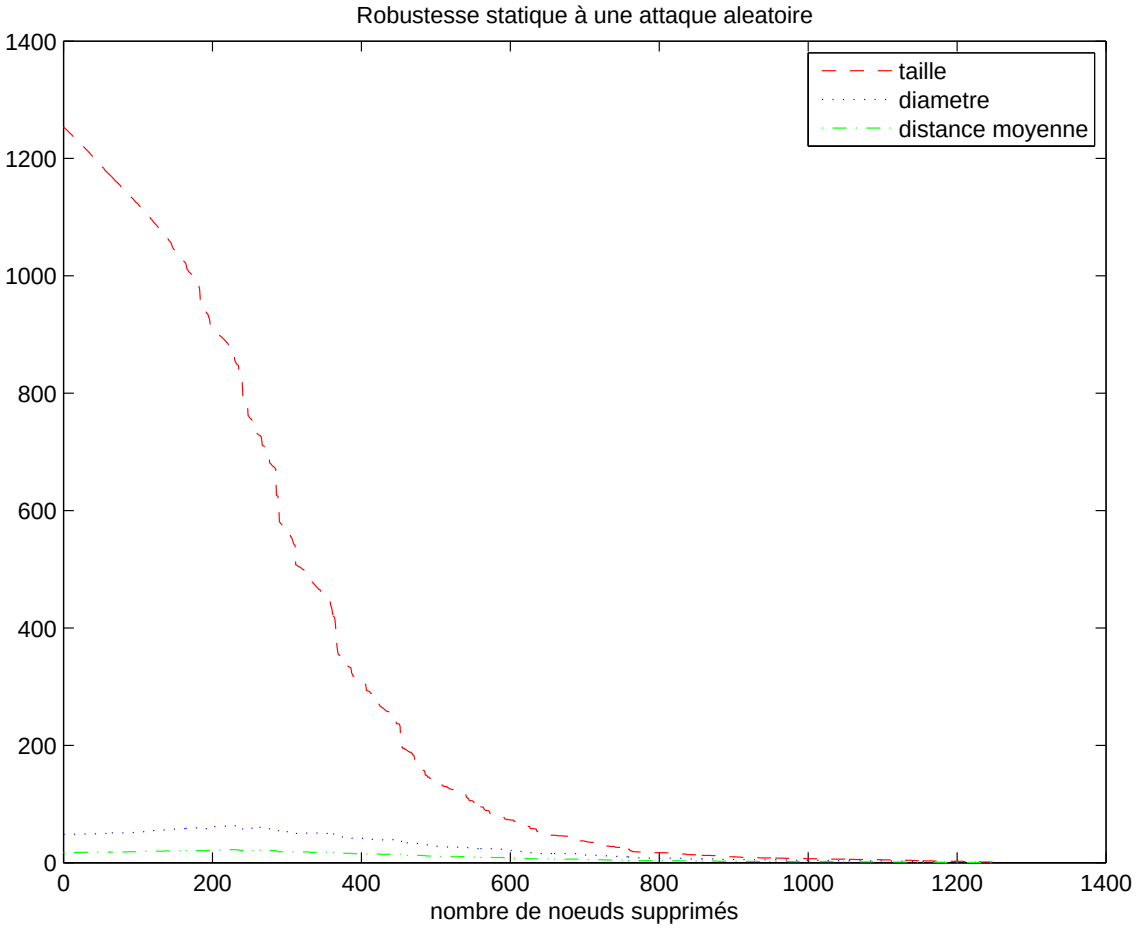

Fig. IV.15 – Robustesse statique du graphe aux pannes aléatoires (moyenne sur 10 réalisations)

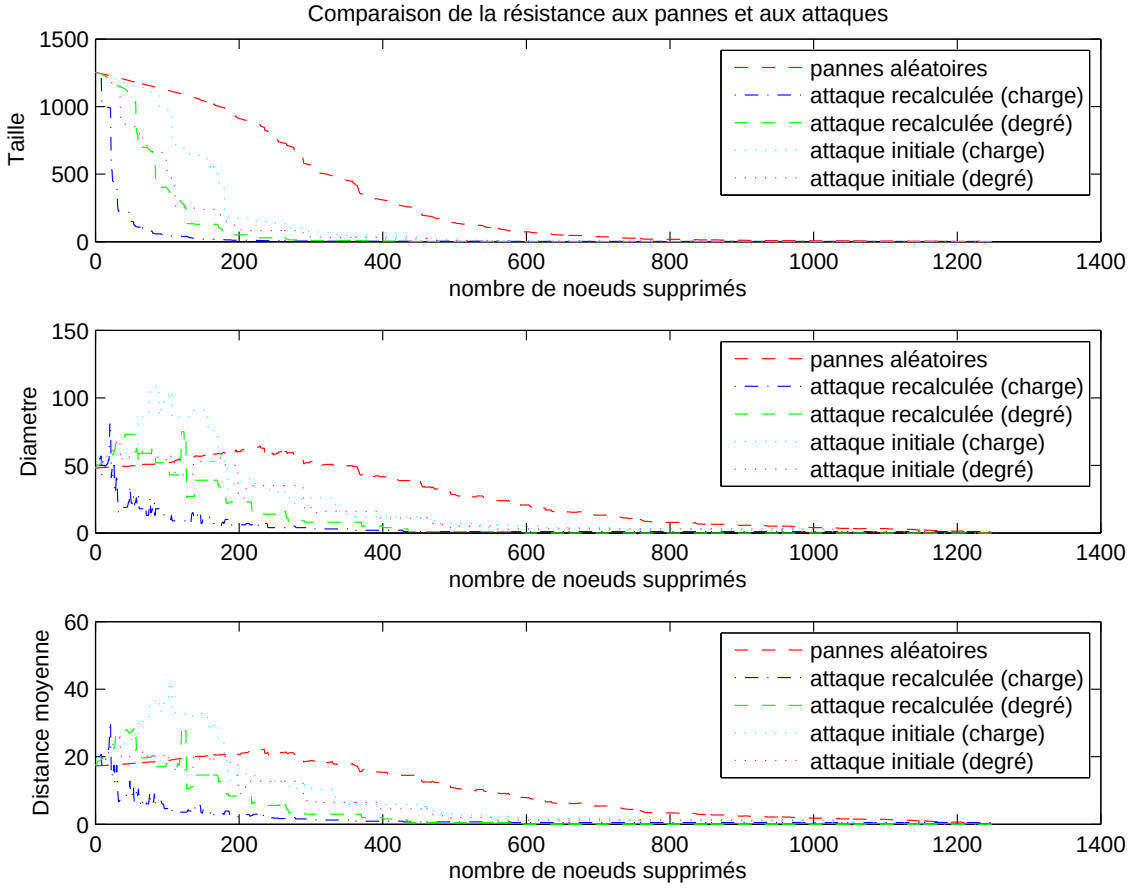

FIG. IV.16 – Robustesse statique du graphe à la suppression de nœuds

basées sur la charge des nœuds) et ceux du diamètre et de la distance moyenne du graphe après chaque suppression sont longs. Ceci est dû au fait qu'ils nécessitent de calculer l'ensemble des chemins géodésiques. On pourrait réduire ce temps sur le calcul de la distance moyenne en n'effectuant une approximation consistant à calculer cette moyenne sur la distance seulement entre certains nœuds choisis aléatoirement ou en n'utilisant simplement que la taille de la plus grande composante connexe comme indicateur.

L'étude sur la suppression des nœuds peut également être effectuée sur les liaisons en se basant sur le critère de centralité d'intermédiarité de liaison, c'est-à-dire le nombre de fois que la liaison considérée est sur un chemin géodésique pour tous les nœuds du graphe. Ce type d'attaque est entre autres étudié dans [LMN04]. De même, il est montré dans [CSCW07] qu'un indice de centralité d'intermédiarité des lignes pondérées peut permettre d'identifier les lignes les plus critiques d'un réseau. Cette étude se rapproche alors du partitionnement selon la méthode de Girvan et Newman où en enlevant petit à petit les 13 liaisons ayant le plus fort coefficient de centralité d'intermédiarité, le graphe se coupe en deux et en enlevant 144 liens, soit seulement 8% des liens du graphes, celui ci est alors composé de 22 sous parties.

Les courbes de la figure IV.17 présentent les résultats obtenus. La courbe en trait plein correspond à des retraits aléatoires de lignes, celle avec des tirets à la suppression de la ligne possédant la plus forte charge, celle avec des traits mixtes également mais en utilisant seulement le calcul initial des charges. Les deux courbes en pointillés (non indiquées dans la légende par clarté) correspondent au retrait de la ligne la moins chargée suivant la répartition initiale ou avec mise à jour. Les résultats pour l'attaque avec mise à jour après chaque suppression de sa charge confirment la constatation précédente liée au partitionnement selon la méthode de Girvan et Newman où peu de suppression de liens suffit pour scinder le graphe en différentes parties.

On peut remarquer que l'attaque sur les liens a des effets similaires sur le graphe d'étude que la meilleure attaque sur les nœuds. Le constat est identique pour les pannes aléatoires. Là encore, le calcul des charges à chaque étape permet d'améliorer l'efficacité de l'attaque. La suppression des liens les moins chargés fait moins de dégâts que les pannes aléatoires. Ce type de suppression permet au réseau de ne pas se scinder en différents sous graphes lors de ce processus et donc d'avoir un diamètre et une distance moyenne qui restent quasiment constant jusqu'à une suppression de 80% des lignes.

IV.5.f Extensions possibles

Une extension possible à cette étude est de choisir un autre indicateur que les trois classiquement utilisés pour évaluer l'impact de l'attaque sur le graphe. Comme exemple d'indicateur, l'efficacité globale du graphe est utilisée dans [CLM04b]. Dans [Sun05] est définit et utilisé le dommage :

$$D = \frac{E_{glob}(G_0) - E_{glob}(G_f)}{E_{glob}(G_0)} \tag{IV.19}$$

$E_{glob}(G)$ étant l'efficacité globale du graphe G (définie dans la première section de ce chapitre). Cet indicateur doit lui aussi être calculé après chaque suppression de nœud, conduisant à une surcharge de calcul pour les grands graphes. Dans la modélisation proposée au chapitre suivant, on utilisera la puissance non fournie aux consommateurs.

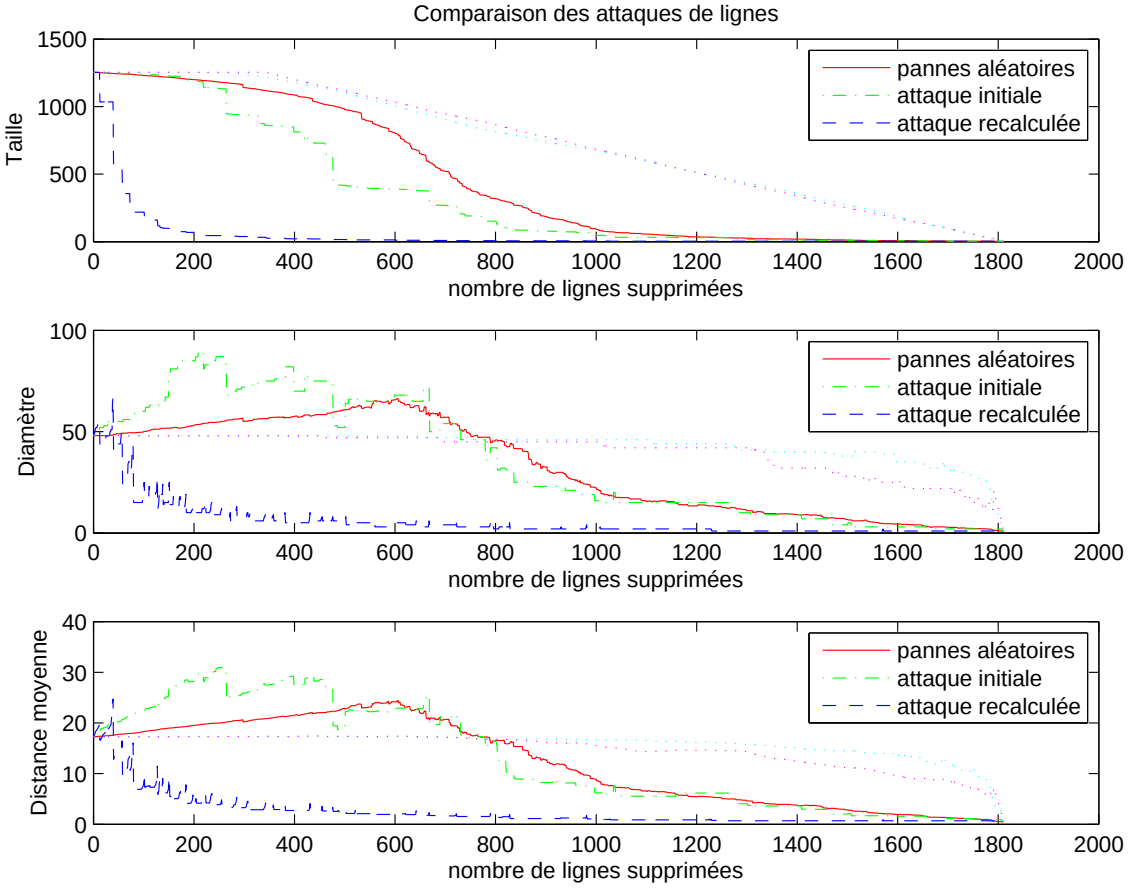

FIG. IV.17 – Robustesse statique du graphe à la suppression de lignes

Une limite à cette méthode d'évaluation de la robustesse est que c'est une méthode dite statique, c'est-à-dire qu'elle ne prend pas en compte les phénomènes de nature dynamique. Pour la dépasser, une autre méthode a été introduite où sont modélisés les effets de cascade.

IV.6 Cascade mono-infrastructure

IV.6.a Objectif

Dans ce chapitre, le mot cascade ne doit pas être pris dans le sens défini au chapitre 1 pour les défaillances multi-infrastructures, mais dans un sens réduit ou une défaillance initiale va en provoquer plusieurs autres dans la même infrastructure et ainsi de suite. Ce type d'étude peut permettre de comprendre les conditions permettant à un incident initial de petite taille de conduire à une panne à grande échelle, phénomène que ne peut pas expliquer la modélisation précédente. De plus, l'étude et la compréhension plus approfondie de ces phénomènes de cascade devrait permettre d'aider à développer des mesures de contre-réaction pour les éviter ou du moins limiter leurs conséquences.

IV.6.b Méthode

Le principe de la modélisation de la cascade de surcharge est le suivant. Chaque élément est doté d'une capacité fixée qui correspond à la charge maximale que l'élément peut supporter. Celle-ci est calculée en prenant la charge initiale de l'élément considéré et en la multipliant par un coefficient de tolérance (ou de surdimensionnement) $1 + \alpha$ que l'on choisi généralement entre 1 et 2, typiquement $1,10$. Ce facteur correspond au coefficient de sécurité en mécanique. Ainsi, à l'instant initial, le taux de charge ou taux d'utilisation vaut

$$\frac{1}{1+\alpha} \tag{IV.20}$$

Le calcul de la charge des nœuds s'effectue selon les mêmes méthodes que décrites précédemment dans la partie IV.5.b. Ensuite, on enlève un élément du graphe et l'on recalcule les charges de tous les éléments restants. Si suite aux reports de charge provoqué par la suppression de l'élément, la charge à un nœud dépasse sa capacité propre alors celui-ci est également supprimé. Ainsi, plusieurs nœuds peuvent être supprimés lors d'une seule étape. Les charges des éléments sont alors recalculés et ainsi de suite jusqu'à ce qu'aucune nouvelle surcharge n'intervienne dans le réseau. Le phénomène peut soit s'arrêter rapidement en restant localisé à une région du graphe soit se propager (phénomène d'avalanche ou effet dominos). L'algorithme de cette modélisation de cascade est donc le suivant :

1. Calcul de la capacité pour chaque élément
2. Suppression de l'élément déclencheur
3. Calcul des nouvelles charges des éléments
4. Si la charge dépasse la capacité pour des éléments
   (a) Suppression des éléments dont la charge est supérieure à la capacité
   (b) Retour à 3.
5. Fin

Ce processus dépend fortement de l'élément déclencheur, c'est-à-dire du premier élément supprimé. Ainsi, pour évaluer la résistance d'un réseau aux effets de cascade, on teste les différentes cascades possibles à partir de tous les éléments (initiateurs) du graphe. Cette étude systématique, que l'on appelle $N-1$ permet également de déterminer les éléments les plus critiques quant au déclenchement de ce phénomène. Cette modélisation du phénomène de cascade est par exemple décrite dans [LMN04] et dans [ML02].

IV.6.c Résultats

Les résultats obtenus de cette étude de cascade sont synthétisés dans la figure IV.18. Par concision, seule les valeurs extrêmes et moyenne de la taille finale du graphe sont indiquées.

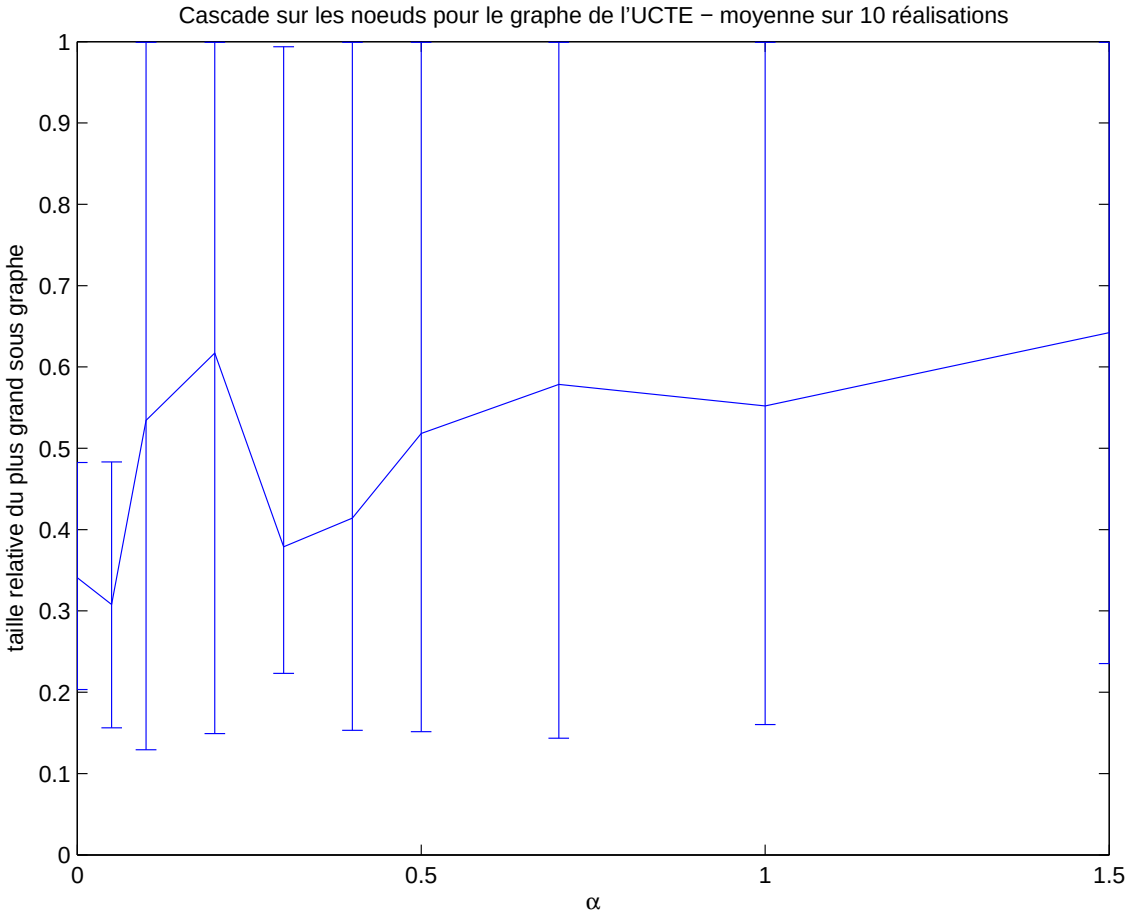

FIG. IV.18 – Évolution de la taille en fonction du coefficient de tolérance

En abscisse, évolue le coefficient α représentant la tolérance admise (c'est-à-dire que la charge maximale est calculé en multipliant la charge initiale par un facteur $1+\alpha$) tandis qu'en ordonnée est représentée la taille du plus grand sous graphe final normalisée par la taille du graphe initial. Ainsi une valeur de 1 signifie que le réseau ne s'est pas scindé tandis que plus la valeur est petite, plus le réseau s'est partitionné. On remarque que pour les deux valeurs de α inférieures à $0,1$ ($0,05$ et 0), la tolérance est tellement faible que tout défaut initial quelque soit le nœud provoque un partitionnement. En pratique, ce

facteur possède bien évidemment une valeur supérieure. Inversement, plus ce coefficient de tolérance est important, moins il y aura d'effet de cascade et plus la taille finale du graphe sera importante. Ce résultat correspond à ce que l'on pouvait attendre intuitivement.

Les nœuds de départ de la cascade ont été choisis aléatoirement. Mais comme pour l'étude de robustesse, on peut choisir le nœud de départ pour simuler une attaque, par exemple celui le plus chargé ou ayant le degré le plus important.

IV.6.d Bilan et extensions possibles

Là encore, plusieurs extensions à cette étude sont possibles. Ces variantes n'ont pas été étudiées car ce mémoire s'intéresse principalement aux systèmes multi-infrastructures. Il est, par exemple possible d'utiliser un autre indicateur pour quantifier les conséquences d'une cascade. Un indicateur possible est l'efficacité E_{glob} [LM01]. Celui-ci a été utilisé dans [CLM04a] et [CLM04b]. Une autre variante consiste à ne pas supprimer les nœuds en cas de surcharge, mais de seulement réduire leur capacité comme effectué dans [CLM04a] et dans [KCAL05] sur le réseau électrique Nord américain.

Cette étude de cascade est classiquement effectuée sur les nœuds. Mais, comme pour l'étude de robustesse, on peut également l'appliquer sur les lignes. Cette option sera utilisée au chapitre suivant pour l'infrastructure électrique.

L'intérêt de ces méthodes par rapport à une simulation temporelle du phénomène de cascade est que elle possède l'avantage d'être beaucoup plus simple dans sa modélisation et surtout plus rapide car les calculs à effectuer sont plus réduits que l'intégration de toutes les équations algébro-différentielles régissant un réseau de cette taille. Cela permet d'éviter la réalisation d'études dynamiques à moyen ou long terme avec des outils du type Eurostag ([RTEb]) ou PSS/Netomac ([Sie]) qui sont alors beaucoup plus lourdes (mais permettent d'obtenir des résultats plus précis et physiquement plus faciles à interpréter).

IV.7 Conclusion partielle

Les méthodes évaluées dans ce chapitre marchent correctement et donnent des résultats intéressants pour un graphe modélisant une seule infrastructure. De plus, elles sont rapides relativement aux simulations temporelles classiques vu la taille du réseau. Ces méthodes et les modèles sont globalement « simples » ce qui permet aux mathématiciens, dans certains cas, de trouver des solutions analytiques pour les différentes classes de graphes. On peut, en outre, affiner les modélisations à loisir comme l'on reste sur de la simulation grâce aux différentes variantes et extensions possibles pour chaque méthode.

Cependant, bien que ces méthodes soient applicables à de nombreuses infrastructures différentes, elles ne sont pour l'instant utilisées que sur une seule infrastructure à la fois. Une tentative de dépasser cette limitation est l'utilisation de réseaux complexes en couches décrit dans les articles [KT06] et [KTH07] et illustrée figure IV.19. Cette figure illustre le fait qu'une défaillance unique dans le graphe physique peut provoquer trois défaillances corrélées sur le graphe logique. Les pointillés représentent les nouveaux liens logiques dans le cas où ils sont reroutés. Cette modélisation permet de prendre en considération l'infrastructure physique (de bas niveau) et l'infrastructure logique (de haut niveau), distinction présente par exemple sur les réseaux de transport ou de communication. Mais cette ap-

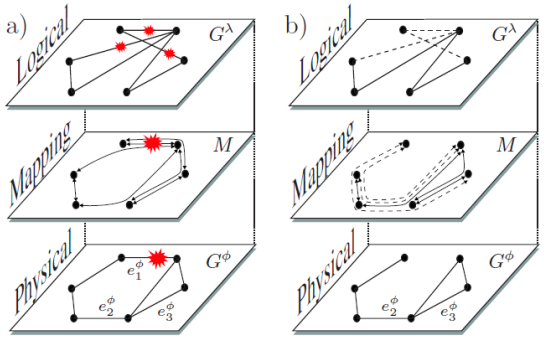

FIG. IV.19 – Illustration de défaillances dans un système à deux couches
Reproduite avec l'autorisation des auteurs [KTH07]

proche n'est pas encore suffisante pour des infrastructures distinctes. Le chapitre suivant présentera une proposition d'approche novatrice, inspirée des méthodes développées dans ce chapitre, et permettant de modéliser les interdépendances entre plusieurs infrastructures hétérogènes.

Chapitre V

Modélisation multi-infrastructures

Sommaire

Résumé

Une proposition de modélisation multi-infrastructures basée sur la théorie des réseaux complexes est présentée dans ce chapitre. Cette modélisation a été mise en œuvre sous forme informatique dans deux environnements différents. Grâce à cette réalisation, il a été ensuite réalisé diverses études paramétriques et d'influence d'hypothèses adoptées sur plusieurs infrastructures mixtes (réseau électrique et de télécommunication associés). Les résultats obtenus permettent d'améliorer la compréhension du comportement des systèmes multi-infrastructures face aux défaillances.

V.1 Introduction

Comme énoncé depuis le début de ce mémoire, le but de ce chapitre est de modéliser les interdépendances des infrastructures critiques. Pour rappel, on considère ici comme interdépendances toutes les interactions, plus ou moins explicites, entre des systèmes différents pouvant mener à des défaillances. Il a été définit lors du premier chapitre trois familles de défaillances entre les infrastructures : en cascade, en aggravation et de mode commun. On a également choisi de limiter l'étude à l'infrastructure électrique et aux systèmes associés de contrôle basé sur les technologies de l'information et de la communication. Ces deux infrastructures sont très différentes et traditionnellement modélisées de façon différente aussi.

Les objectifs de cette modélisation sont les suivants :

- caractérisation de la criticité du réseau de communication en vue de la sécurité du réseau électrique,
- un modèle *commun / unique* de modélisation,
- mise en évidence des modes communs de défaillances et des effets de cascade,
- recherche des points les plus faibles, qui ne sont pas nécessairement des éléments physiques, cela peut être par exemple une topologie. Il s'agit d'une étude de vulnérabilité.

Cette modélisation se veut être une approche complémentaire à la simulation comportementale décrite dans le chapitre 3. Cette approche est basée sur des concepts abordés dans la théorie des réseaux complexes présentés dans le chapitre 4.

V.2 Présentation de la proposition de modélisation

V.2.a Description globale

La modélisation proposée se fonde sur deux graphes distincts, chacun étant composé de nœuds et de liens (ou de lignes suivant la terminologie du réseau électrique). Un des graphes représente l'infrastructure électrique et le second, le réseau de communication et d'information associé (déjà décrit dans le chapitre 3). Pour le graphe du réseau électrique, les nœuds peuvent être générateurs, consommateurs ou aucun des deux. Les liens correspondent aux lignes électriques et aux transformateurs (même si ces derniers n'ont pas été considérés lors de l'établissement du modèle de l'UCTE décrit au chapitre précédent). Pour le graphe du réseau de communication, les nœuds correspondent aux routeurs. Les liens représentent tous les moyens de communication qui peuvent exister entre ces routeurs, qu'ils soient filaires, optiques ou hertziens. Ces deux graphes distincts sont reliés par des règles d'interdépendances.

La figure V.1 illustre cette modélisation. Le graphe du réseau électrique est symbolisé en trait plein avec des nœuds pleins. Celui du réseau de communication est représenté en pointillé avec les nœuds en gris. Les règles d'interdépendances entre les deux réseaux sont les flèches en trait mixte.

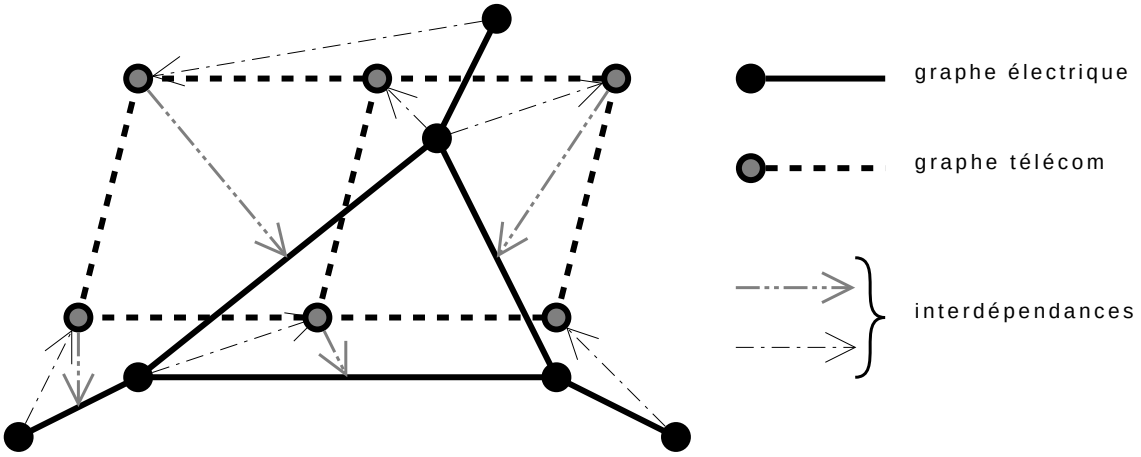

FIG. V.1 – Illustration de la modélisation

V.2.b Éléments de la modélisation

Comme il y a deux graphes et que chacun comporte deux structures élémentaires, il y a un total de quatre éléments différents dans la modélisation proposée : nœud électrique, ligne électrique, nœud de communication et lien de communication. Chacun de ces éléments est composé :

- d'une variable booléenne associé à son *état fonctionnel* (*True* l'appareil fonctionne ou *False* il est défaillant),
- d'une constante *référence géographique* situant la localisation de cet élément. Ce champ sera utile pour la réalisation des défauts de mode commun de nature géographique et également pour les interdépendances. Cette constante est une valeur indiquant la zone dans laquelle est situé l'élément, pas nécessairement ses coordonnées géographiques exactes.

De plus, les nœuds électriques et les nœuds de communication comportent une constante de *description* de l'appareil qui servira pour les défauts de mode commun s'appliquant à un type de composant particulier. Il peut s'agir par exemple du nom d'un modèle de routeur ayant une configuration particulière.

En plus de ces valeurs, les lignes électriques et les nœuds de communication comportent :

- une variable réelle appelée *charge* et qui est calculée par l'algorithme correspondant à la physique de son réseau (explicité ci-après),
- une constante *charge maximale*.

Ces deux valeurs seront utilisées pour la modélisation des cascades. La charge maximale d'un nœud de communication est calculée à partir de sa charge initiale et en lui appliquant un facteur multiplicatif comme réalisé au chapitre 4. Ce facteur est appelé par la suite coefficient de tolérance ou α. Le choix de ce facteur multiplicatif fera l'objet d'une analyse présentée par la suite. En ce qui concerne le réseau électrique, la charge maximale d'une ligne correspond à sa puissance maximale admissible. Pour finir, à chaque nœud de communication est associé une constante *alimentation* correspondant au nœud électrique qui l'alimente.

Le tableau V.1 récapitule les valeurs dont chaque élément est constitué. L'utilité de ces variables et les raisons pour lesquelles elles ne sont pas présentes pour tous les éléments sont expliqués dans les sous-sections suivantes.

Tab. V.1 – Valeurs associées à chaque élément

valeurs	nœud élec	ligne élec	nœud com	lien com
état fonctionnel	√	√	√	√
référence géographique	√	√	√	√
description	√		√	
charge		√	√	
charge maximale		√	√	
alimentation			√	

V.2.c Réseau électrique

Pour le réseau électrique, le calcul de la charge des lignes, qui correspond à la puissance les traversant, se fait classiquement par un calcul de répartition de charge. Ce problème est formulé par un ensemble de $2N$ équations non linéaires à $2N$ inconnues avec N le nombre de nœuds du réseau. Les variables d'état sont la tension dans les nœuds (amplitude et angle), les puissances actives et réactives. Il existe plusieurs variantes du calcul de répartition de charge suivant les hypothèses que l'on peut admettre et la contrainte sur le temps de calcul. La résolution de ce problème est très souvent effectuée avec la méthode de Newton-Raphson [Wee87]. Lorsqu'il est nécessaire d'avoir un temps de calcul réduit pour réaliser des études systématiques en grand nombre, ou lorsque l'on ne s'intéresse qu'à la puissance active (par exemple des études économiques) ou lorsque l'on ne dispose pas des données complètes du réseau, il existe une simplification de ce problème appelée *DC load flow*. Comme on est concerné par les trois conditions précédentes, c'est ce mode de calcul qui a été choisi.

Le *DC load flow* se base sur trois hypothèses principales :

- les composantes résistives et capacitives du modèle des lignes sont négligées. Seule la composante inductive est prise en considération,
- on néglige les flux de puissance réactive Q,
- on considère que la tension vaut en tout point sa valeur nominale.

Ces hypothèse permettent de transformer le problème du calcul de répartition de charge, qui pour rappel comporte $2N$ équations non linéaires à $2N$ inconnues en un problème à N équations *linéaires* et N inconnues, d'où son nom. En effet, en assimilant les admittances à des résistances, les différences d'angle à des tensions et les puissances dans les lignes à des courants continus, le problème est alors analogue à une résolution de circuit en courant continu. La résolution ne consiste alors plus qu'à une inversion de matrice. Elle est donc non itérative et a fortiori convergente. Des logiciels spécifiques tels que PSAT [Mil05b] ou Eurostag [RTEb] ne sont plus nécessaires, et tous les logiciels pouvant effectuer du calcul numérique sont alors capables de le résoudre. Matlab, Octave et Python qui seront utilisés

pour cette étude et qui ont déjà été présentés dans le chapitre 3 réalisent ces calculs. Le *DC load flow* est, certes, moins précis que le calcul de répartition de charge AC (qui peut être résolu par la méthode de Newton-Raphson) avec toutes les hypothèses nécessaires pour trouver un état statique prises en compte. Le gain de rapidité est néanmoins très important.

La modélisation proposée s'applique naturellement aux réseaux de transport. C'est ce type d'infrastructures qui sera étudié dans ce mémoire. Néanmoins, la modélisation est très générique et pourrait très bien être utilisée à d'autres niveaux de tension à condition de respecter l'esprit de la modélisation, en particulier un nombre de nœuds suffisamment important. Bien entendu, si on l'applique à un réseau de distribution, il ne faudra pas utiliser le *DC load flow* car ses hypothèses ne sont pas adaptées à ce type de réseau.

Il peut arriver au cours de la simulation, suite à des suppressions de lignes, que le réseau électrique se scinde en plusieurs parties. Dans ce cas, une zone est considérée comme viable si elle comprend plus de la moitié des nœuds présents à cette étape de la simulation. L'ensemble des nœuds n'appartenant pas à une zone remplissant cette condition sont supprimés. En effet, on considère, dans de tels cas de partitionnement, que la situation est très grave et est susceptible de mener à un écroulement complet du réseau. On ne cherche donc pas à vérifier les capacités de fonctionnement autonome de ces petites zones. Ainsi, il ne peut y avoir au plus qu'une seule zone au cours de la simulation.

En plus de cette vérification sur la taille des zones, on vérifie également, après un partitionnement, que la capacité de génération est suffisante pour assurer l'équilibre production consommation. Dans ce calcul, on ne considère pas les pertes dans le réseau du fait des hypothèses du *DC load flow* car on néglige la résistance des lignes. On prend également comme hypothèse que le nœud bilan (*slack bus* [Wee87]) ne doit pas fournir plus de 20% de la consommation. En effet, dans la modélisation, ce nœud ne possède pas de limitation de puissance, mais dans la réalité, tout générateur est limité en capacité de production. Cette limite de 20% a été choisie de manière arbitraire et peut être adaptée suivant le réseau considéré.

V.2.d Réseau de télécommunication

Partant du fait que l'on ne dispose pas de la topologie des infrastructures de communication et d'information associées aux réseaux électriques, on a choisi de construire ce réseau. Cette approche va ainsi permettre d'étudier différentes topologies et de les comparer. Bien entendu, la modélisation proposée pourra aussi s'appliquer à la topologie réelle par quiconque possédant ces données. Travailler sur des modèles construits plutôt que sur des données réelles qui n'existent généralement pas est d'usage courant dans l'étude de ce genre de réseau.

Les différentes topologies étudiées pour le réseau de communication sont les suivantes :

Miroir : le réseau de communication est identique au réseau électrique. Chaque nœud de télécommunication reçoit son alimentation électrique du nœud électrique dont il est l'image et appartient à la même zone géographique. L'étude de cette topologie se justifie par le fait qu'il existe des réseaux de communication dont les liens suivent les lignes électriques. Ainsi Arteria est un réseau de fibres optiques à haut débit suivant les lignes électrique du réseau de transport de RTE.

Barabási-Albert : graphe aléatoire en utilisant le modèle de l'attachement préférentiel de Barabási-Albert décrit dans [BA99]. Ce modèle nécessite deux paramètres : n le nombre de nœuds et m le nombre de liens à attacher d'un nouveau nœud aux nœuds existants. Le graphe est construit de la façon suivante : on part de m nœuds non connectés entre eux et on ajoute petit à petit les $n - m$ autres nœuds au graphe. Chaque nœud ajouté est créé avec m liens allant vers les nœuds déjà existant avec une probabilité proportionnelle au degré. Ainsi, il est plus probable qu'un nouveau nœud se connecte à un autre déjà fortement connecté plutôt qu'à un lien isolé, d'où le nom d'attachement préférentiel. Il y a au total $m * (n - m)$ liens. Ce type de graphes, simple à construire, est souvent utilisé pour modéliser le Web ou l'Internet, c'est pour cette raison que l'on a choisi d'étudier cette topologie pour le réseau de communication. Deux exemples d'un tel graphe construits avec $n = 6$ et $m = 2$ sont présentés figure V.2.

Grille : le graphe est semblable à une grille de dimension 2. Ce modèle prend deux paramètres m et n que sont la taille de chaque dimension (suivant chaque axe). Il y a $m * n$ nœuds et le nombre de liens vaut

$$(m - 1) * n + (n - 1) * m = 2 * m * n - m - n \tag{V.1}$$

La grille 5×4 est présentée figure V.2.

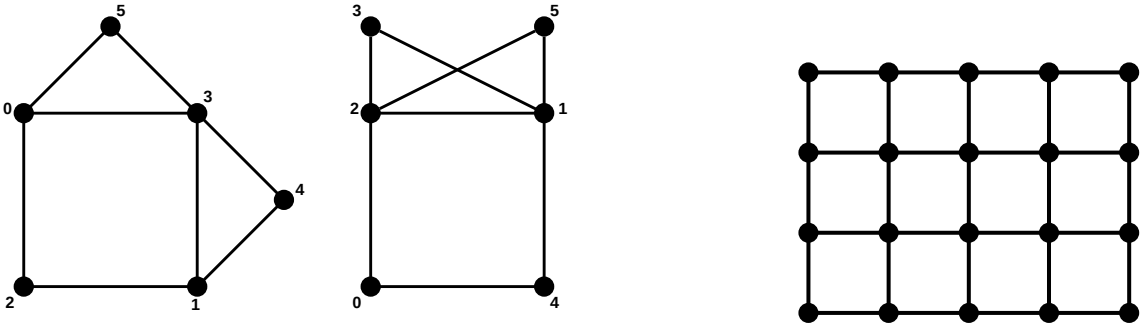

Fig. V.2 – Exemples de graphes Barabási-Albert ($n = 6$ et $m = 2$) et grille 5×4

Comme réalisé au chapitre précédent, la charge des nœuds de ce réseau est calculée par le coefficient de centralité d'intermédiarité non normalisé, autrement dit par le nombre de chemins géodésiques les traversant. Ce choix se justifie par le fait que de nombreux protocoles de routage dans les réseaux de communication se basent sur l'algorithme de Dijkstra qui permet de déterminer le plus court chemin. Un exemple de ces protocoles est OSPF (*Open Shortest Path First*) qui est couramment utilisé à l'intérieur des systèmes autonomes. Ainsi lorsqu'ils doivent envoyer des informations vers une destination donnée, les routeurs déterminent la meilleure route qu'ils utilisent pour cette transmission.

V.2.e Prise en compte des différents phénomènes

Pour parvenir à l'objectif fixé tel que décrit dans l'introduction, l'approche proposée doit permettre la modélisation des effets de cascade, des modes communs de défaillances et toutes autres interdépendances pouvant exister entre les infrastructures.

Modélisation des effets de cascade

Les effets de cascade sont pris en compte de manière différente pour chaque infrastructure. En ce qui concerne le réseau électrique, les cascades observées sont des cascades de lignes. Lorsqu'une ligne déclenche suite à une surcharge, le report de charge sur les lignes avoisinantes peut également les faire déclencher et ainsi de suite. Par conséquent, dans l'approche proposée, seules les lignes dans le réseau électrique possèdent une charge et une charge maximale et il ne peut y avoir de cascade sur les nœuds. Réciproquement, pour le réseau de télécommunication, ce sont les routeurs (modélisés par les nœuds) qui sont susceptibles de surcharge et non pas les liens de communication. En effet, lorsque ces derniers sont utilisés au maximum de leur capacité, ce sont les routeurs qui stockent les paquets en attente. Donc sur le réseau de télécommunication, la cascade a lieu sur les nœuds, pas sur les liens qui ne disposent donc pas de valeur de charge ni de charge maximale.

Modélisation des modes communs de défaillance

La prise en compte des défaillances de mode commun se fait lors de la réalisation du défaut initial. Tous les éléments de chaque infrastructure possèdent une valeur associée à leur localisation géographique. Il est ainsi possible de mettre hors service l'ensemble des éléments situés à un endroit spécifié pour simuler des événements tels qu'un incendie, un tremblement de terre ou une inondation. Le second type de mode commun considéré concerne les défaillances dues à un matériel identique défectueux. Dans cette approche, on a considéré que cela pouvait s'appliquer seulement aux nœuds des deux réseaux, mais que les lignes électriques et les liens de communication n'étaient pas vulnérables à ce genre de défaillance. Par conséquent, tous les nœuds disposent d'une valeur description correspondant au type de matériel utilisé. Bien entendu, la description des nœuds de télécommunication est différente de celle des nœuds électriques. Là encore, il est possible de mettre hors service l'ensemble des éléments identiques pour simuler un mode commun particulier tel que, par exemple, un type de routeur vulnérable à une cyber-attaque spécifique.

Modélisation des interdépendances

Au niveau des interdépendances directes entre les infrastructures, on peut les diviser en deux catégories : la dépendance du réseau de communication envers le réseau électrique et réciproquement.

La dépendance de première catégorie est triviale : une panne du réseau électrique conduit, tôt ou tard, à l'arrêt des composants du réseau de communication l'alimentant, comme déjà expliqué dans le premier chapitre. Ce comportement est pris en compte dans cette approche grâce à la valeur *alimentation* des nœuds du réseau de communication. Ainsi, on associe à chacun de ces nœuds, un nœud électrique. Lorsque un nœud électrique est supprimé (du fait d'un défaut de mode commun, par suppression de toutes les lignes auquel il est connecté ou parce qu'il est dans une zone ilôtée non viable) alors tous les nœuds de télécommunication qu'il alimentait sont supprimés. Il n'est pris en compte un paramètre *alimentation* que pour les nœuds de communication, on suppose que les liens reçoivent leur alimentation en énergie électrique par leurs extrémités. Comme dès que l'on supprime un nœud, tous les liens connectés sont également supprimés, ces derniers sont

également impactés indirectement par le manque d'alimentation.

La dépendance du réseau électrique envers le réseau de communication est plus subtile. Comme développé dans le premier chapitre, le réseau électrique a été créé puis a d'abord fonctionné sans le second. L'utilisation des moyens de communication et d'information pour la conduite du réseau électrique s'est faite de manière progressive. Dans l'état actuel de l'imbrication de ces infrastructures, un problème sur les moyens de communication et d'information provoque principalement une perte d'observabilité de l'état du réseau électrique. Celle-ci peut empêcher les opérateurs de se rendre compte d'un problème et donc, en l'absence de contre-mesure associées, amplifier le problème électrique. Ce fut le cas lors de la panne généralisée du mois d'août 2003 aux États-Unis. Pour modéliser ce phénomène complexe, car faisant intervenir de nombreux paramètres et en particulier le comportement humain, une règle simple a été définie. Cette dernière est que si il y a une suppression d'un nœud de communication, alors elle provoque la suppression du lien électrique le plus chargé de la même zone. On choisit de se restreindre à la zone du nœud, car l'on considère que la perte d'observabilité s'applique principalement sur la zone géographique concernée. Compte tenu de la hiérarchisation de la conduite du réseau électrique et de la couverture et responsabilités des centres de conduites régionaux et nationaux, cette hypothèse est assez logique.

Ces deux règles définies sont le cœur de la modélisation de l'interdépendance entre les infrastructures. Ce sont les deux phénomènes qui font qu'un problème sur le réseau électrique peut se propager au réseau de communication et réciproquement.

On peut rétorquer à cette approche qu'elle est trop brutale, pas assez subtile et surtout bien éloignée de la réalité. En particulier la seconde règle où un problème sur un routeur ne provoque pas toujours un déclenchement de ligne du réseau électrique. Cela est vrai, mais l'esprit de cette approche est de s'intéresser au pire des cas. Il ne faut pas oublier, que généralement, le couplage du réseau électrique et d'un réseau de communication fonctionne bien et que un problème de télécommunication n'engendre pas systématiquement un problème de nature électrique. Modéliser le cas général où tout marche correctement ne présente que peu d'intérêt pour la compréhension des interdépendances. On doit également avoir en tête que des événements tels que les grandes pannes présentées dans le premier chapitre sont très rares. Lorsque elles arrivent, elles sont le fruit de la conjonction de plusieurs événements jugés hautement improbables auparavant. Et pourtant, ces pannes existent. C'est dans cet esprit que cette approche de modélisation est proposée. Il ne s'agit pas de simuler le fonctionnement habituel des infrastructures mais d'évaluer le pire des cas. Il s'agit, en effet, d'une analyse de criticité. C'est également dans cet esprit qu'il faudra appréhender les résultats obtenus qui sont présentés section V.4. Si pour deux cas différents, on obtient une panne généralisée une fois sur deux dans l'un et seulement un problème minime dans la même proportion dans l'autre, il ne s'agit pas de dire que la modélisation montre qu'une panne généralisée arrive la moitié du temps dans le premier cas. Mais par contre, on peut conclure que la première situation est potentiellement plus critique que la seconde. La tendance des conséquences est également intéressante à déterminer, et dans ce but l'influence de l'impact de cette seconde règle d'interdépendance sera analysée par la suite. Vu l'ensemble des hypothèses de la modélisation proposée (pour chaque réseau et pour les interdépendances), les résultats ne représentent pas la valeur exacte de la conséquence. Cependant, ils peuvent être un outil utile d'aide à la décision

pour la planification ou pour les opérateurs.

V.2.f Algorithme

Le déroulement de la simulation est le suivant :

1. Initialisation : création de tous les éléments de la modélisation à partir de l'importation des données et calcul éventuel de paramètres tels que la charge maximale des nœuds du réseau de communication
2. Réalisation du défaut initial
3. Calcul des charges du réseau électrique
4. Si surcharge électrique, suppression des lignes concernées et retour à 3
5. Suppression des éventuels nœuds de communication n'ayant plus d'alimentation électrique
6. Si cette suppression conduit à supprimer des lignes électriques, les supprimer et retour à 3
7. Sinon, calcul des charges du réseau de communication
8. Si surcharge de communication, suppression des éléments concernés et retour à 3
9. Sinon, fin de la simulation : évaluation des conséquences

La mise en œuvre effectuée de cet algorithme est présentée sur l'organigramme figure V.3.

Ainsi, les résultats sont obtenus de manière séquentielle, mais en s'affranchissant d'une simulation temporelle, telle que présentée au chapitre 3, coûteuse en temps de calcul. La contrepartie est que l'on ne dispose pas d'informations temporelles sur le déroulement des cascades d'évènements. Ainsi, certaines étapes, identiques dans la modélisation, peuvent simuler des événements durant dans la réalité de quelques milisecondes à quelques minutes.

En ce qui concerne le point 2, le défaut initial peut être réalisé de différentes manières, lesquelles peuvent être associées à un type de défaillance :

- défaut(s) sur un élément d'une des infrastructures de manière systématique ou aléatoire,
- défaut sur une zone géographique : défaillance de mode commun,
- défaut sur un type de composant : défaillance de mode commun,
- augmentation de la puissance électrique consommée en un nœud (qui provoquera une surcharge de lignes).

Le défaut sur un élément d'une des infrastructures peut être réalisé de manière systématique avec évaluation des conséquences et de la gravité conduisant ainsi à une étude appelée N-1. De même, on peut réaliser de manière systématiques deux défauts, étude que l'on nomme N-2 [RTE04].

En ce qui concerne le dernier point de l'algorithme, les conséquences sont évaluées par la puissance non fournie aux consommateurs. On ne considère donc que l'état final du réseau électrique. En effet, le réseau de communication étudié a pour objectif de faire fonctionner le réseau électrique, donc ses conséquences propres ne sont pas directement intéressantes. De même, le réseau électrique a pour but d'alimenter des consommateurs en énergie électrique, donc le nombre de lignes ayant déclenché n'est pas le plus important dans l'évaluation. Il faudrait normalement s'intéresser à l'énergie non distribuée, car c'est

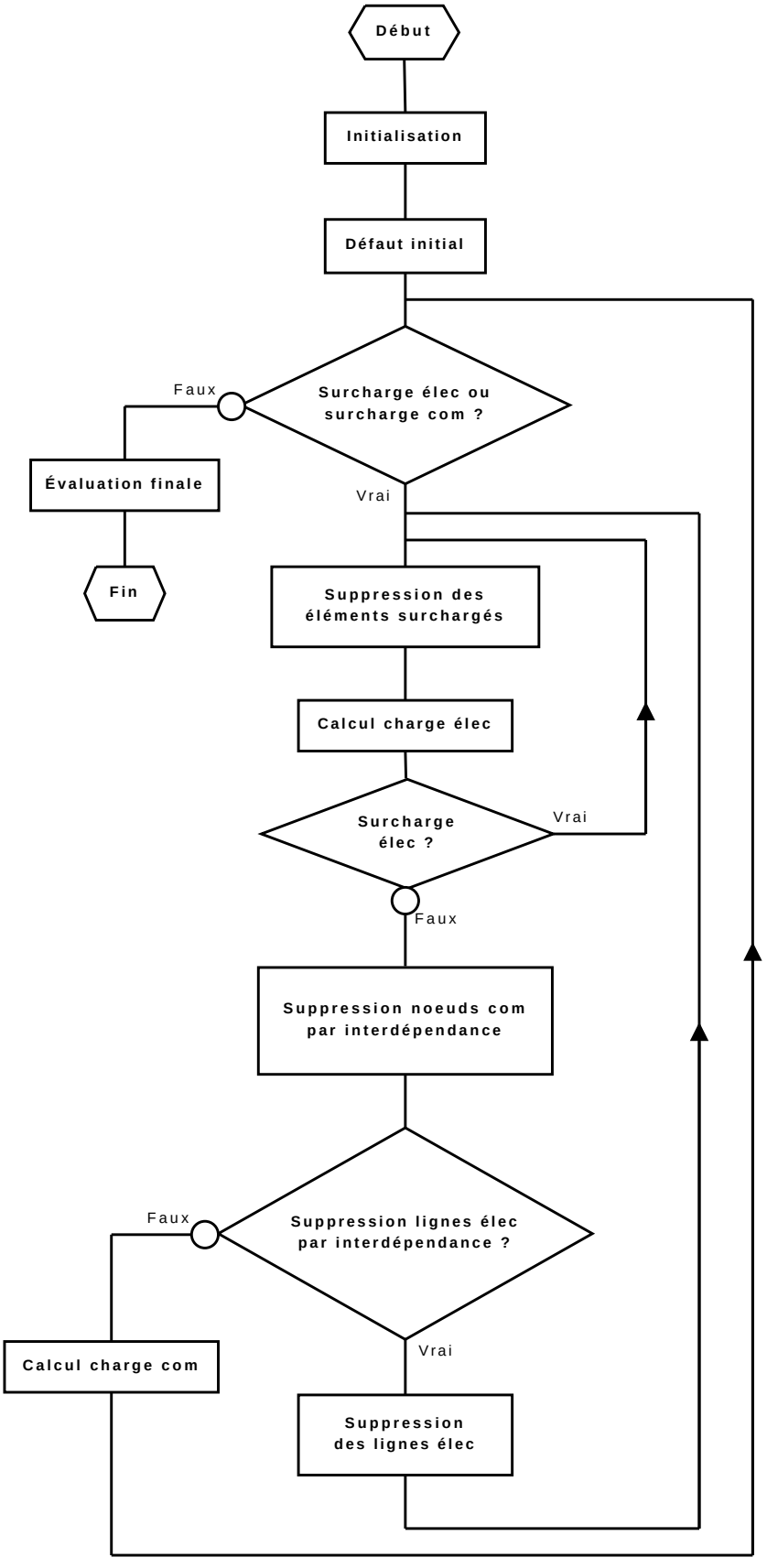

Fig. V.3 – Organigramme de l'algorithme de simulation

cette dernière qui porte le plus de préjudices aux consommateurs. Mais l'aspect temps étant absent de l'approche proposée, on ne peut calculer d'énergie. C'est pour cette raison que l'on parle seulement de puissance non fournie.

Comme on peut l'observer sur l'organigramme V.3, il a été choisi d'imbriquer la cascade électrique dans la cascade de télécommunication. Il aurait également été possible de les réaliser simultanément ou de manière séquentielle (l'une après l'autre). La raison de ce choix est que lorsqu'une ligne électrique déclenche, le report de charge se fait instantanément sur les autres lignes et que si elle dépasse leur seuil de déclenchement immédiat (pas celui à 20 minutes) alors les déclenchements se font quasi instantanément. Sur le réseau de communication, lorsqu'un routeur est surchargé, il faudra plus de temps pour que les autres routeurs s'en rendent compte et mettent à jour leur table de routage pour diriger leurs paquets vers une autre route. De plus, la première relation d'interdépendance (problème sur le réseau électrique provoque l'arrêt des éléments du réseau de communication l'alimentant) est elle aussi plus directe que la seconde (problème sur le réseau de communication provoque du fait de la perte d'observabilité le déclenchement de la ligne la plus chargée de la zone). Un troisième argument, plus pragmatique, concerne le temps de calcul. En effet, de toutes les étapes de l'algorithme, celle prenant le plus de temps de calcul est le calcul des charges du réseau de communication. En effet, ce dernier nécessite de calculer la totalité des chemins géodésiques entre tous les nœuds soit $N * (N - 1)$ chemins à calculer. Tandis que pour la charge du réseau électrique, il n'y a qu'une inversion de matrice carré de taille N. Donc le fait de mettre la boucle de la cascade électrique à l'intérieur de celle du réseau de communication permet d'effectuer moins souvent le calcul de charge dans ce dernier et donc diminuer le temps global de calcul.

La simulation se termine lorsqu'aucune ligne électrique et aucun nœuds de communication n'est surchargé. Cela peut arriver lorsqu'il n'y a plus aucune ligne électrique dans le réseau suite à une panne généralisée totale ou juste après le premier défaut si les reports de charge dûs à celui-ci ne sont pas contraignants pour les autres éléments.

V.3 Réalisation logicielle

Il n'existe pas de logiciels de référence permettant de simuler directement la modélisation proposée. Il a donc été choisi de la mettre en œuvre avec l'aide de logiciels d'usage général. Pour ce faire, deux plates-formes différentes ont été utilisées. Matlab et Python, logiciels déjà présentés lors des chapitres 3 et 4 ont été retenus. Cette double réalisation apporte plusieurs avantages. Le plus important est qu'elle fournit un moyen de vérification à la condition de ne pas calquer un développement sur l'autre. Cette condition est respectée car la programmation Matlab a été réalisée de manière fonctionnelle et celle sous Python de type orienté objet. Bien entendu cela ne suffit pas à garantir qu'il n'existe pas des erreurs communes aux deux réalisations mais permet tout de même d'en éviter de nombreuses. Un autre avantage est que cela permet de profiter des avantages des deux logiciels que sont la simplicité de programmation et l'utilisation du module pour réseaux complexes déjà existant (NetworkX) avec Python et la connaissance de Matlab au sein du laboratoire et du milieu académique en général pour la reprise ultérieure des travaux. Un dernier avantage est que une fois les deux mises en œuvre effectuées et comparées, on peut choisir la plus rapide pour réaliser les diverses études. Ces avantages sont obtenus au prix

de quelques inconvénients. Ainsi, sous Matlab, il est nécessaire de coder quelques fonctions supplémentaires n'existant pas. Le travail à effectuer étant presque double cela prend du temps et exige également un effort supplémentaire pour la maintenance.

En pratique, le code Python correspond à environ 540 lignes de code. Celui sous Matlab est répartis en 34 fonctions créées pour un total d'environ 1200 lignes de code.

En terme de temps de calcul, sur un PC équipé d'un P4 cadencé à 2,80 GHz le calcul de charge du réseau de communication ayant la même topologie que le réseau UCTE (miroir) est de 263 secondes sous Matlab et 94 secondes avec Python. Sur l'ensemble d'une simulation, la quasi totalité du temps de calcul est passée dans la fonction d'évaluation du coefficient de centralité d'intermédiarité pour les nœuds. Cette fonction est de taille réduite et est figée (c'est-à-dire qu'elle n'évoluera pas en fonction des divers cas d'étude). C'est donc la situation idéale pour prendre le temps de la coder en langage C et la compiler. Cela a été effectué pour la mise en œuvre avec Matlab qui permet de créer des fonctions compilés (à partir de code en Fortran ou en C) que l'on peut appeler directement depuis l'environnement Matlab. C'est ce que l'on appelle des *Mex-files*. Dans ce cas, sur le même ordinateur, la fonction de référence ne nécessite plus qu'une durée de 18 secondes au lieu de 263 secondes soit une division par presque 15 du temps de calcul. Du fait de ses performances, cette mise en œuvre a logiquement été choisie pour les études réalisées et présentées par la suite.

V.4 Résultats

La mise en œuvre de la modélisation proposée, décrite ci-avant, a permis d'effectuer diverses études. Les résultats de ces études sont présentés dans cette section. Il s'agit tout d'abord de comprendre l'influence du coefficient de tolérance du réseau de communication à travers une étude paramétrique. Celle-ci pourra être conduite sur différentes topologies de ce réseau. Une fois étudiée l'influence du réseau de communication, on pourra analyser l'impact de deux incidents dans la même infrastructure et dans les infrastructures distinctes suite à un défaut localisé. La modélisation sera ensuite appliquée à d'autres réseaux électriques pour vérifier que les tendances ne sont pas spécifiques au cas d'étude. Et pour finir, il est nécessaire de reconsidérer l'hypothèse d'interdépendance la plus contestable qui est la propagation d'une défaillance du réseau de communication sur le réseau électrique.

V.4.a Protocole utilisé

Un $N-1$ du réseau électrique et un $N-1$ du réseau de communication (voir un $N-2$ dans V.4.d) est réalisé pour chaque cas étudié. La grandeur de sortie observée est la puissance non fournie dans chaque cas.

Comme premier réseau électrique étudié, il a été choisi celui de la France dont les données sont extraites du réseau UCTE présenté au chapitre 4. Le graphe résultant comporte 318 nœuds et 519 lignes et la représentation graphique est donnée figure V.5. Pour rappel, seules les lignes 400 kV et 225 kV sont considérées. Celles ayant une impédance trop faible (du fait de leur faible longueur) sont ignorées. Pour comparaison, la carte du réseau de transport français telle que donnée par son gestionnaire est présentée figure V.6. On peut

voir que les données utilisées sont assez réalistes par rapport à la réalité. Les dimensions de ce graphe sont suffisamment grandes pour obtenir des résultats significatifs, sans être trop importantes ce qui mènerait à des temps de calcul pour les simulations très longs. Comme la France était dans une situation exportatrice dans ces données (correspondant à un jour d'été en 2002), l'ensemble de la puissance des générateurs a dû être baissé de 8% pour avoir un équilibre entre la production et la consommation. Dans une première approche, le réseau de communication possède la topologie miroir au réseau électrique.

Plusieurs simulations ont tout d'abord été effectuées pour avoir un aperçu des résultats que l'on peut obtenir. Les histogrammes obtenus de la puissance non fournie non nulle pour différents $N-1$ sont présentés figure V.4. Ces histogrammes représentent le nombre de fois où il y a eu effectivement un problème dans le réseau électrique ainsi que sa conséquence évaluée par la quantité de puissance non fournie. Les résultats avec le défaut initial sur le réseau électrique sont présentés sur la colonne de gauche et lorsqu'il est sur le réseau de communication, sur la colonne de droite. Les histogrammes sont tracés pour différentes valeurs du coefficient de tolérance α. Le nombre de fois où la puissance non fournie est nulle, c'est-à-dire lorsque aucun consommateur n'a été impacté, n'est pas représenté par une barre, mais indiqué dans la légende. Pour une meilleure visualisation de l'histogramme dans les différents cas, les échelles ont été modifiées.

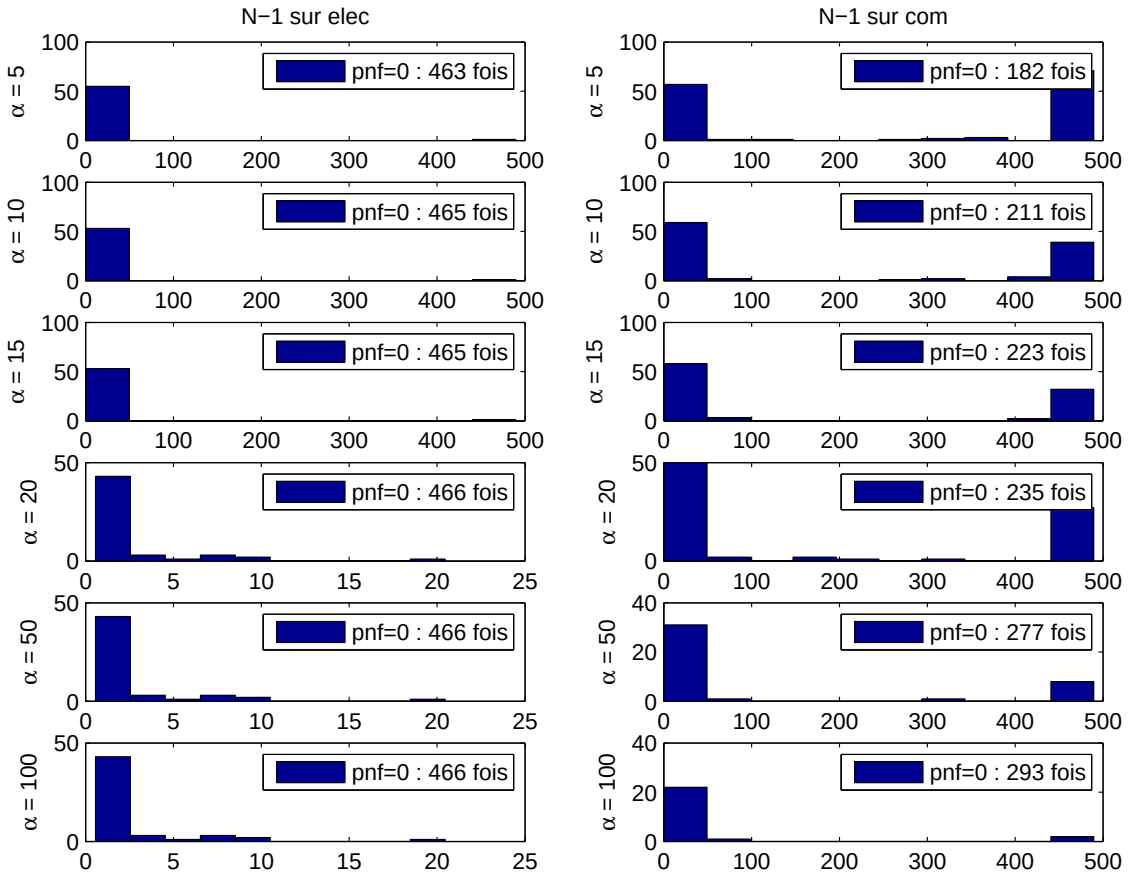

FIG. V.4 – Histogrammes de la puissance non fournie pour différents $N-1$

D'après les résultats de ces simulations, il s'avère que l'on peut dissocier différents cas

de figure : soit la puissance non fournie est nulle (c'est-à-dire aucun consommateur n'est impacté, le cas idéal), soit elle faible (suite à une défaillance restant localisée) ou soit elle correspond à l'ensemble de la puissance du réseau (le réseau est totalement écroulé : panne généralisée). Il n'y a que très peu de cas où la puissance non fournie concerne beaucoup de consommateurs sans avoir une panne généralisée. Suite à ce constat, il a été décidé de créer quatre catégories différentes pour classer la gravité :

gravité 0 : la puissance non fournie est nulle : il n'y a aucun problème pour les consommateurs,

gravité 1 : la puissance non fournie est non nulle et inférieure à 10% de la puissance totale : le problème reste localisé,

gravité 2 : la puissance non fournie est incluse entre 10% (non compris) et 90% (compris) de la puissance totale : le problème est grave mais n'est pas une panne généralisée,

gravité 3 : la puissance non fournie est strictement supérieure à 90% de la puissance totale : il y a eu une panne quasi généralisée.

Ensuite, pour chaque étude $N-1$ réalisée, on calcule le pourcentage de défaillances ayant conduit aux différentes catégories de gravité. Ces quatre classes de gravité vont permettre d'évaluer plus facilement chaque situation testée et surtout simplifier les comparaisons entre différents cas d'étude.

V.4.b Étude paramétrique du coefficient de tolérance

Les réseaux utilisés sont le réseau électrique français décrit précédemment et le réseau de communication ayant la topologie miroir. L'étude paramétrique réalisée consiste à faire varier le coefficient de tolérance α du réseau de communication. Pour chaque valeur de ce coefficient, 519 défauts initiaux différents sur l'infrastructure électrique (suppression de lignes) sont étudiés et 318 défauts initiaux sur celle de télécommunication (suppression de nœuds). On calcule ensuite le pourcentage d'incidents dont les conséquences appartiennent à chaque classe de gravité.

Les résultats obtenus pour le $N-1$ sur les 519 lignes du réseau électrique sont présentés figure V.7. L'ensemble des coefficients entre 0 et 100 a été testé, ce qui donne 101 points de mesure (en abscisse). La première constatation concerne les variations du pourcentage de chaque classe de gravité (en ordonnée) en fonction de α : elle est toujours inférieure à 1%. Autrement dit, le dimensionnement du réseau de télécommunication n'a qu'une faible influence sur l'impact final d'un défaut ayant pour origine un problème électrique. Ensuite, d'une manière générale, lorsque le coefficient de tolérance est supérieur à 20% alors 9 fois sur 10, il n'y a pas de conséquence finale sur les consommateurs et 1 fois sur 10 il y en a de très faibles (ce qui est le cas lorsque, par exemple, on supprime l'unique ligne alimentant un consommateur donné) et aucun défaut ne provoque de défaillance plus grave. Ensuite, si le coefficient de tolérance du réseau de communication est réduit, alors il commence à apparaître un peu plus de défaut de faible gravité et surtout des défauts de gravité plus élevée. Comme indication, un défaut correspond à légèrement moins que $0,2\%$ des cas considérés. Donc, un dimensionnement plus limite du réseau de communication (entre 8 et 20%) peut transformer une panne localisée en panne généralisée. Avec un dimensionnement encore plus faible (α inférieur à 8%), deux incidents électriques distincts peuvent chacun

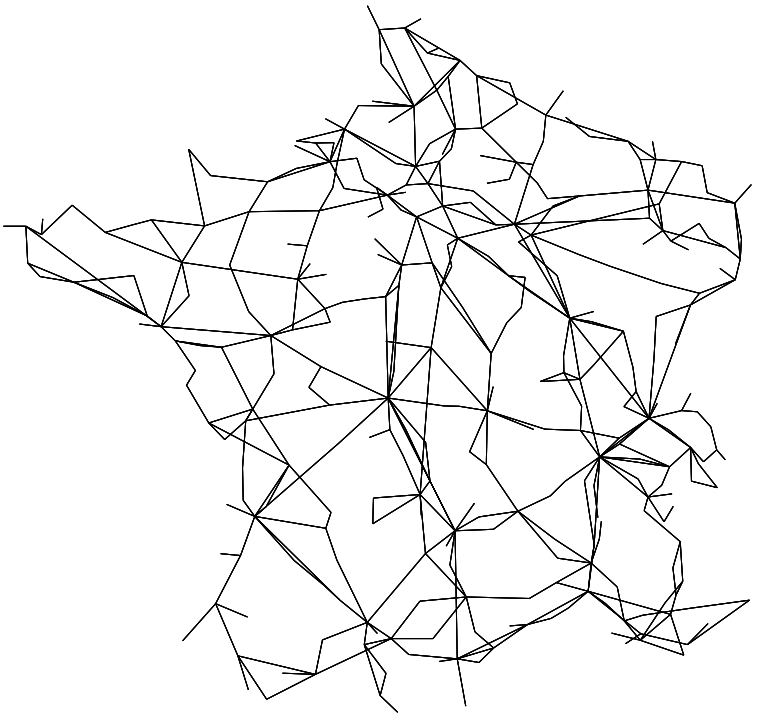

FIG. V.5 – Graphe du réseau de la France

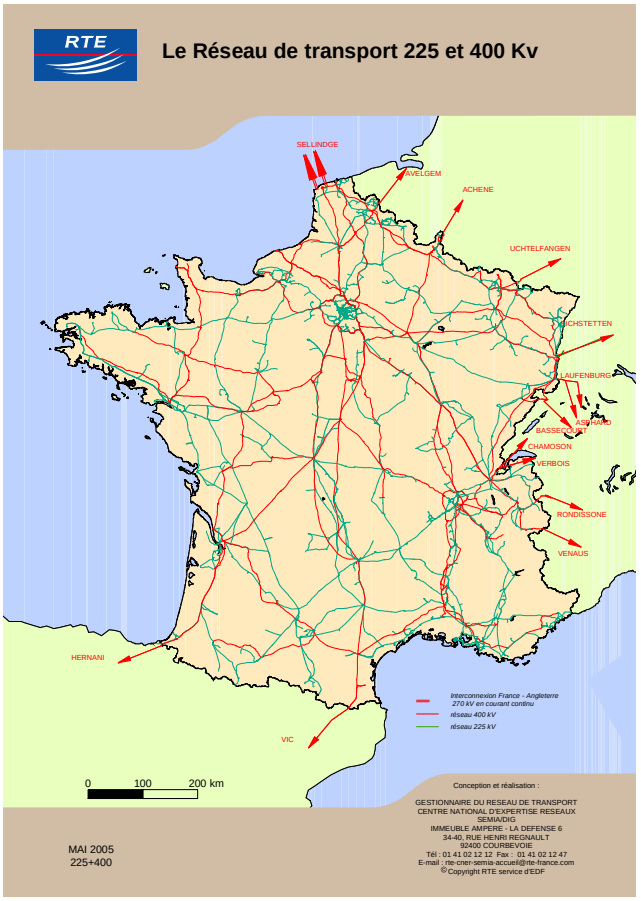

FIG. V.6 – Carte du réseau de transport français (Crédit RTE)

conduire à des pannes généralisées. D'une manière générale, le réseau français est conçu pour résister à une $N-1$ électrique, ce qui explique, pour partie, le fait que le faible nombre d'incidents conduisant à une gravité 2 ou 3.

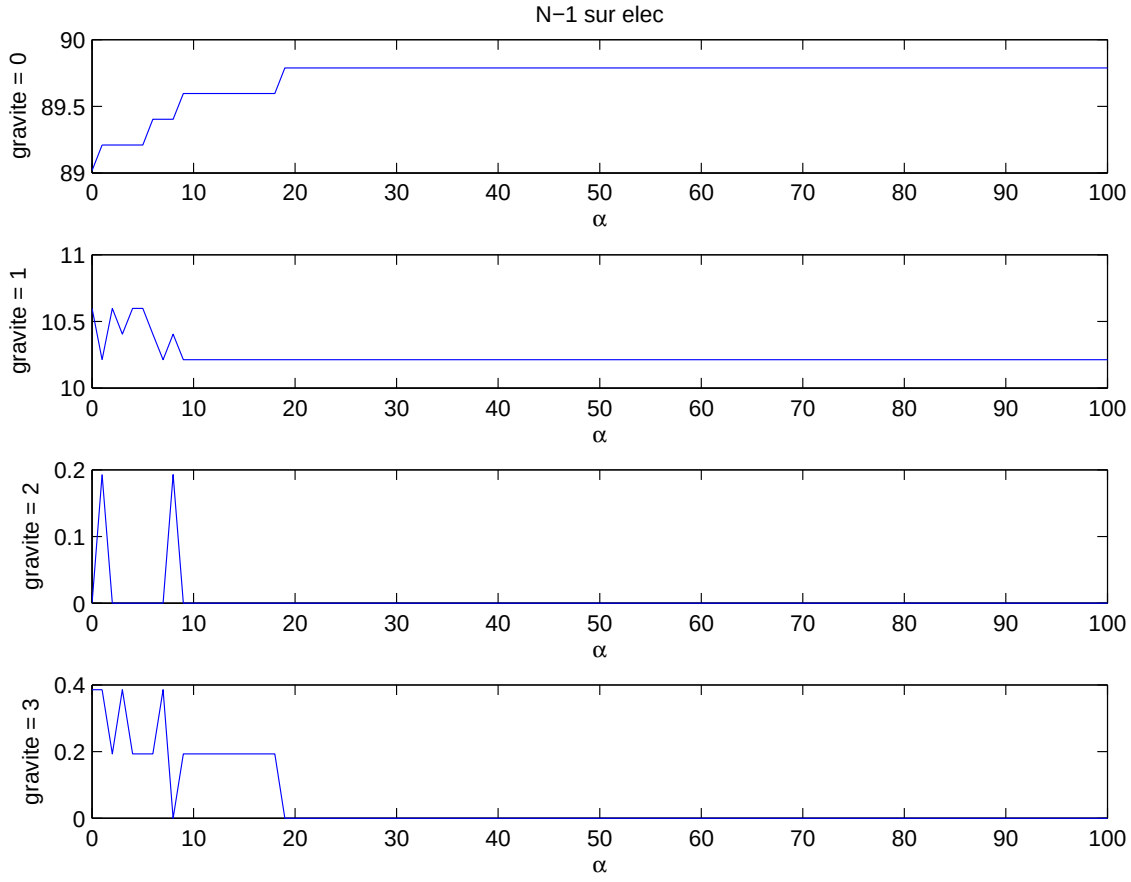

Fig. V.7 – Variation du pourcentage de la gravité pour un $N-1$ sur le réseau électrique (miroir)

Après cette première étude avec un défaut initial sur le réseau électrique, il en a été réalisé une seconde avec un $N-1$ sur les 318 nœuds du réseau de communication. Les résultats obtenus sont présentés figure V.8. Là encore, les graphes sont obtenues pour 101 valeurs différentes de α. La première observation est que l'amplitude de variation du pourcentage de chaque classe de gravité est beaucoup plus grande lorsque l'on réalise le défaut sur le réseau de communication plutôt que sur le réseau électrique. En ce qui concerne les sens de variation, comme l'on pouvait s'y attendre, plus le réseau de communication est dimensionné juste (c'est-à-dire plus le coefficient de tolérance est faible) alors plus on a défaillances de classe 1, 2 et 3 et moins on a d'incident sans gravité. Les différentes courbes ont des allures d'exponentielles. Les incidents de gravité 2 représentent toujours un faible pourcentage par rapport à ceux des autres classes.

De ces deux résultats, on peut d'ores et déjà remarquer que pour la suite des études, il ne faut pas choisir un coefficient de tolérance du réseau de communication trop grand afin de pouvoir observer des pannes généralisées. Inversement, il ne faut pas non plus choisir une valeur trop petite pour qui conduit à obtenir de manière trop fréquente des incidents

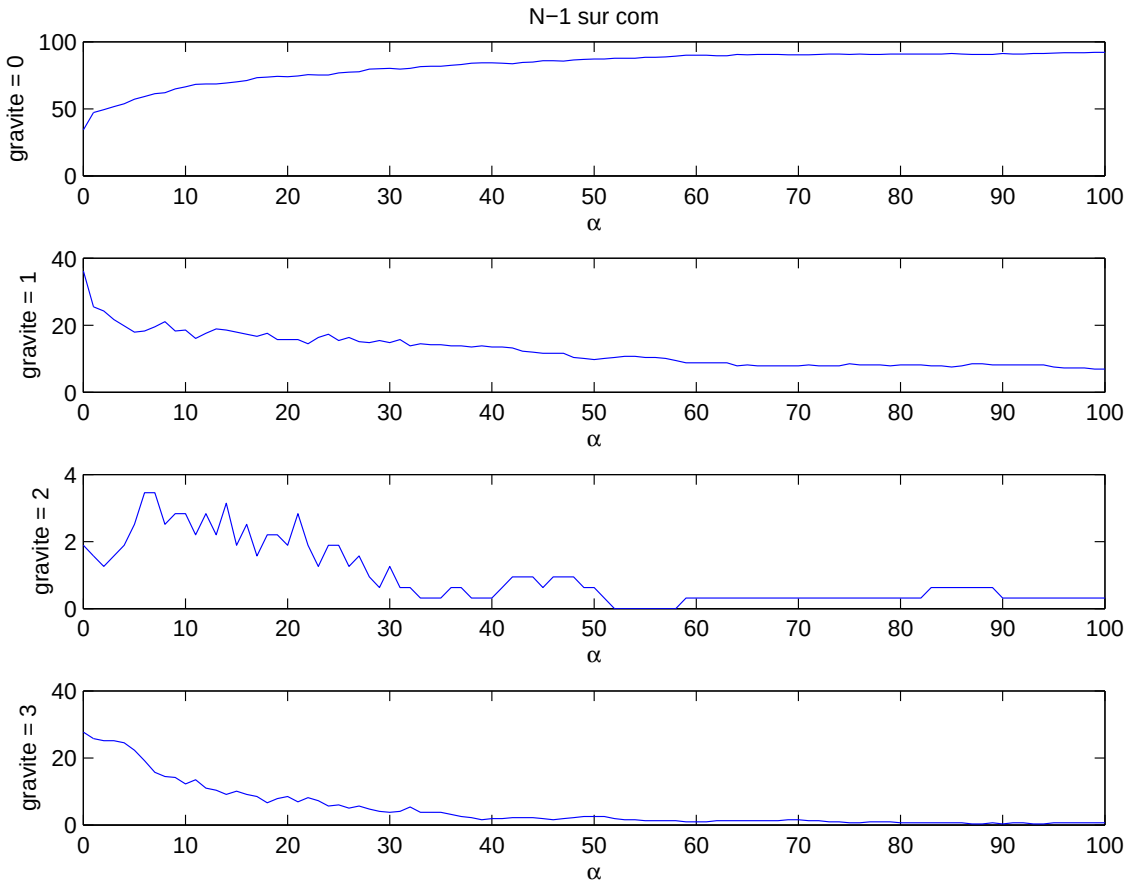

FIG. V.8 – Variation du pourcentage de la gravité pour un $N-1$ sur le réseau de communication (miroir)

importants. Comme ordre de grandeur, une valeur de α comprise entre 10 et 20% semble être un bon compromis.

V.4.c Étude de la topologie du réseau de communication

Après la première étude paramétrique du coefficient de tolérance α pour une topologie du réseau de communication donné, il est intéressant d'effectuer cette même étude avec d'autres topologies pour ce réseau. Les topologies du réseau de télécommunication étudiées sont le miroir, le modèle de Barabási-Albert et la grille, toutes trois décrites en V.2.d. Pour effectuer une comparaison équilibrée, toutes ces topologies ont été choisies avec un nombre de nœuds identique. Cette règle permet également de faciliter la correspondance des nœuds de communication avec les nœuds électriques les alimentant.

La topologie miroir a déjà été étudiée lors de la première étude paramétrique, on va donc pouvoir lui comparer deux autres topologies.

Le graphe issu du modèle de Barabási-Albert comporte n nœuds et $m * (n - m)$ liens. n est fixé à 318. On souhaite que le nombre de liens soit de l'ordre de 519. Par conséquent, comme m est nécessairement entier, m peut prendre deux valeurs qui sont 2 et 316, le nombre de liens total étant alors 632. Le problème avec $m = 316$ est que le graphe est alors créé avec 316 nœuds non connectés et que seul deux noeuds sont ajoutés, chacun possédant 316 liens. La suppression de ces 2 nœuds provoquera alors la désintégration totale du réseau de télécommunication. Ce cas n'étant pas réaliste, les paramètres choisis pour l'établissement des graphes issus du modèle Barabási-Albert sont $n = 318$ et $m = 2$. Ce modèle de graphe faisant appel à des probabilités, deux créations successives avec les mêmes paramètres fourniront deux réseaux différents. Par conséquent, il n'est pas possible de se contenter que d'une seule étude.

Les résultats de la même étude que pour la topologie miroir sont présentés figure V.9. Il y a plusieurs courbes, car dix graphes différents issues du modèle Barabási-Albert ont été testés. En effet, ce modèle faisant appel à des probabilités, il engendre des graphes différents y compris avec les mêmes paramètres. Les remarques énoncées pour le $N - 1$ électrique pour la topologie miroir restent toutes valables pour cette topologie, on n'observe pas de différences majeures entre ces résultats.

Les résultats pour le $N - 1$ sur le réseau de communication sont présentés figure V.10. Les dix courbes présentées suivant la même évolution, on considère que la tendance reste la même pour les graphes issus de ce modèle. Dans ce cas, les différences entre la topologie miroir et le modèle Barabási-Albert sont plus importantes. La différence majeure s'observe pour des faibles valeurs du coefficient de tolérance (α proche de 0). Dans ce cas, il n'y a presque pas d'incidents de gravité 0 et une majorité de défaillance de gravité 3. On peut donc constater, pour le cas étudié et sous nos hypothèses, que pour de faibles valeurs de α, la topologie miroir est plus robuste que celles du modèle Barabási-Albert. Afin de faciliter la comparaison, les deux résultats ont été superposés figure V.11. Les résultats pour la topologie miroir sont en trait mixte et seulement deux courbes ont été tracées pour le modèle de Barabási-Albert. On remarque que pour des valeurs de α supérieures à 10, la topologie miroir donne moins d'incident de gravité nulle et plus d'incidents de gravité 1. Autrement dit, pour l'infrastructure étudiée, les réseaux issus du modèle Barabási-Albert permettent d'éviter des conséquences de faible gravité pour un coefficient de tolérance

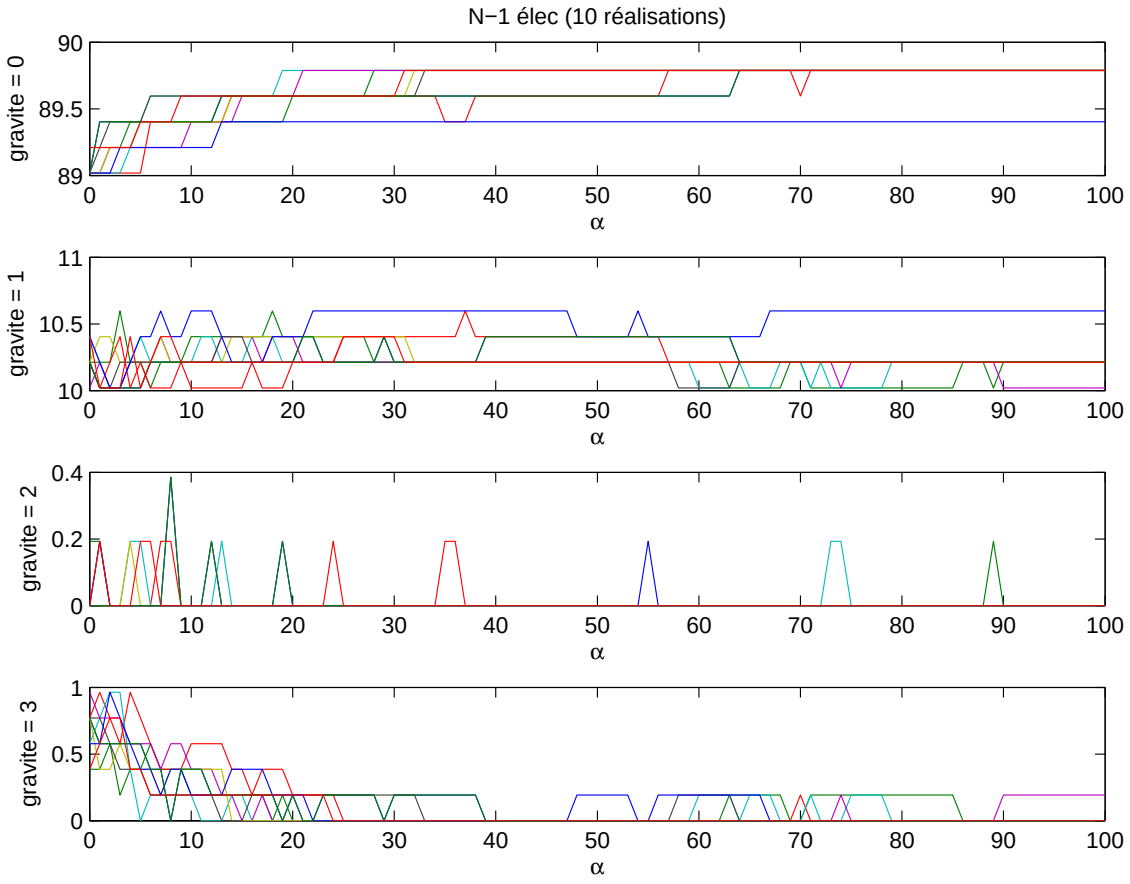

FIG. V.9 – Variation du pourcentage de la gravité pour un $N-1$ sur le réseau électrique (10 graphes issus du modèle Barabási-Albert)

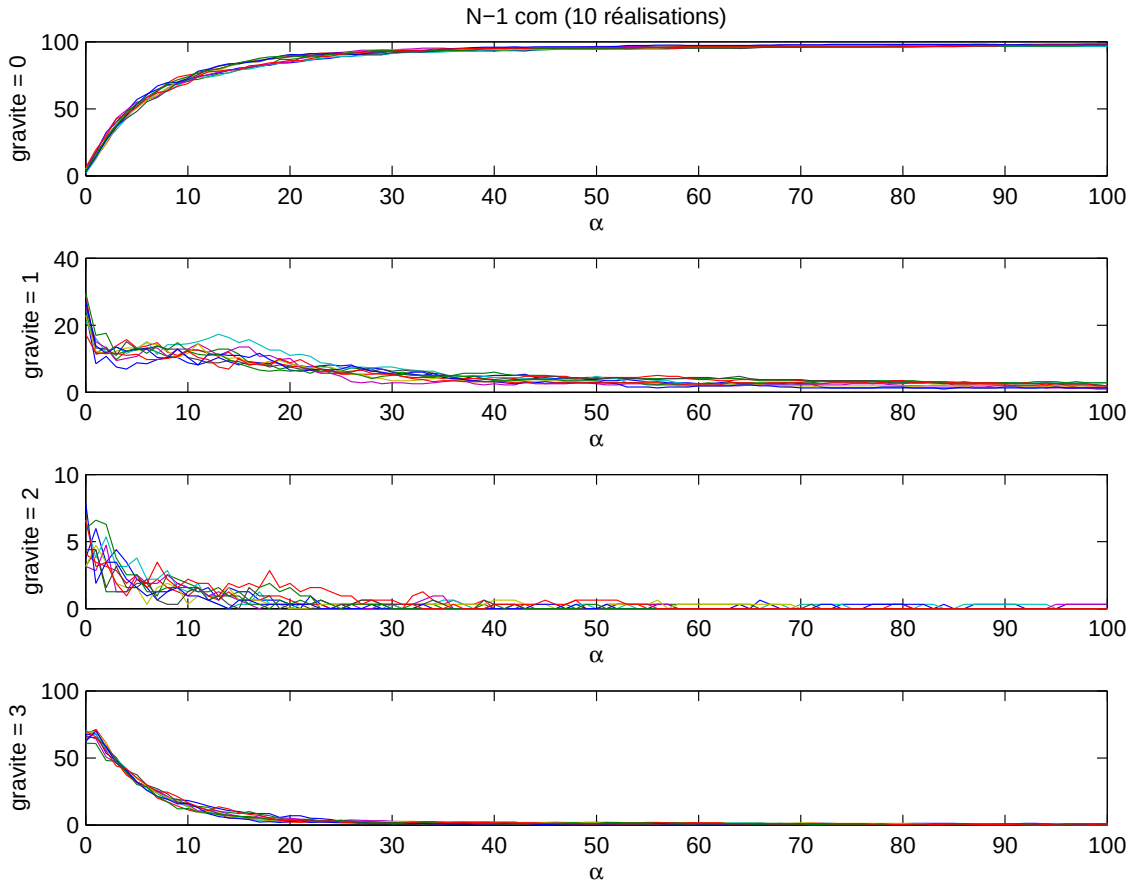

Fig. V.10 – Variation du pourcentage de la gravité pour un $N-1$ sur le réseau de communication (10 graphes issus du modèle Barabási-Albert)

supérieur à 10%. Pour les incidents de gravité 2 et 3 et $\alpha > 10\%$, les différences entre ces deux topologies ne sont pas très importantes.

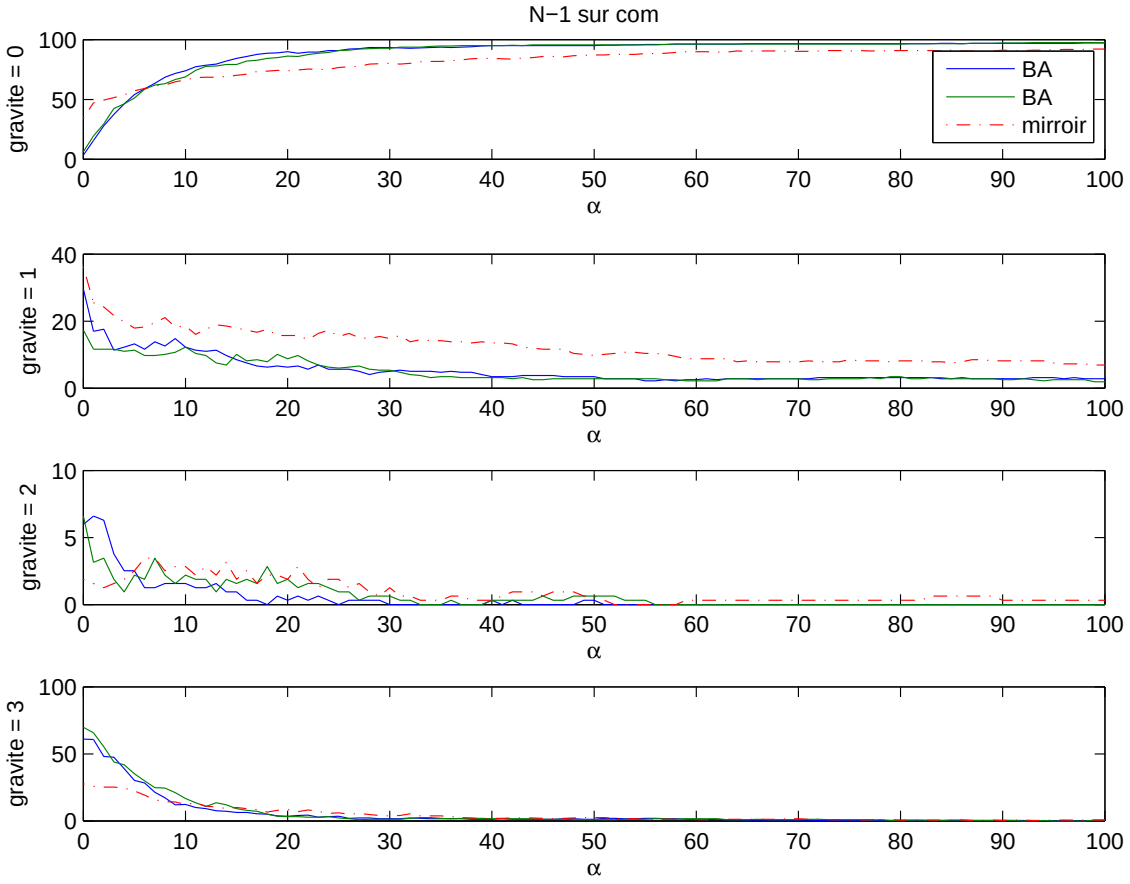

FIG. V.11 – Comparaison entre la topologie miroir et le modèle de Barabási-Albert (2 graphes) pour le réseau de communication

La troisième topologie étudiée est la grille de dimension 2. Une possibilité pour avoir 318 nœuds est d'utiliser une grille de taille 53×6. Cela donne un total de 577 liens de communication.

Les résultats pour cette topologie avec le $N-1$ réalisé sur le réseau électrique sont présentés figure V.12. Là encore, les allures sont semblables à la topologie miroir. La principale différence se situe pour α inférieur à 40% où il y a moins d'incidents sans gravité et plus avec une gravité de classe 1 ou 2. Pour ces valeurs du coefficient de tolérance, l'utilisation de la forme de grille pour le réseau de communication est moins bonne que les deux autres topologies étudiées.

Les résultats avec le $N-1$ sur le réseau de communication sont présentés figure V.13. On peux facilement identifier trois zones distinctes. La première est obtenue pour α inférieur à 40%. Dans ce cas, un incident sur le réseau de communication provoque un défaillance de classe 1 une fois sur deux et de gravité supérieure deux fois sur cinq. La seconde zone est obtenue pour α supérieur à 60%. Dans cette zone il n'y a plus de défaillance de classe 2 ou 3 et un très faible nombre de défaillance de gravité 1. Pour finir, entre ces deux zones, c'est-à-dire α compris entre 40% et 60%, il existe une troisième zone de transition où la

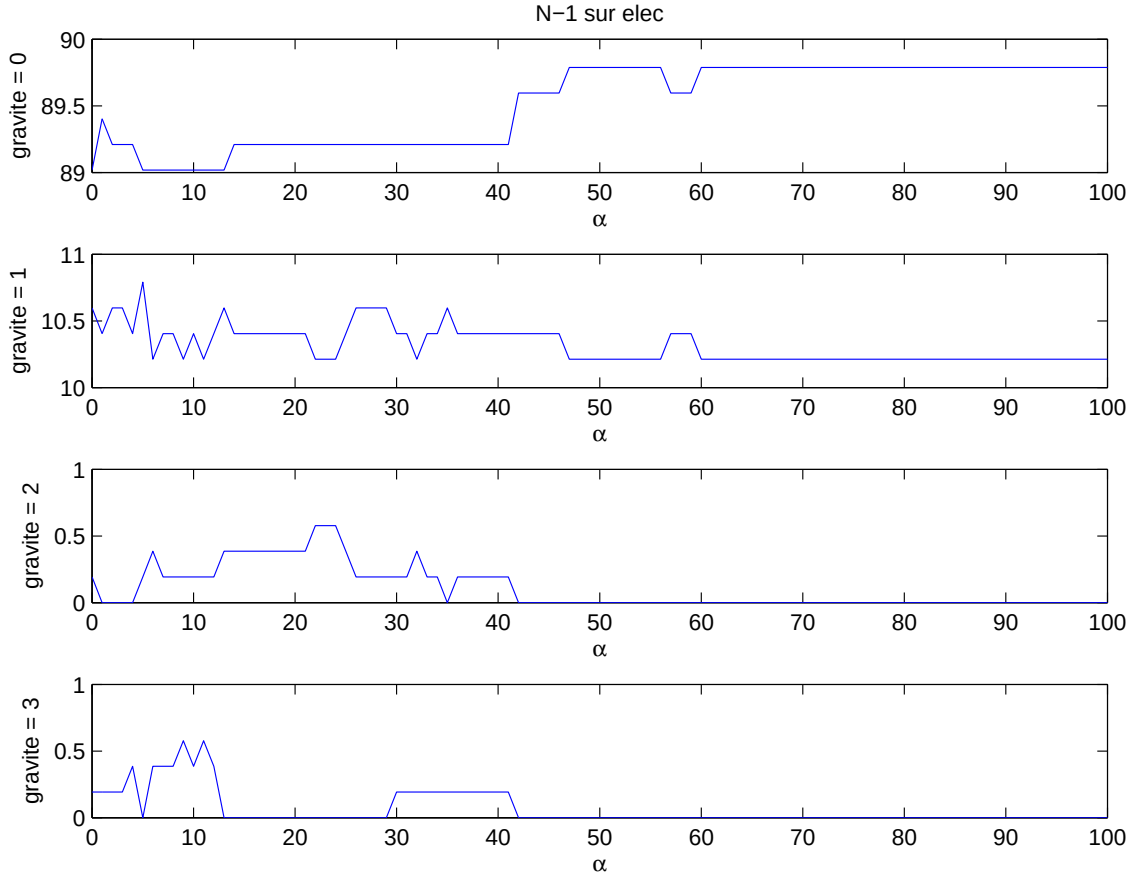

Fig. V.12 – Variation du pourcentage de la gravité pour un $N-1$ sur le réseau électrique (grille 2d)

proportion d'incident de gravité nulle augmente et celle de gravité non nulle décroît.

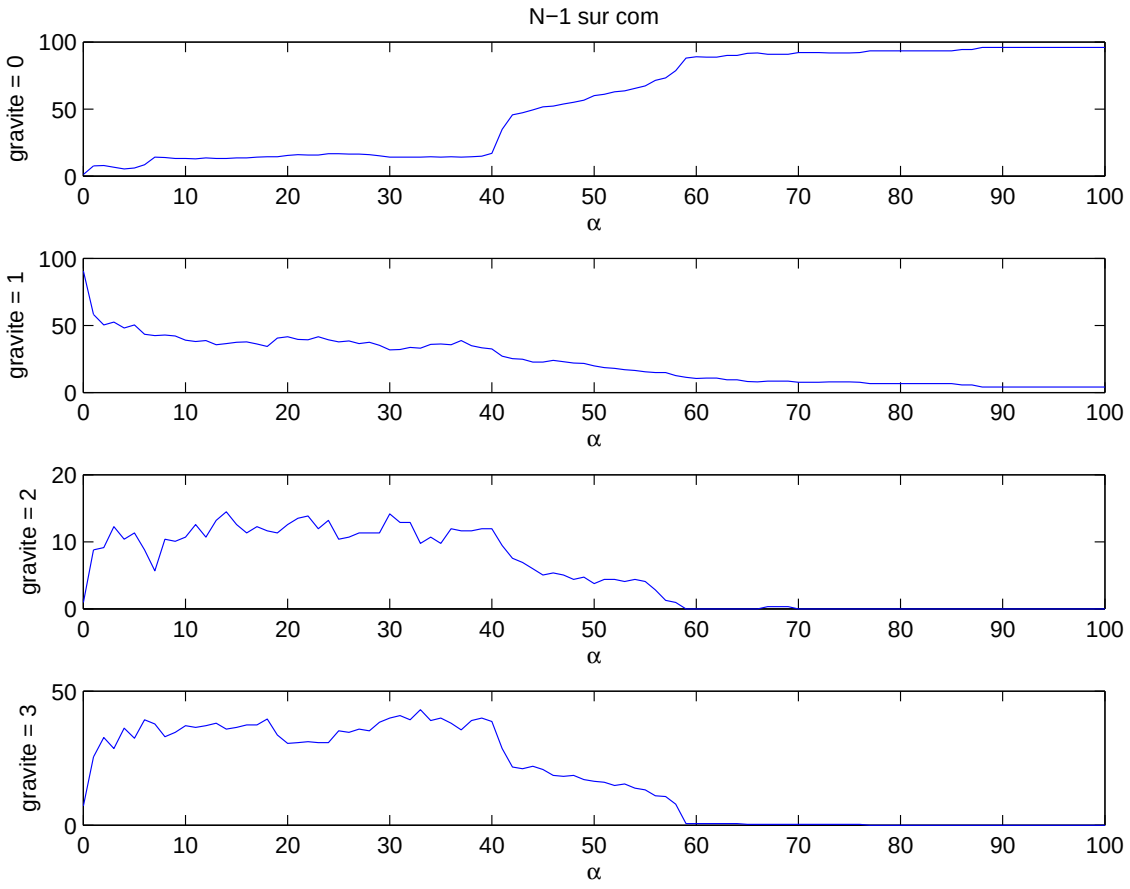

FIG. V.13 – Variation du pourcentage de la gravité pour un $N-1$ sur le réseau de communication (grille 2d)

Ainsi la topologie en forme de grille pour le réseau de communication offre de très mauvaises performances pour un dimensionnement trop juste ($\alpha < 40\%$) et de bonnes performances pour un dimensionnement plus large ($\alpha > 60\%$). Cet effet de seuil bien marqué est caractéristique de la grille.

Pour conclure, cette étude a montré que la topologie du réseau de télécommunication n'a qu'une faible influence sur les conséquences d'un incident d'origine électrique. Cette influence est certes faible, mais elle existe, d'où l'importance de prendre en compte l'infrastructure de communication et ses interdépendances. Elle a également montré que la topologie du réseau de communication a une plus grand importance sur les conséquences d'un incident se produisant dans ce réseau. En particulier, il a été montré que lorsque le réseau est suffisamment dimensionné, alors avoir un réseau de communication en miroir de l'infrastructure électrique n'est pas aussi bon qu'une topologie issue du modèle de Barabási-Albert et que dans le cas d'un réseau de communication en forme de grille, il doit être très bien dimensionné pour éviter de graves conséquences quasi systématiques.

V.4.d Étude de l'impact de deux incidents

Pour approfondir l'étude systématique des conséquences d'un incident, il peut être intéressant de regarder les conséquences de deux incidents simultanés. Cette étude s'appelle alors logiquement $N-2$. Le nombre de cas à étudier étant alors beaucoup plus important, il a été choisi de réaliser cette étude seulement pour une valeur du coefficient de tolérance pour le réseau de communication ($\alpha = 10\%$: c'est une valeur intermédiaire choisie à partir de l'étude $N-1$ réalisée ci-avant) avec la topologie miroir. Cette étude a été réalisée pour deux défauts sur le réseau électrique et également sur le réseau de communication.

La figure V.14 présente la matrice de gravité pour le $N-2$ systématique effectué sur le réseau électrique. L'abscisse et l'ordonnée correspondent tous deux à l'indice de la ligne électrique supprimée. La couleur bleu foncé correspond à la gravité 0, le bleu clair à la gravité 1, l'orange à la gravité 2 et le rouge à la gravité 3 (panne généralisée). Cette matrice est symétrique par construction. Il n'a été calculé que les points de la matrice supérieure, ceux de la matrice inférieure s'en déduisant. De plus, on retrouve les résultats de l'étude $N-1$ sur la diagonale. La première constatation est que la majorité des points correspondent à une gravité nulle, preuve de la robustesse du réseau. Ensuite, il y a de nombreuses lignes (verticales et horizontales). En effet, lorsqu'un défaut seul provoque un incident, il est fortement probable qu'avec un second incident ajouté à ce premier, les conséquences seront similaires. De plus, on peut remarquer l'existence d'une ligne rouge (indiquée par les flèches) correspondant à la suppression d'une ligne provoquant par cascade une panne généralisée. Il est intéressant de remarquer que sur cette ligne se situent des points de gravité 2, voir 1 ou 0. Cela signifie donc que le second défaut permet de limiter la conséquence du premier. Alors que cela peut paraître contre intuitif, ce phénomène peut s'expliquer aisément sur un exemple simple. En effet, imaginons un gros consommateur ou un gros producteur connecté au reste du réseau par seulement deux lignes. La suppression d'une seule des lignes, va provoquer un report de charge dans l'autre, qui peut ensuite surcharger les lignes amonts et provoquer une cascade aboutissant à une panne généralisée. Tandis que si ces deux lignes sont enlevés simultanément, alors le nœud du consommateur ou producteur se retrouvera isolé et donc supprimé. La cascade d'événements pourra s'arrêter là, provoquant ainsi moins de conséquences négatives. Cela est équivalent à supprimer un domino sur un chemin de dominos afin d'éviter que la chute du premier entraîne par réaction en chaîne l'écroulement de l'ensemble. Cette matrice permet donc de proposer des contre-mesures permettant de limiter les conséquences d'un défaut en effectuant la suppression préventive d'un élément.

La figure V.15 présente la matrice de gravité (avec la même convention de couleur) pour deux défauts effectués simultanément sur le réseau de télécommunication. Les coordonnées représentent maintenant les indices des nœuds de communication supprimés. Les résultats obtenus sont analogues au $N-2$ précédent et donc l'ensemble des conclusions alors énoncées restent valables.

Pour conclure, l'étude $N-2$ permet de connaître le comportement du système étudié dans le cas de deux défauts. Cela permet en particulier d'identifier des contre-mesures de mitigation des défaillances pouvant conduire à une panne généralisée au prix d'un temps de simulation plus important.

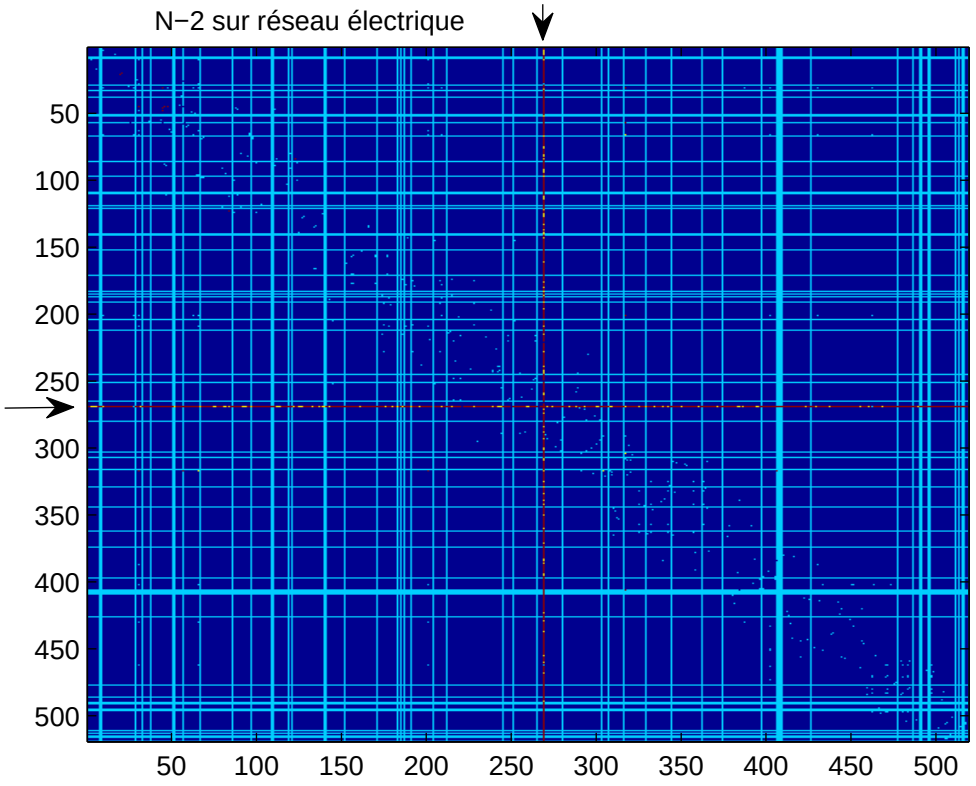

FIG. V.14 – Matrice de gravité pour un $N-2$ sur le réseau électrique

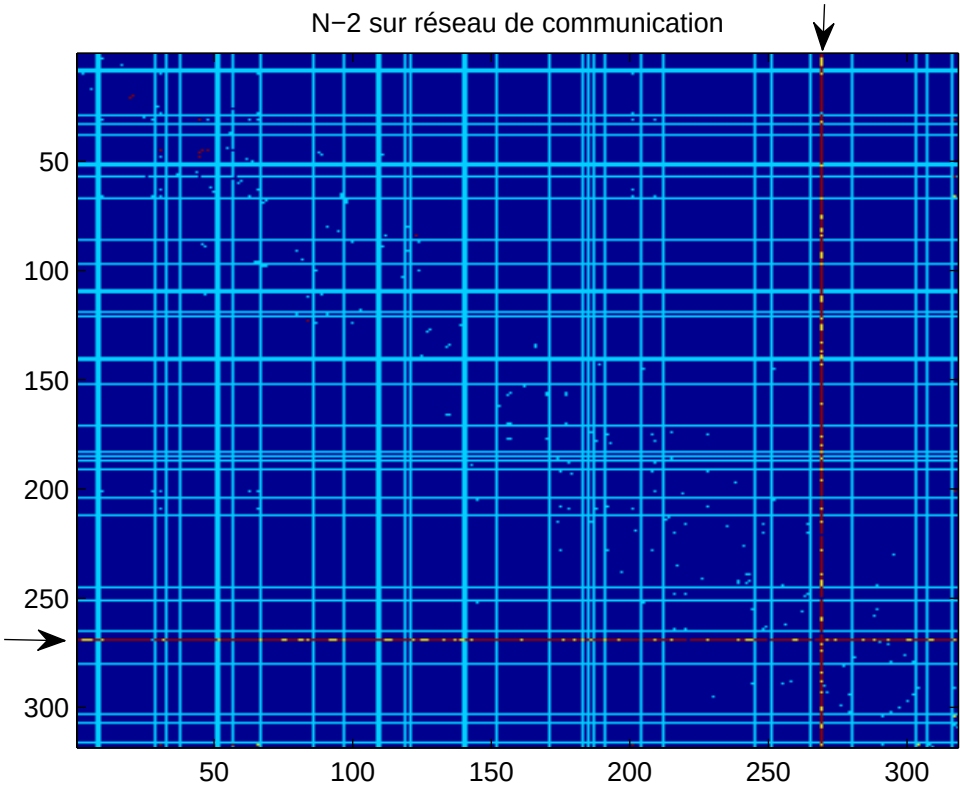

Fig. V.15 – Matrice de gravité pour un $N-2$ sur le réseau de communication

V.4.e Étude des défauts géographiques

Après avoir étudié l'impact de deux défauts se déroulant dans la même infrastructure, il peut être intéressant d'étudier l'impact de deux défauts simultanés, mais chacun dans une infrastructure différente. Ce genre d'incident est le cas typique d'un défaut de mode commun de type géographique et localisé. Ainsi, le défaut initial sera la suppression d'un nœud électrique et par conséquent suppression des lignes connectées à ce nœud ainsi que la suppression du nœud de télécommunication associé. Tout comme l'étude du $N-2$, cette étude des défauts de mode commun localisés a été réalisée sur le réseau français, avec une infrastructure de communication ayant la topologie miroir et un coefficient de tolérance $\alpha = 10\%$. Les résultats avec des éléments de comparaison sont présentés dans le tableau V.2.

Tab. V.2 – Répartition des incidents pour des défauts géographiques

gravité	0	1	2	3
Défaut géographique localisé	8,2%	72,0%	3,1%	16,7%
N-1 suppression de nœud élec sans réseau de com	15,1%	84,3%	0,3%	0,3%
N-1 classique sur le réseau de com	66,3%	18,6%	2,8%	12,3%

La première ligne correspond à un défaut touchant chaque nœud électrique et le nœud de communication associé. On peut la comparer avec la seconde ligne qui représente un $N-1$ sur les nœuds électriques tel qu'il est habituellement réalisé par les gestionnaires de réseaux de transport, c'est-à-dire sans considérer l'influence du réseau de télécommunication sur le réseau électrique. On constate que le fait de considérer le réseau de communication augmente fortement la proportion d'incident ayant un impact non nul et en particulier supérieur à 10% de la puissance non distribuée. La troisième ligne reprend les résultats du $N-1$ sur le réseau de communication tel que effectué dans les sous-sections précédentes. Comme l'on pouvait s'y attendre, le fait d'avoir un défaut en plus dans le réseau électrique, c'est-à-dire un mode commun plutôt qu'un défaut simple, diminue considérablement le nombre d'incidents sans gravité et par conséquent augmente la proportion d'incidents de gravité non nulle.

V.4.f Étude sur d'autres réseaux électriques

L'étude paramétrique de l'impact du coefficient de tolérance pour le $N-1$ systématique sur le réseau électrique et sur le réseau de communication a également été réalisée sur d'autres réseaux électriques (avec leur infrastructure de communication associée). Le but est de vérifier si les tendances observées sur le cas de référence sont toujours valables quelque soit le réseau (réaliste) considéré : c'est-à-dire vérifier la non versatilité des résultats.

Réseau de l'UCTE

Le premier cas d'étude choisi est l'ensemble du réseau de transport de l'UCTE, c'est à dire la même topologie que celle étudiée au chapitre 4. Par contre, dans ce cas, l'impédance

des lignes électriques est prise en considération. La taille du réseau est très grande et donc mène à des temps de simulation importants. L'étude a alors due être limitée à la topologie miroir pour le réseau de communication.

Les résultats obtenus pour le $N-1$ sur le réseau électrique sont présentés figure V.16. Pour l'établissement de ces courbes, 101 valeurs de α ont été testées.

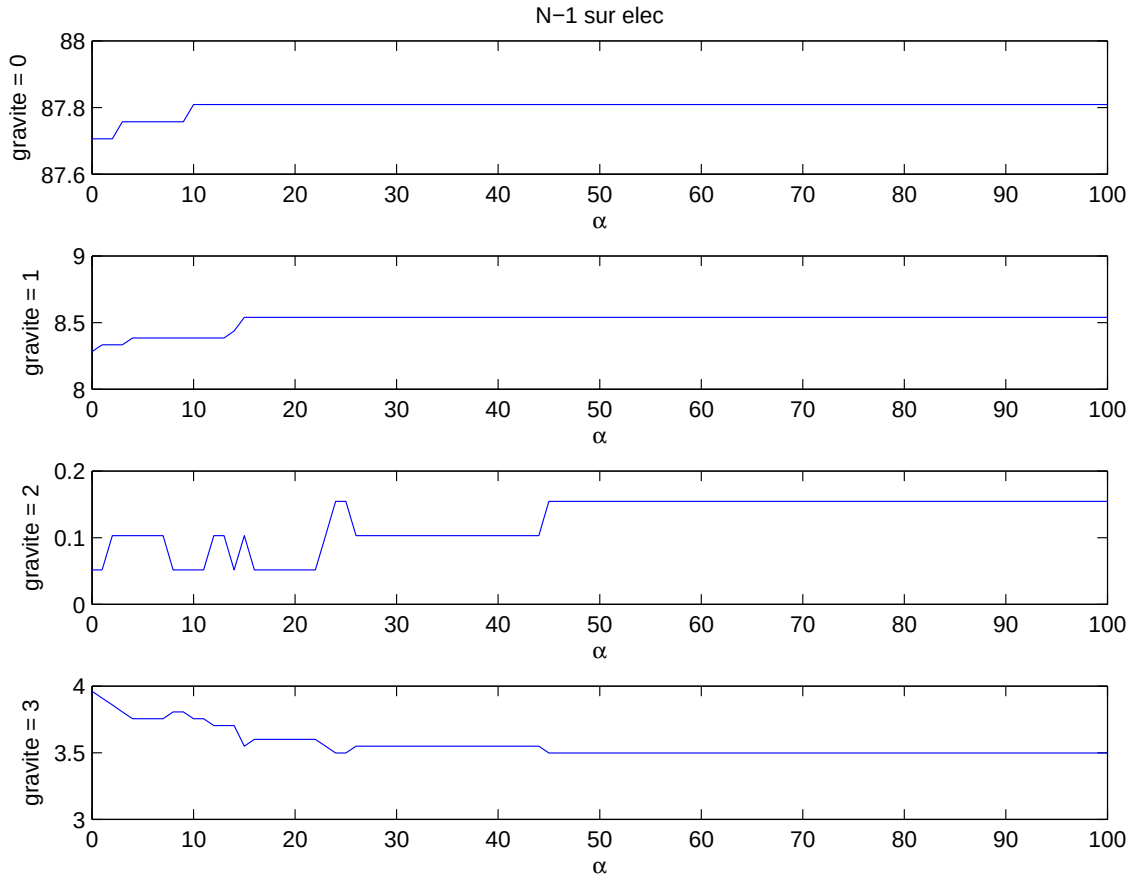

Fig. V.16 – Variation du pourcentage de la gravité pour un $N-1$ sur le réseau électrique de l'UCTE

On remarque que la tendance est identique pour les incidents sans gravité. Par contre, ceux de gravité 3 sont beaucoup plus nombreux (entre 3,5 et 4%). Le réseau étudié est donc plus sensible à un écroulement complet que le cas de référence (réseau français). En effet, pour le cas de référence, l'ensemble de la production avait été baissée de 8% afin d'être équilibrée avec la consommation. Le réseau disposait alors de plus de marges et était donc dans un état moins critique lui permettant de mieux résister à la suppression d'éléments. Pour le cas de l'UCTE, on remarque également que les proportions d'incidents de gravité 1 et 2 augmentent lorsque le coefficient de tolérance est plus important, ce qui peut sembler anormal. Cela s'explique tout simplement par le fait qu'il y a plus d'incidents de gravité 3 dont les conséquences diminuent vers ces catégories que d'incidents de ces catégories se transformant en gravité nulle. Pour rappel, les catégories de gravité sont mutuellement exclusives.

Les résultats pour le $N-1$ sur le réseau de télécommunication sont présentés fi-

gure V.17. Vu la durée des simulations, seules dix valeurs du coefficient de tolérance ont été testées : 0, 5, 10, 15, 20, 25, 30, 40, 50 et 100.

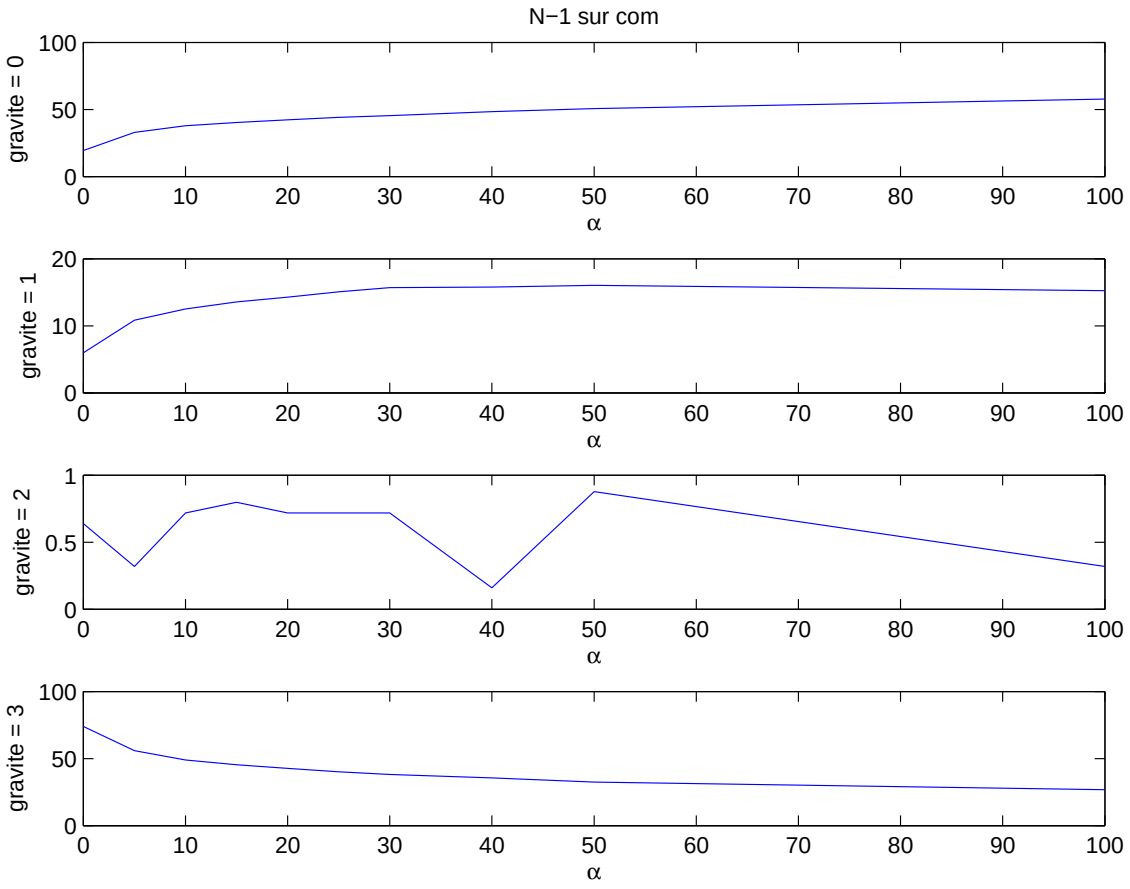

FIG. V.17 – Variation du pourcentage de la gravité pour un $N-1$ sur le réseau de communication de l'UCTE

On retrouve les mêmes constatations que le $N-1$ sur le réseau électrique. Ainsi, il y a beaucoup plus d'incidents de gravité non nulle dûs à l'état de fonctionnement du réseau plus proche de ses limites. On observe également des tendances identiques pour les incidents de gravité 0 et 3 que sur le réseau français et les incidents de gravité 1 augmentent avec le facteur α du fait de la baisse de la gravité 3 plus que de l'augmentation de la gravité 0. Les incidents de gravité 2 sont toujours minoritaires (inférieurs à 1%) et leurs variations ne sont pas trop significatives.

Réseau IEEE 300 nœuds

Afin de pouvoir vérifier que les effets de taille ne sont pas la cause des différences entre le réseau français et celui de l'UCTE dans son ensemble et également pour pouvoir étudier les autres topologies du réseau de communication, la même étude que celle sur le réseau français a été effectuée sur un autre réseau de transport d'énergie ayant un nombre de nœuds équivalent. Le réseau choisi est un réseau d'étude IEEE qui a été développé par

la *IEEE Test Systems Task Force* sous la direction de Mike Adibi en 1993[1]. Ce réseau comporte 300 nœuds et 411 lignes. Il est décrit au format IEEE en annexe A.

Ici, contrairement au réseau de l'UCTE, on dispose des données complètes permettant de réaliser un calcul de répartition de charge classique (méthode de Newton-Raphson), c'est-à-dire sans les hypothèses simplificatrices du *DC load flow* (V.2.c). Cela permet donc d'évaluer l'erreur réalisée par cette dernière méthode. Ces deux calculs de répartition de charge ont été réalisés et on a ensuite calculé l'erreur relative apportée par les hypothèses du *DC load flow*. L'histogramme de cette erreur est représenté figure V.18, chaque barre verticale ayant une largeur de 1%. On constate que 84 lignes ont une puissance dont l'erreur est inférieure à 1%, 268 lignes pour un seuil de 10% et 381 lignes ont une erreur de puissance calculée inférieure à 100%. Il existe donc 30 lignes sur 411 dont l'erreur relative due aux hypothèses du *DC load flow* dépasse les 100% (non représentées sur l'histogramme).

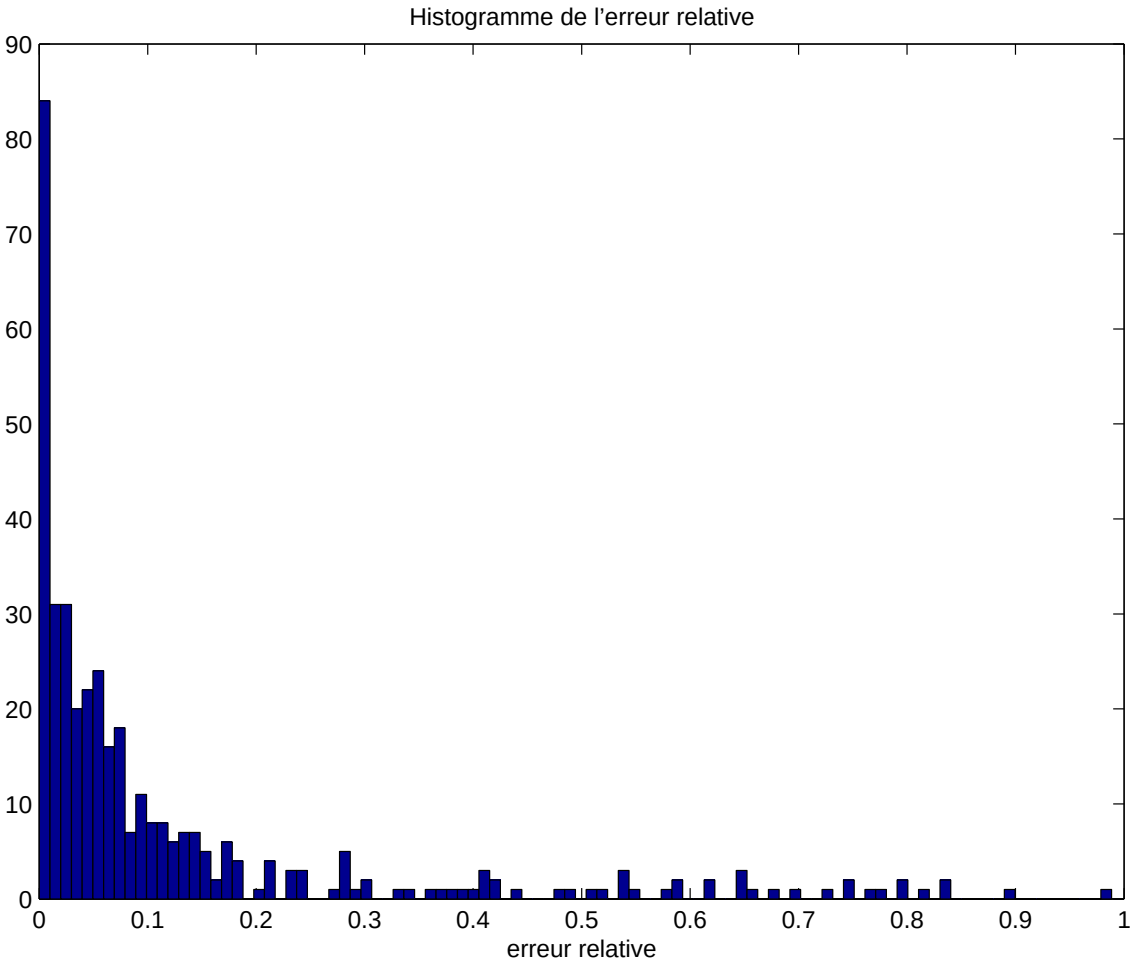

Fig. V.18 – Histogramme tronqué de l'erreur relative entre le calcul de répartition de charge (Newton-Raphson) et le *DC load flow*

Cette comparaison permet d'évaluer l'erreur commise par le choix du mode de calcul de répartition de charge. Dans la modélisation proposée, le *DC load flow* apporte un bon

[1]Les données de ce réseau sont disponibles à l'adresse `http://www.ee.washington.edu/research/pstca/pf300/pg_tca300bus.htm`

compromis entre la précision obtenue et la rapidité du calcul.

Les résultats des deux études paramétriques vis à vis du coefficient de tolérance du réseau de communication α pour un défaut initial dans chaque graphe sont présentés figures V.19 et V.20.

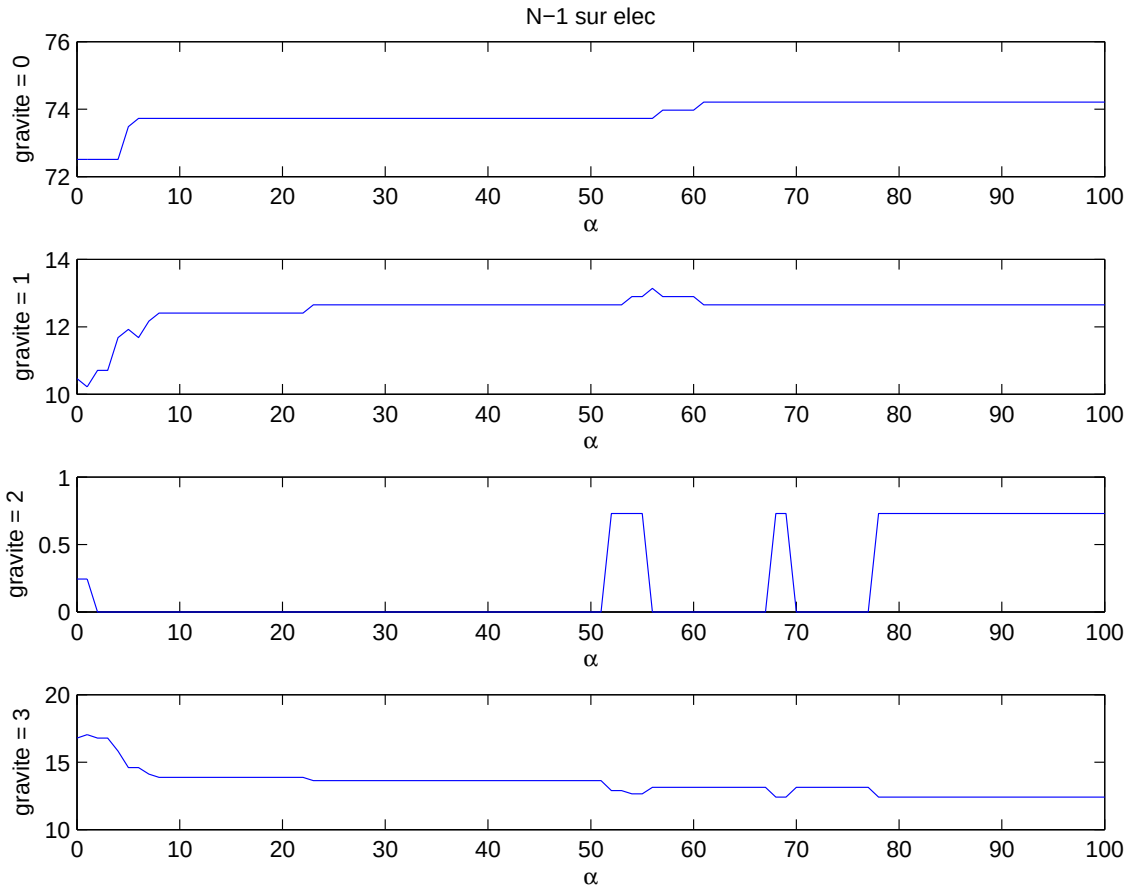

FIG. V.19 – Variation du pourcentage de la gravité pour un $N-1$ sur le réseau électrique IEEE 300 nœuds (miroir)

Comme pour le réseau de l'UCTE, le point de fonctionnement du 300 nœuds est plus proche de ses limites et, par conséquent, on observe une bonne proportion d'incidents de gravité non nulle. Les incidents de gravité 2 sont toujours en très faible nombre. Et les tendances des courbes pour les autres catégories de gravité sont identiques à celles de l'UCTE.

Pour les deux $N-1$, on observe un phénomène de baisse brusque des pannes généralisée pour α proche de 4% se reportant sur une augmentation des incidents de gravité 1. Enfin, on peut remarquer que la valeur de α n'a dans ce cas aucune influence sur le nombre d'incidents sans conséquences lorsque le défaut initial a lieu sur le réseau de communication.

La taille du réseau a permis l'étude des deux autres modèles de topologie. Ainsi, il a été étudié des graphes du réseau de communication construits à partir de modèle de Barabási-Albert. Les paramètres choisis sont $n = 300$ et $m = 2$ ce qui donne un total de 596 liens. Chaque étude a été réalisée sur deux constructions de graphe du réseau de communication différentes.

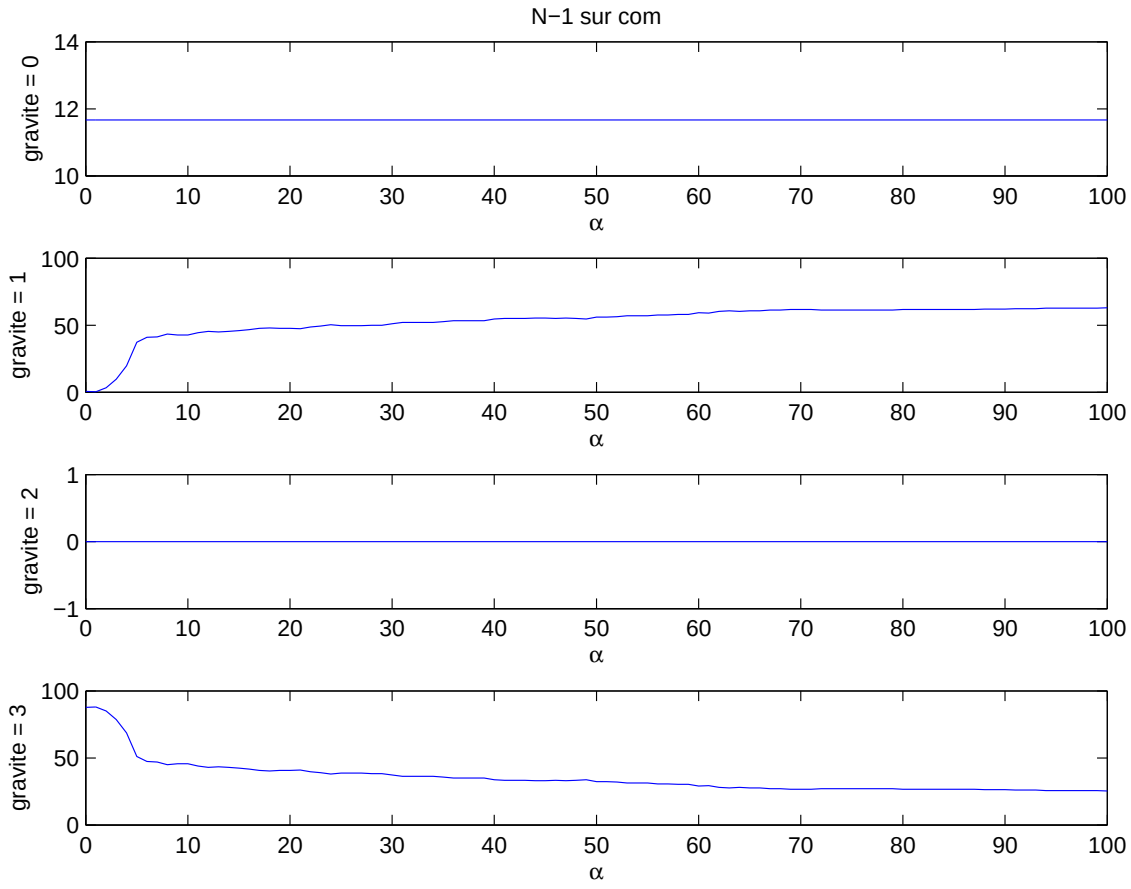

Fig. V.20 – Variation du pourcentage de la gravité pour un $N-1$ sur le réseau de communication IEEE 300 nœuds (miroir)

Les résultats montrant la variation du pourcentage de la gravité pour un $N-1$ sur le réseau électrique sont présentés figure V.21. On observe des différences entre les variations des courbes des dix réalisations, montrant une fois encore, que la topologie réseau de communication a une influence sur la robustesse du réseau électrique. Comme pour les autres $N-1$, les variations en fonction du coefficient de tolérance sont plus importantes lorsque le défaut initial a lieu dans le réseau de communication. La figure V.22 présente ces résultats. Par rapport à la topologie miroir, ce modèle de graphe est bien moins robuste. En effet, on n'observe quasiment pas d'incidents de gravité 1, seulement 10% de gravité 0 et donc près de 90% de pannes généralisées. Sept fois sur les dix graphes testés, la valeur de α n'a que peu d'influence sur la robustesse sauf lorsqu'elle est inférieure à 10% ou quasiment tous les défauts de communication aboutissent alors à un incident de gravité 3.

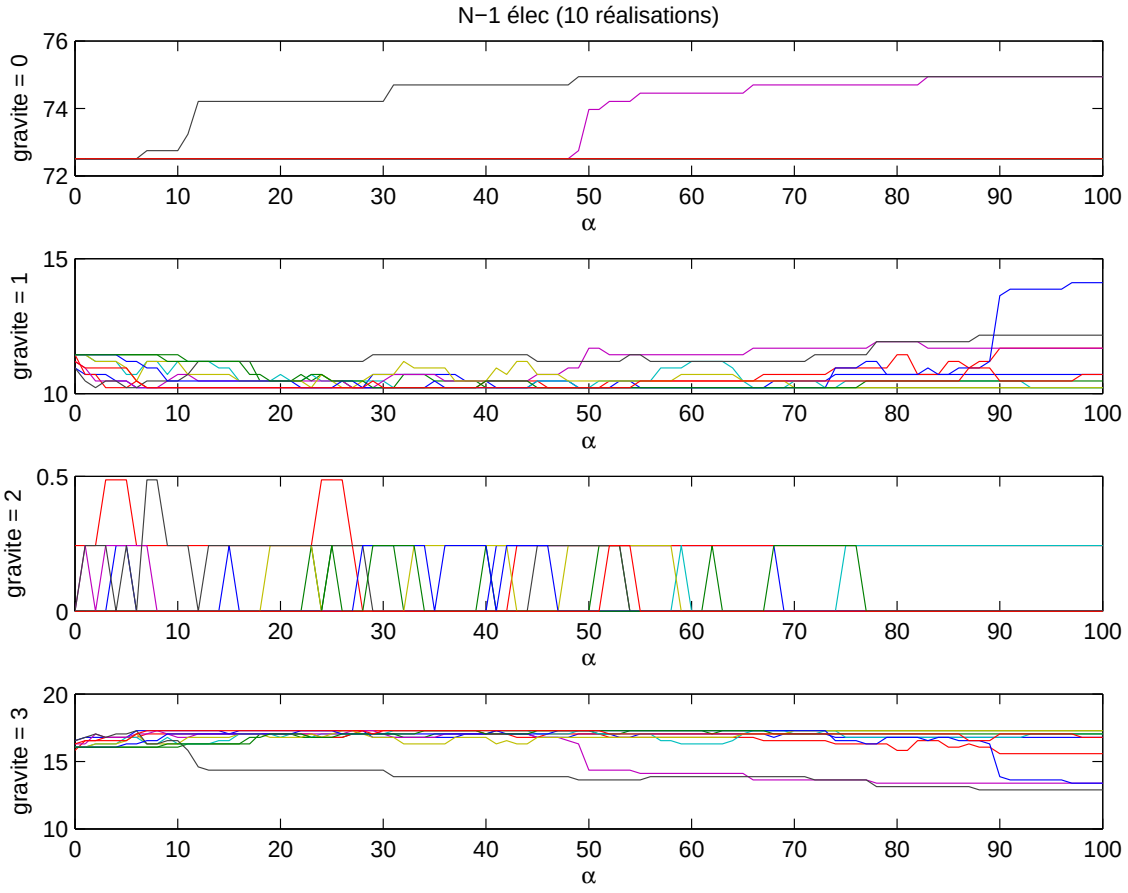

FIG. V.21 – Variation du pourcentage de la gravité pour un $N-1$ sur le réseau électrique IEEE 300 nœuds (Barabási-Albert)

La topologie grille a également été étudiée. Les 300 nœuds ont été alors disposés en une grille de taille 20×15, soit un total de 565 liens. Les résultats sont présentés figure V.23 pour le $N-1$ sur le réseau électrique et figure V.24 pour le $N-1$ sur le réseau de communication. Les proportions pour chaque gravité sont du même ordre de grandeur que celles pour la topologie miroir. Et comme pour le réseau français, on retrouve de manière très flagrante l'effet de seuil avec les trois comportements différents en fonction du coefficient de tolérance : beaucoup de pannes généralisées pour α inférieur à 25% (et non

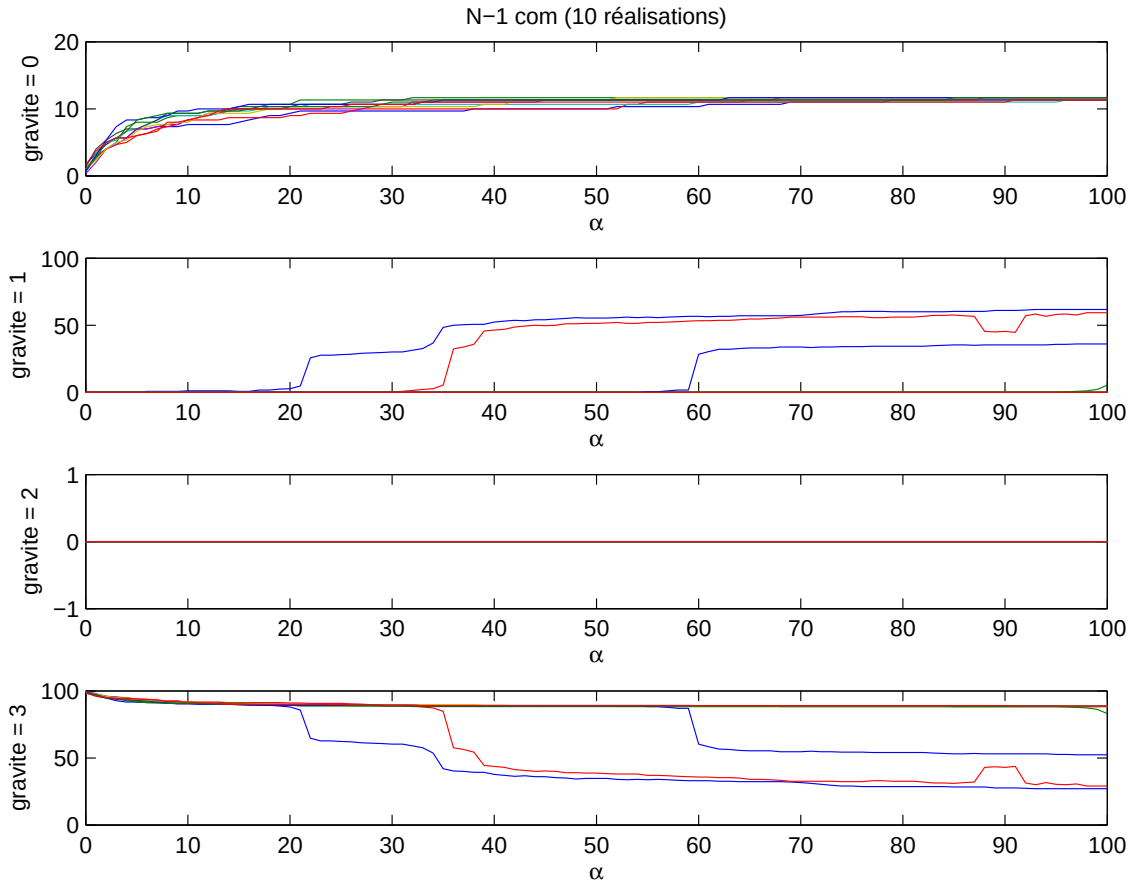

Fig. V.22 – Variation du pourcentage de la gravité pour un $N-1$ sur le réseau de communication IEEE 300 nœuds (Barabási-Albert)

40% comme pour le réseau français), une meilleure robustesse pour α très grand (supérieur à 70%) et une zone de transitions entre les deux.

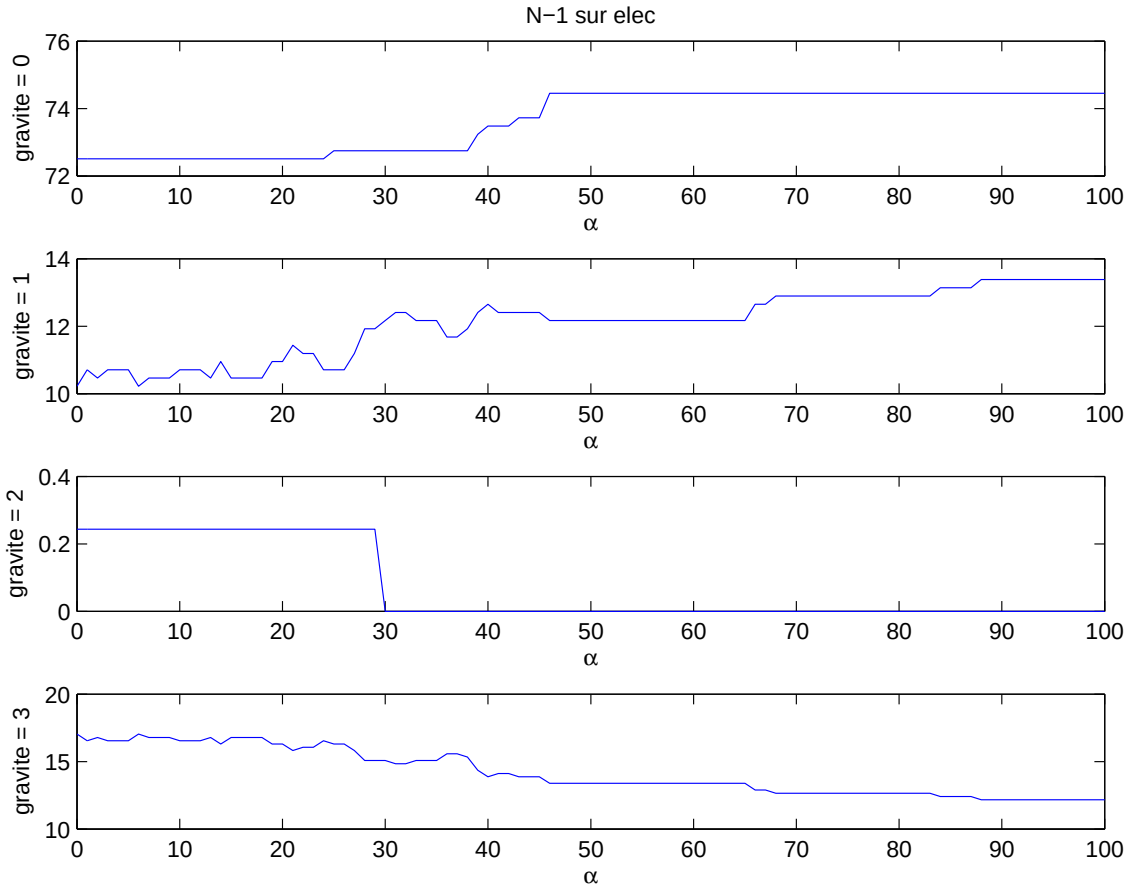

FIG. V.23 – Variation du pourcentage de la gravité pour un $N-1$ sur le réseau électrique IEEE 300 nœuds (grille)

Bilan de l'étude sur d'autres réseaux électriques

De l'ensemble des cas d'étude présentés, il est possible de dégager des tendances générales. Tout d'abord, pour effectuer une comparaison entre deux réseaux différents, il faut garder à l'esprit que l'état de fonctionnement initial influe fortement sur les résultats. Ainsi, il n'est pas possible de simplement se contenter des chiffres obtenus dans l'absolu pour affirmer qu'un réseau est meilleur qu'un autre. Ce comportement, même s'il ne facilite pas l'exploitation des résultats, est normal. En effet, plus un réseau est chargé, plus le phénomène de cascade sera susceptible de se produire.

En ce qui concerne les topologies, il a été montré que la grille n'est satisfaisante que si le coefficient de tolérance est important. La topologie miroir produit des résultats corrects et surtout ayant une plus faible sensibilité à α. Ainsi, elle est bien adaptée dans les études pour être prise comme cas de référence.

Dans tous les cas, lorsque le $N-1$ est effectué sur le réseau de télécommunication, il y a plus de variations dues aux changement de topologie ou de α que lorsqu'il est réalisé

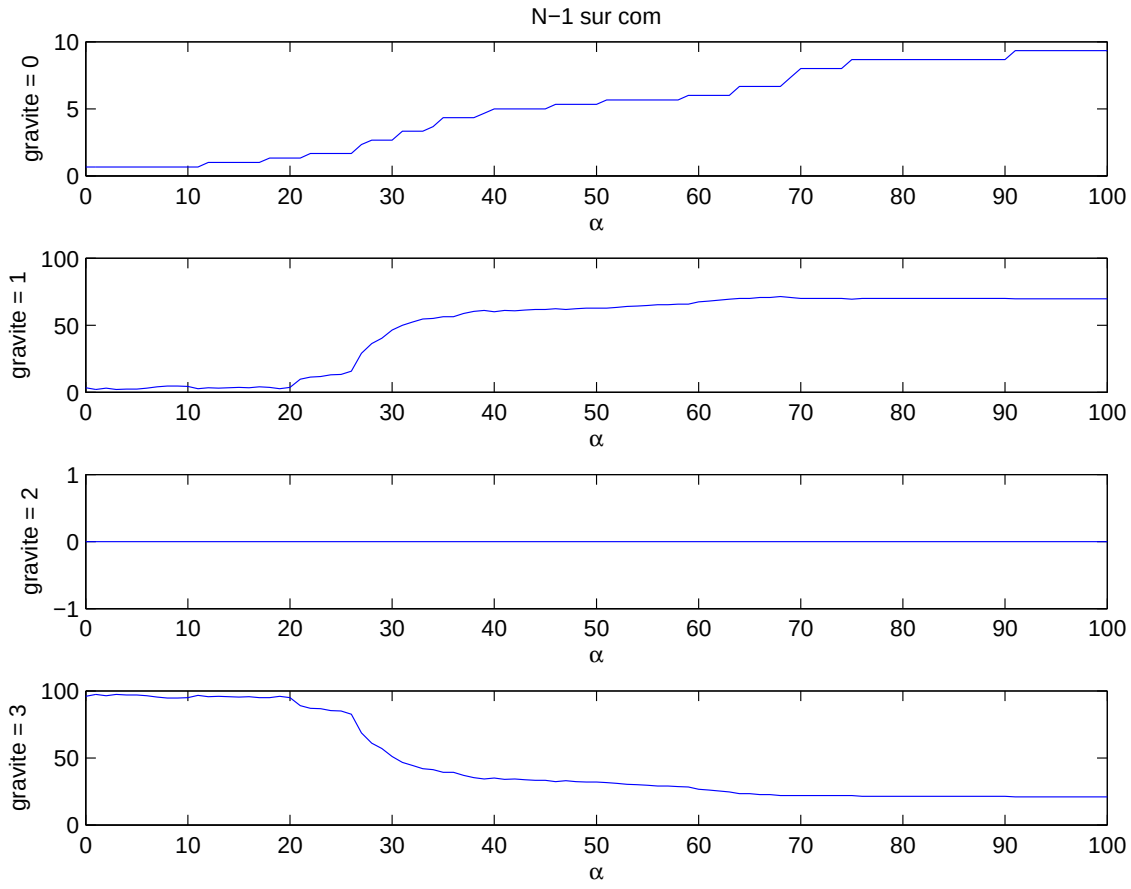

Fig. V.24 – Variation du pourcentage de la gravité pour un $N-1$ sur le réseau de communication IEEE 300 nœuds (grille)

sur le réseau électrique.

Enfin, le réseau de communication en terme de topologie et également de coefficient de tolérance a toujours une influence sur ce qui se passe sur le réseau électrique. Il doit donc être choisi précisément.

V.4.g Influence d'une hypothèse d'interdépendance

Après avoir étudié l'influence de la topologie du réseau de communication et de son dimensionnement et après avoir vérifié la non versatilité des résultats obtenus, il est nécessaire de reconsidérer l'hypothèse la moins triviale, celle de la règle d'interdépendance du réseau de communication envers le réseau électrique.

Pour cela, la démarche utilisée a été de remplacer la suppression systématique de la ligne la plus chargée de la zone suite à une suppression de routeur de communication par une probabilité que cette suppression ait lieu. Cette valeur de probabilité peut varier de un (ce qui correspond à l'ensemble des cas étudiés précédemment) à zéro, ce qui est équivalent à une non prise en compte de l'effet d'interdépendance du réseau électrique envers l'infrastructure de communication.

Deux couples d'infrastructures ont été étudiés afin de, là encore, vérifier la non versatilité des résultats. Il s'agit du réseau électrique français avec le réseau de communication en miroir et $\alpha = 10\%$ et du réseau IEEE 300 nœuds avec le réseau de communication en miroir également et $\alpha = 100\%$. Ce coefficient de tolérance a été choisi plus grand car, comme il a été vu précédemment, ce réseau fonctionne plus près de ses limites électriques que le précédent. Cinq différentes valeurs de probabilité ont été étudiées : 1, 3/4, 1/2, 1/4 et 0. Pour les trois valeurs intermédiaires, les résultats de l'exécution ne sont pas déterministes et, par conséquent, chaque simulation a été réalisée 100 fois afin de pouvoir dégager des tendances. Pour chacun de ces cas, sont représentés sur les figures les proportions maximales et minimales et le tracé correspond à la valeur moyenne obtenue.

Les résultats pour le $N-1$ sur le réseau électrique sont présentés figure V.25 pour le réseau français et figure V.26 pour le réseau IEEE 300 nœuds. Dans les deux cas, on remarque que la baisse significative du nombre de pannes généralisées se fait entre les valeurs de probabilité 1/4 et 0. Ainsi, choisir une probabilité de 1 pour cette interdépendance ne change que peu le résultat obtenu par rapport à une probabilité de 1/4.

La sensibilité à cette valeur de probabilité est beaucoup plus importante lorsque le défaut initial se produit dans le réseau de communication. Les résultats de ces cas d'étude sont présentés figure V.27 et V.28 pour respectivement le réseau français et le IEEE 300 nœuds.

Le cas où la probabilité a une valeur nulle, c'est-à-dire lorsque un problème sur le réseau de communication n'a aucun impact sur l'infrastructure électrique provoque, comme attendu, aucun incident de gravité 1 ou supérieur et donc une totalité d'incidents sans impacts. Lorsque la probabilité vaut l'unité, alors on retrouve le cas étudié auparavant. Entre ces deux extrêmes, la variation est linéaire dans le cas du réseau IEEE 300 nœuds. Pour le réseau français, on peut remarquer tout d'abord une légère augmentation des incidents de faible gravité lorsque la probabilité passe de 1 à 1/2. Cette augmentation est due à la diminution des incidents de gravité moyenne ou forte, incidents dont l'impact se réduit sans pour autant s'annuler. Ensuite toutes les proportions de gravité non nulle se

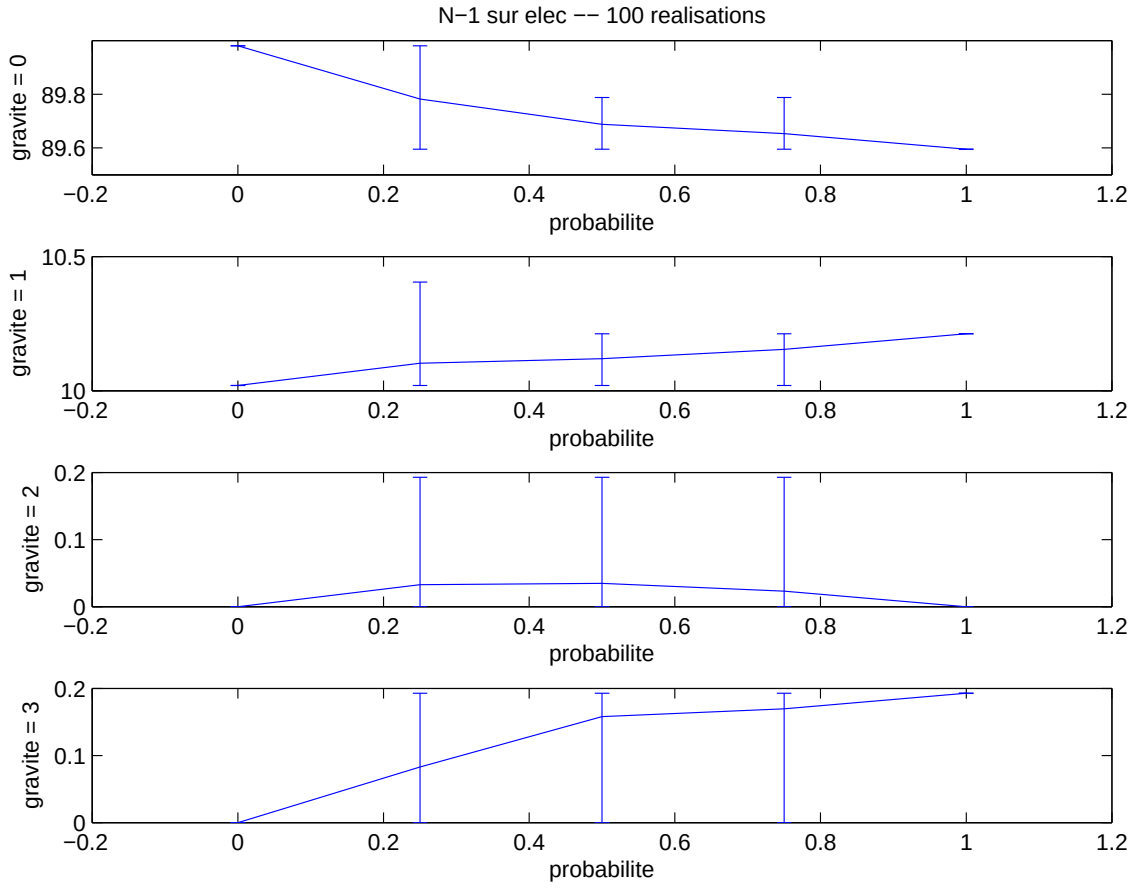

Fig. V.25 – Évolution de la gravité en fonction de la probabilité de l'interdépendance pour un $N-1$ électrique (France)

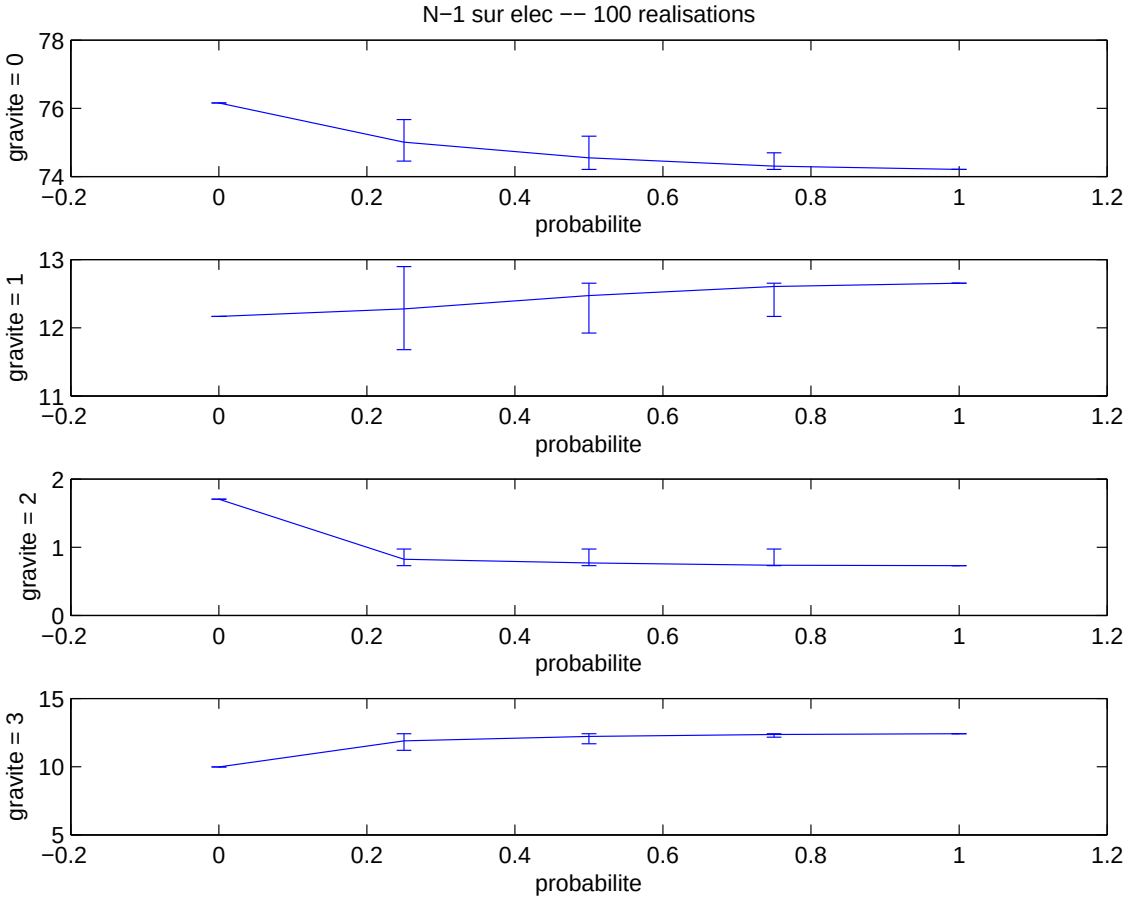

FIG. V.26 – Évolution de la gravité en fonction de la probabilité de l'interdépendance pour un $N-1$ électrique (300 nœuds)

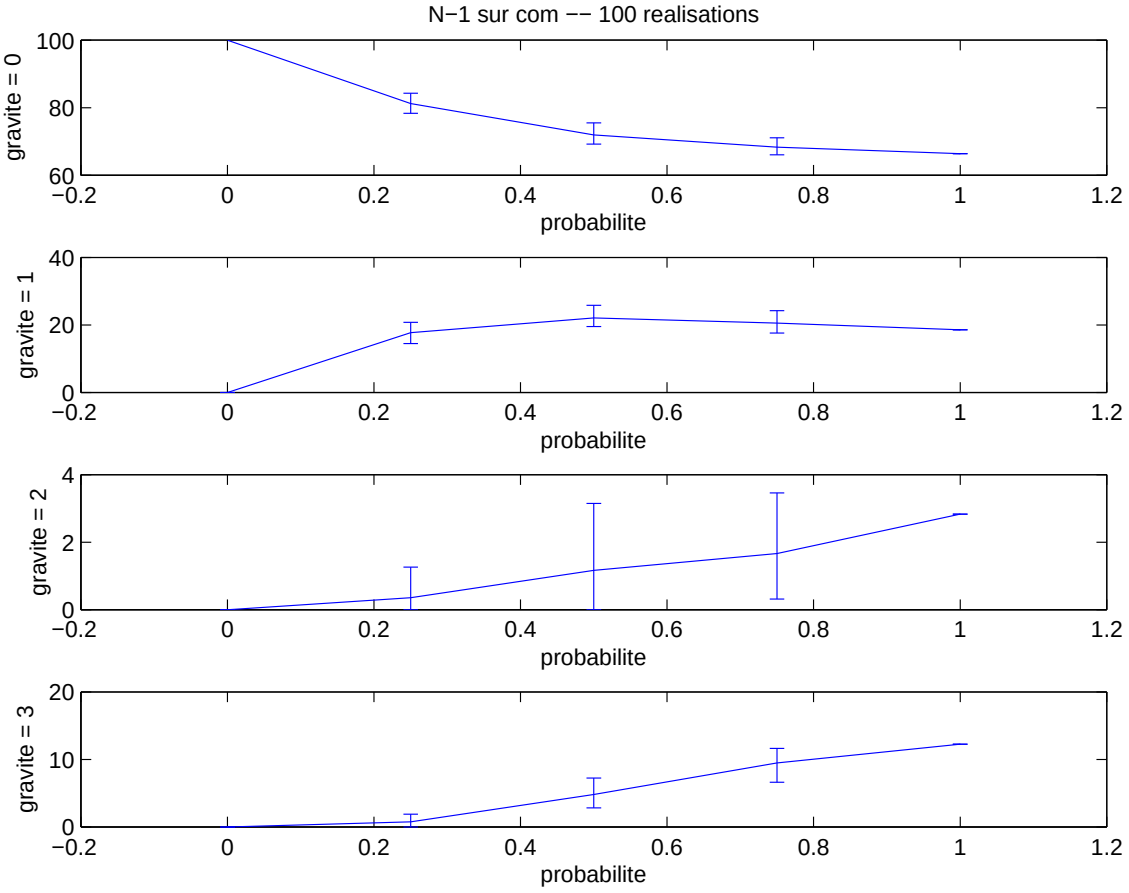

Fig. V.27 – Évolution de la gravité en fonction de la probabilité de l'interdépendance pour un $N-1$ de communication (France)

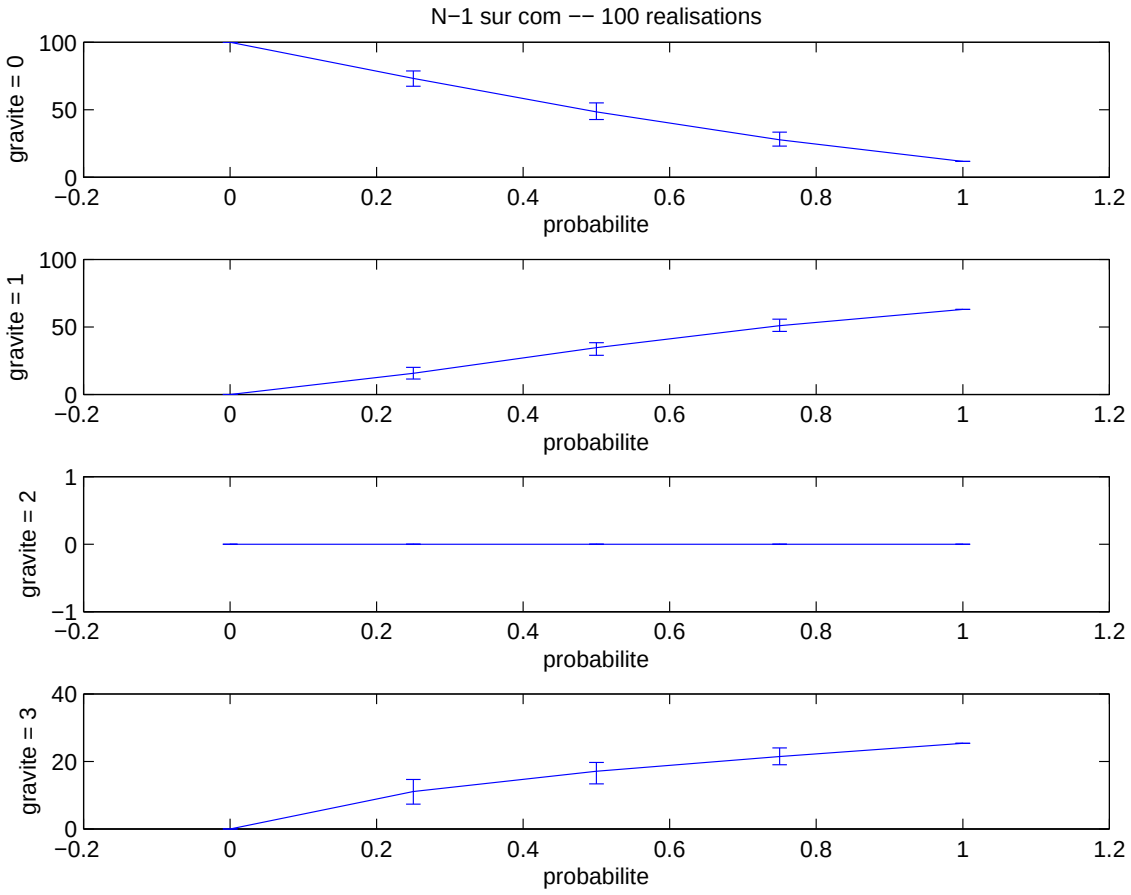

FIG. V.28 – Évolution de la gravité en fonction de la probabilité de l'interdépendance pour un $N-1$ de communication (300 nœuds)

réduisent pour s'annuler en 0.

D'une manière générale, on constate que même en réduisant la radicalité de cette hypothèse de couplage, il n'existe que très peu d'incident de gravité 2. Ainsi, le phénomène d'avalanche qui conduit à avoir soit des incidents à faible conséquences, soit des pannes généralisés ne dépend pas de la finesse des règles adoptées, mais ce phénomène est inhérent aux réseaux.

Pour conclure, cette étude de l'influence d'une des hypothèses de l'interdépendance permet de mieux comprendre son impact et d'évaluer la différence entre le cas extrême étudié et des cas plus réalistes.

V.5 Conclusion partielle

Dans ce chapitre, il a été présenté une modélisation basée sur la théorie des réseaux complexes. Cette proposition est une approche novatrice qui répond aux objectifs fixés. Ainsi c'est un modèle commun prenant néanmoins en considération la spécificité de chaque infrastructure. Les modes communs de défaillances ainsi que les effets de cascade ont été modélisés. Cette approche permet de caractériser la criticité du réseau de communication en vue de la sécurité du réseau électrique et aussi d'évaluer la vulnérabilité de chaque élément des infrastructures ou de la topologie du réseau de communication.

L'étude paramétrique sur le coefficient de tolérance a permis d'évaluer son influence sur la vulnérabilité des deux infrastructures couplées. Grâce aux différents réseaux étudiés, il a été possible de dégager des tendances généralement valables et celles spécifiques aux cas considérés. Il a été montré que lorsque un incident a des conséquences, elles sont soit faibles (moins de 10% du total de la charge) et localisées ou soit l'incident dégénère en panne généralisée à cause des effets de cascade. Il n'y a que peu de pannes intermédiaires, même lorsque l'on assouplie les règles d'interdépendances. L'étude du $N-2$ systématique a permis de mettre en évidence des moyens de bloquer un écroulement du réseau. Il a également été montré que la topologie de grille pour le réseau de communication n'offre des performances correctes que si le coefficient de tolérance est supérieur à un seuil. Les performances de topologie miroir sont généralement satisfaisantes et ont une bien moindre sensibilité à ce coefficient de tolérance. Les variations des paramètres du réseau de communication (topologie et dimensionnement) ont une plus grande influence sur les conséquences lorsque le $N-1$ est effectué sur le réseau de télécommunication plutôt que sur le réseau électrique.

Cette proposition de modélisation offre la possibilité d'affiner le modèle à volonté, ce qui permet d'évaluer chaque hypothèse. Elle possède également l'avantage d'être très générale et très générique. Elle peut ainsi être appliquée à tout réseau électrique et de communication.

Les résultats de simulation obtenus en faisant varier les paramètres d'études et en remettant en cause une hypothèse d'interdépendances sont intéressants car ils permettent de mieux comprendre le comportement des systèmes multi-infrastructures couplés face aux défaillances.

Conclusion générale et perspectives

Conclusion générale

Le travail de recherche présenté dans ce mémoire de thèse s'inscrit dans un contexte de profondes mutations de la gestion des réseaux électriques. Ces transformations sont principalement dues aux immenses progrès des technologies de l'information et de la communication. L'utilisation croissante de ces technologies, qui répond à des besoins réels, a clairement apporté de nombreux bénéfices. Mais l'utilisation de ces techniques, qui évoluent très rapidement et qui sont de plus en plus complexes, possède aussi de nombreux revers. Elles sont, en effet, de plus en plus difficiles à maîtriser totalement. L'impact de ces technologies sur le fonctionnement du réseau électrique est encore mal connu et surtout, elles sont sources de nouvelles vulnérabilités.

Afin de bien situer l'état de l'art dans le domaine de la modélisation des interdépendances entre les infrastructures critiques, une large étude bibliographique a d'abord été réalisée. Le travail a ensuite été réalisé par étapes. Tout d'abord, il a été effectué un choix des méthodes que l'on a jugées les plus adaptées par rapport aux objectifs définis. Puis, un outil multi-logiciel de simulation comportementale multi-infrastructures permettant la compréhension des phénomènes a été créé. Ensuite, une exploration d'outils d'étude des systèmes complexes mono-infrastructure a été réalisée. Suite à ces étapes, il a été proposé une modélisation unifiée des interdépendances dans les infrastructures critiques. Cette modélisation unifiée est nécessaire afin de pouvoir appréhender au mieux le comportement émergeant des systèmes couplés.

Les principales difficultés de ce travail ont pour origine l'hétérogénéité des systèmes étudiés et la nouveauté scientifique de ce sujet. En effet, le travail présenté est précurseur dans ce domaine avec l'étude couplée des réseaux électrique et de communication associé.

Dans ce travail, ont été proposées :

- une méthodologie d'évaluation des vulnérabilités des réseaux électriques vis à vis des systèmes d'information et de communication,
- une modélisation des interdépendances des systèmes couplés ainsi que des modes communs de défaillance et les effets de cascade,
- une évaluation des risques et des impacts potentiels de ces défaillances sur les pannes généralisées.

Les méthodes proposées dans le chapitre cinq sont originales et novatrices par rapport à l'état de l'art avant cette thèse. En effet, elles apportent une quantification numérique

de l'évaluation des vulnérabilités et non pas seulement une appréciation subjective. Les méthodes sont adaptées à l'étude d'infrastructures critiques susceptibles à l'effet de cascade et surtout applicables à des systèmes multi-infrastructures. Plusieurs systèmes ont été pris en compte de manière intégrée tout en restant sur une modélisation réaliste. La mise en œuvre a été effectuée sur deux logiciels différents dans un soucis de vérification. Elle a été testée sur des réseaux de grande taille (300 et 1254 nœuds). Cela a permis de montrer que les algorithmes proposés sont bien adaptés à l'étude réelle sur de grands réseaux allant jusque l'échelle continentale en un temps raisonnable et surtout inférieure à une simulation dynamique équivalente. Les méthodes proposées peuvent être utilisées en planification et sont prêtes à l'être directement.

Les résultats obtenus, suite à la modélisation des interdépendances des infrastructures critiques, permettent de progresser dans la compréhension du comportement des systèmes couplés. Cette progression dans la compréhension participe ainsi au but de sécurisation des infrastructures critiques.

Cette proposition de modélisation possède quelques limitations dues à l'ensemble des hypothèses considérées. Ainsi, on ne dispose pas d'informations temporelles. Par conséquent, il n'est possible que de calculer une puissance non fournie et non pas une énergie non distribuée.

Perspectives

Plusieurs perspectives sont possibles à ce travail de recherche. La principale voie à explorer consiste à mieux prendre en considération l'aspect temporel. Ceci afin de pouvoir calculer une énergie non distribuée et non plus seulement une puissance non fournie. Il s'agit donc d'effectuer une modélisation dynamique tout en gardant l'avantage de simulations rapides par rapport à l'intégration des équation différentielles. Une possibilité pour atteindre cet objectif est de réaliser une simulation à temps discret.

Il est également possible de continuer ce travail vers une meilleure formalisation des interdépendances afin de faire abstraction des hypothèses considérées ou de proposer d'autres règles déterministes d'interdépendances. La réflexion peut également s'étendre sur les interdépendances entre télécommunications et systèmes d'information.

À partir de la modélisation proposée, des travaux peuvent être réalisés sur la topologie des réseaux de communication avec mise en place de règles de conception ainsi que sur le dimensionnement de ces réseaux et les aspects de redondance.

L'outil de cosimulation multi-infrastructures peut-être étendu à l'utilisation de plusieurs centre de conduite, chacun gérant sa propre région électrique. On peut également lui adjoindre un préprocesseur et un dispositif de traitement des résultats en vue d'effectuer des études statistiques pour identifier des vulnérabilités.

Enfin, il serait fortement utile de pouvoir valider l'ensemble sur un réseau test correspondant à une infrastructure réelle avec des données réelles pouvant servir de cas de référence.

Bibliographie

[AB02] R. Albert and A.-L. Barabási. Statistical mechanics of complex networks. *Reviews of Modern Physics*, 74 :47–97, 2002.

[Arr08] D. Arrowsmith. Manmade, diagnosing vulnerability, emergent phenomena, and volatility in manmade networks. In *International Summer School on Risk Measurement and Control*, July 2008.

[BA99] A.L. Barabási and R. Albert. Emergence of scaling in random networks. *Science*, 286 :509 – 512, October 1999.

[BBV06] A. Barrat, M. Barthélemy, and A. Vespignani. Réseaux complexes et physique statistique. *Images de la Physique*, 2006.

[BLM+06] S. Boccaletti, V. Latora, Y. Moreno, Chavez M., and D.-U. Hwanga. Complex networks : Structure and dynamics. *Physics reports*, 424(4–5) :175–308, 2006.

[Bon02] 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.

[Bra01] U. Brandes. A faster algorithm for betweenness centrality. *Journal of Mathematical Sociology*, 25 :163–177, 2001.

[BS00] 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.

[CGT07] E. Casalicchio, E. Galli, and S. Tucci. Federated agent-based modeling and simulation approach to study interdependencies in it critical infrastructures. In *Distributed Simulation and Real-Time Applications, 2007. DS-RT 2007. 11th IEEE International Symposium*, pages 182–189, October 2007.

[CLDG07] S. Chiaradonna, P. Lollini, and F. Di Giandomenico. On a modeling framework for the analysis of interdependencies in electric power systems. In *Dependable Systems and Networks, 2007. DSN'07. 37^{th} Annual IEEE/IFIP International Conference on*, pages 185–195, June 2007.

[CLDN02] B. A. Carreras, V. E. Lynch, I. Dobson, and D. E. Newman. Critical points and transitions in an electric power transmission model for cascading failure blackouts. *CHAOS*, 12(4) :985–994, December 2002.

[CLM04a] P. Crucitti, V. Latora, and M. Marchiori. Model for cascading failures in complex networks. *Physical Review E*, 69(4) :92–97, April 2004.

[CLM04b] P. Crucitti, V. Latora, and M. Marchiori. A topological analysis of the italian electric power grid. *Physica A Statistical Mechanics and its Applications*, 338 :92–97, July 2004.

[CNG+07] B. A. Carreras, D. E. Newman, P. Gradney, V. E. Lynch, and I. Dobson. Interdependent risk in interacting infrastructure systems. In *Proc.* 40^{th} *Hawaii Int. Conference on System Sciences*, January 2007.

[CSCW07] X. Chen, K. Sun, Y. Cao, and S. Wang. Identification of vulnerable lines in power grid based on complex network theory. In *Power Engineering Society General Meeting*, pages 1–6, June 2007.

[DA89] R. David and H. Alla. *Du Grafcet aux réseaux de Petri*. Hermes, Octobre 1989.

[Dac04] R. F. Dacey. Critical infrastructure protection - challenges and efforts to secure control systems. Technical Report GAO-04-354, United States General Accounting Office (GAO), Washington, DC 20548, March 2004.

[Die00] Reinhard Diestel. *Graph Theory*. Springer-Verlag, second edition, 1997,2000.

[DM01] S. N. Dorogovtsev and J. F. F. Mendes. Evolution of networks. *Advances in Physics*, 2001.

[DM04] L. Donetti and M. A. Muñoz. Detecting network communities : a new systematic and efficient algorithm. *J. Stat. Mech*, 2004.

[DM05] L. Donetti and M. A. Muñoz. Improved spectral algorithm for the detection of network communities. *Modeling Cooperative Behavior in the Social Sciences*, 779 :104–107, July 2005.

[Eat02] John W. Eaton. *GNU Octave Manual*. Network Theory Limited, 2002.

[EWE09] EWEA. Wind energy – the facts executive summary. Technical report, WindFacts European project, March 2009.

[Fon08] M.A. Fontela. *Interaction des réseaux de transport et de distribution en présence de production décentralisée*. PhD thesis, Grenoble INP, 07 2008.

[GD03] O. Gursesli and A. A. Desrochers. Modeling infrastructure interdependencies using petri nets. In *IEEE Int. Conf. on Systems, Man and Cybernetics*, volume 2, pages 1506–1512, October 2003.

[GJ02] M. Girvan and Newman M. E. J. Community structure in social and biological networks. In *Proceedings of the National Academy of Sciences*, December 2002.

[Gri99] 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.

[Hel] M. Heller. Interdependencies in civil infrastructure systems. National Academy of Engineering Website `http://www.nae.edu/nae/bridgecom.nsf/weblinks/KGRG-573PLA?OpenDocument`.

[Hol06] A. J. Holmgren. Using graph models to analyze the vulnerability of electric power networks. *Risk analysis*, 26(4) :955–969, 2006.

[HSS05] A. Hagberg, D. Schult, and P. Swart. Networkx : Python software for the analysis of networks. Technical report, Mathematical Modeling and Analysis, Los Alamos National Laboratory, 2005. `http://networkx.lanl.gov/`.

[HWG+06] K. Hopkinson, X. Wang, R. Giovanni, J. Thorp, K. Birman, and D. Coury. Epochs : A platform for agent-based electric power and communication simulation built from commercial off-the-shelf components. *IEEE Transactions on Power Systems*, 21(2) :548–558, May 2006.

[IRR06] IRRIIS. Intermediate report on lcci topology and vulnerability assessment. Technical Report D 2.1.1, Integrated Risk Reduction of Information-based Infrastructure Systems, July 2006.

[JW08] C.W. Johnson and R. Williams. Computational support for identifying safety and security related dependencies between national critical infrastructures. In *System Safety, 2008 3rd IET International Conference on*, October 2008.

[KBB05] H. M. Kim, M. Biehl, and J. A. Buzacott. M-ci^2 : Modelling cyber interdependencies between critical infrastructures. In 3^{rd} *IEEE Int. Conf. on Industrial Informatics (INDIN'05)*, pages 644–648, August 2005.

[KCAL05] R. Kinney, P. Crucitti, R. Albert, and V. Latora. Modeling cascading failures in the north american power grid. *European Physical Journal B*, 46(1) :101–107, July 2005.

[KO03] A. Krings and P. Oman. A simple gspn for modeling common mode failures in critical infrastructures. In *Proc.* 36^{th} *Hawaii Int. Conference on System Sciences*, January 2003.

[KT06] M. Kurant and P. Thiran. Layered complex networks. *Physical Review Letters*, 96, 2006.

[KTH07] M. Kurant, P. Thiran, and P. Hagmann. Error and attack tolerance of layered complex networks. *Physical Review E*, 76(2), August 2007.

[Kun94] P. Kundur. *Power system stability and control.* McGraw-Hill Professional, 1994.

[LKK07] J.-C. Laprie, K. Kanoun, and M. Kaâniche. Modelling interdependencies between the electricity and information infrastructures. In F. Saglietti and N. Oster, editors, *Computer Safety, Reliability, and Security :* 26^{th} *International Conference, SAFECOMP 2007*, Nurmberg, September 2007. Springer.

[LM01] V. Latora and M. Marchiori. Efficient behavior of small-world networks. *Physical Review Letters*, 87(19), November 2001.

[LM04] V. Latora and M. Marchiori. The architecture of complex systems. In *Nonextensive Entropy : Interdisciplinary Applications.* Oxford University Press, 2004.

[LMMW03] E. E. Lee, D. J. Mendonça, J. E. Mitchell, and W. A. Wallace. Restoration of services in interdependent infrastructure systems : A network flows approach. Technical Report 38-03-507, Rensselaer Polytechnic Institute, Troy, NY, June 2003.

[LMN04] Y.-C. Lai, A. E. Motter, and T. Nishikawa. *Lect. Notes Phys.*, volume 650, chapter Attacks and Cascades in Complex Networks, pages 299–310. Springer, 2004.

[LMW04] E. E. Lee, J. E. Mitchell, and W. A. Wallace. Assessing vulnerability of proposed designs for interdependent infrastructure systems. In *Proc.* 37^{th} *Hawaii Int. Conference on System Sciences*, January 2004.

[LMW07] E.E. Lee, J.E. Mitchell, and W.A. Wallace. Restoration of services in interdependent infrastructure systems : A network flows approach. *Systems, Man, and Cybernetics, Part C : Applications and Reviews, IEEE Transactions on*, 37(6) :1303–1317, November 2007.

[Mas02] M. Masera. An approach to the understanding of interdependencies. In *Power Systems and Communications Infrastructures for the future*, Beijing, September 2002.

[Mea97] R. T. Marsh et al. Critical foundations, protecting america's infrastructures. Technical report, President's Commission on Critical Infrastructure Protection, October 1997.

[MHVJ06] J. R. Martí, J. A. Hollman, C. Ventura, and J. Jatskevich. Design for survival real-time infrastructures coordination. In *CNIP, Rome*, March 2006.

[Mil05a] F. Milano. *Documentation for PSAT version 1.3.4*, July 2005.

[Mil05b] F. Milano. An open source power system analysis toolbox. *Power Systems, IEEE Transactions on*, 20(3) :1199–1206, August 2005.

[Mil08] F. Milano. *Quick Reference Manual for PSAT version 2.1.2*, June 2008.

[ML02] A. E. Motter and Y.-C. Lai. Cascade-based attacks on complex networks. *Phys. Rev. E*, 66(6), December 2002.

[MN05] C. Macal and M. North. Tutorial on agent-based modeling and simulation. In *Proc. of the 2005 Winter Simulation Conf.*, December 2005.

[MS99] Charles M. Macal and David Sallach, editors. *Workshop on Agent Simulation : Applications, Models, and Tools*, The University of Chicago, October 1999.

[New01] M. E. J. Newman. Scientific collaboration networks : Ii. shortest paths, weighted networks, and centrality. *Physical Review E*, 64(1), July 2001.

[New03] M. E. J. Newman. The structure and function of complex networks. *SIAM Review*, 45(2) :167–256, 2003.

[NG04] M. E. J. Newman and M. Girvan. Finding and evaluating community structure in networks. *Physical Review E*, 69(2), February 2004.

[NNC+05] D. E. Newman, B. Nkei, B. A. Carreras, I. Dobson, V. E. Lynch, and P. Gradney. Risk assessment in complex interacting infrastructure systems. In *Proc.* 39^{th} *Hawaii Int. Conference on System Sciences*, January 2005.

[ORK07] G.P. O'Reilly, S.H. Richman, and A. Kelic. Power, telecommunications, and emergency services in a converged network world. In *Design and Reliable Communication Networks, 2007. DRCN 2007. 6th International Workshop on*, October 2007.

[OUCB05] G. O'Reilly, H. Uzunalioglu, S. Conrad, and W. Beyeler. Inter-infrastructure simulations across telecom, power, and emergency services. In *Design of Reliable Communication Networks, 2005. (DRCN 2005). Proceedings.5th International Workshop on*, October 2005.

[PDHP06] P. Pederson, D. Dudenhoeffer, S. Hartley, and M. Permann. Critical infrastructure interdependency modeling : A survey of u.s. and international research. Technical report, Idaho National Laboratory, August 2006.

[peelcdle06] Le parlement européen et le conseil de l'union européenne. Directive 2005/89/ce. *Journal officiel de l'Union européenne*, L33, 02 2006.

[Per07] M.R. Permann. Toward developing genetic algorithms to aid in critical infrastructure modeling. In *Technologies for Homeland Security, 2007 IEEE Conference on*, pages 192–197, May 2007.

[Pha06] T.T.H. Pham. *Influences de la production décentralisée sur la gestion des infrastructures critiques des réseaux de puissance*. PhD thesis, Grenoble INP, 10 2006.

[PLT87] J.P. Paul, J.Y. Leost, and J.M. Tesseron. Survey of the secondary voltage control in france : Present realization and investigations. *Power Systems, IEEE Transactions on*, 2(2) :505–511, May 1987.

[PS08] S. Panzieri and R. Setola. Failures propagation in critical interdependent infrastructures. *International Journal of Modelling, Identification and Control*, 3(1), 2008.

[PSU04] S. Panzieri, R. Setola, and G. Ulivi. An agent based simulator for critical interdependent infrastructures. In *Proc. 2^{nd} Conf. on Securing Critical Infrastructures*, October 2004.

[PSU05] S. Panzieri, R. Setola, and G. Ulivi. An approach to model complex interdependent infrastructures. In 16^{th} *IFAC World Congress 2005*, 2005.

[RBT07] V. Rosato, S. Bologna, and F. Tiriticco. Topological properties of high-voltage electrical transmission networks. *Electric Power Systems Research*, 77(2) :99–105, 2007.

[RCH+09] B. Rozel, R. Caire, N. Hadjsaid, J.-P. Rognon, and C. Tranchita. Complex network theory and graph partitioning : Application to large interconnected networks. In *PowerTech, 2009 IEEE Bucharest*, July 2009.

[RD06] T. Rigole and G. Deconinck. A survey on modeling and simulation of interdependent critical infrastructures. In 3^{rd} *IEEE Benelux Young Researchers Symposium in Electrical Power Engineering*, Gent, Belgium, April 2006.

[Rin04] S. M. Rinaldi. Modeling and simulating critical infrastructures and their interdependencies. In *Proc. 37^{th} Hawaii Int. Conference on System Sciences*, January 2004.

[RPK01] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly. Identifying, understanding, and analysing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6) :11–25, December 2001.

[RTEa] RTE. *Référentiel technique de RTE*. `http://www.rte-france.com`.

[RTEb] RTE et Tractebel. *Eurostag : logiciel de simulation dynamique des réseaux électriques*. `http://www.eurostag.be`.

[RTE04] RTE. *Mémento de la sûreté du système électrique*, 2004. `http://www.rte-france.com`.

[RTE09] RTE. Le bilan électrique français 2008, janvier 2009.

[RVC+08] B. Rozel, M. Viziteu, R. Caire, N. Hadjsaid, and J.-P. Rognon. Towards a common model for studying critical infrastructure interdependencies. In *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, July 2008.

[RVD06] T. Rigole, K. Vanthournout, and G. Deconinck. Interdependencies between an electric power infrastructure with distributed control, and the underlying ict infrastructure. In *Int. Workshop on Complex Network and Infrastructure Protection*, pages 428–440, Rome, Italy, March 2006.

[SDK+95] M. Shaw, R. DeLine, D.V. Klein, T.L. Ross, D.M. Young, and G. Zelesnik. Abstractions for software architecture and tools to support them. *Software Engineering, IEEE Transactions on*, 21(4) :314–335, April 1995.

[SH05] K. Sun and Z.-X. Han. Analysis and comparison on several kinds of models of cascading failure in power system. In *Transmission and Distribution Conference and Exhibition : Asia and Pacific*, pages 1–7, 2005.

[Sie] Siemens. *PSS/NETOMAC (Power System Simulator NETOMAC)*. `http://www.netomac.com`.

[SLP06] K. Schneider, C.-C. Liu, and J.-P. Paul. Assesment of interactions between power and telecommunications infrastructures. *IEEE Transactions on Power Systems*, 21(3) :1123–1130, August 2006.

[SM03] B. Saha and B. Moody. The economic cost of the blackout. Technical report, ICF Consulting, 2003.

[Sun05] K. Sun. Complex networks theory : A new method of research in power grid. In *Transmission and Distribution Conference and Exhibition : Asia and Pacific*, pages 1–6, 2005.

[Tan99] A. Tanenbaum. *Reseaux*. Dunod/Prentice Hall, troisième edition, 1999.

[TWR+04] W. J. Tolone, D. Wilson, A. Raja, W. Xiang, H. Hao, S. Phelps, and E. W. Johnson. *Critical Infrastructure Integration Modeling and Simulation*, pages 214–225. H. Chen et al., 2004.

[UCT07] UCTE. Final report on the disturbances of 4 november 2006, janvier 2007.

[Viz07] M. Viziteu. Sécurisation des infrastructures critiques : modélisation des interdépendances. Master's thesis, INP Grenoble, juillet 2007.

[Wee87] B.M. Weedy. *Electric Power Systems*. John Wiley & Sons, third edition, 1987.

[Wol05] S. D. Wolthusen. Gis-based command and control infrastructure for critical infrastructure protection. In *Proc. 1^{st} Int. Workshop on Critical Infrastructure Protection (IWCIP'05)*, November 2005.

[ZB05] Q. Zhou and J.W. Bialek. Approximate model of european interconnected system as a benchmark system to study effects of cross-border trades. *Power Systems, IEEE Transactions on*, 20(2) :782–788, May 2005.

[Zim04] R. Zimmerman. Decison-making and the vulnerability of interdependent critical infrastructure. In *IEEE Int. Conf. on Systems, Man and Cybernetics*, volume 5, pages 4059–4063, October 2004.

[ZPF03] P. Zhang, S. Peeta, and T. Friesz. Dynamic game theoretic of multi-layer infrastructure networks. In 10^{th} *Int. Conf. on Travel Behaviour Research*, Lucerne, August 2003.

Annexe A

Données du réseau IEEE 300 nœuds

```
TAPE
 13/05/91 CYME INTERNATIONAL    100.0 1991 S IEEE 300-BUS TEST SYSTEM
BUS DATA FOLLOWS                                300 ITEMS
   1  1           1  1  0 1.0284   5.95    90.00    49.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0    1
   2  1           1  1  0 1.0354   7.74    56.00    15.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0    2
   3  1           1  1  0 0.9971   6.64    20.00     0.00     0.00    0.00 230.00 0.0000    0.00    0.00 0.0000 0.0000    0    3
   4  1           1  1  0 1.0308   4.71     0.00     0.00     0.00    0.00 345.00 0.0000    0.00    0.00 0.0000 0.0000    0    4
   5  1           1  1  0 1.0191   4.68   353.00   130.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0    5
   6  1           1  1  0 1.0312   6.99   120.00    41.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0    6
   7  1           1  1  0 0.9934   6.19     0.00     0.00     0.00    0.00 230.00 0.0000    0.00    0.00 0.0000 0.0000    0    7
   8  1           1  1  2 1.0153   2.40    58.00    14.00    -5.00    0.00 115.00 1.0153   10.00  -10.00 0.0000 0.0000    8    8
   9  1           1  1  0 1.0034   2.85    96.00    43.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0    9
  10  1           1  1  2 1.0205   1.35   148.00    33.00    -5.00    0.00 230.00 1.0205   20.00  -20.00 0.0000 0.0000   10   10
  11  1           1  1  0 1.0057   2.46    83.00    21.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   11
  12  1           1  1  0 0.9974   5.21     0.00     0.00     0.00    0.00 230.00 0.0000    0.00    0.00 0.0000 0.0000    0   12
  13  1           1  1  0 0.9977  -0.55    58.00    10.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   13
  14  1           1  1  0 0.9991  -4.81   160.00    60.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   14
  15  1           1  1  0 1.0343  -8.59   126.70    23.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   15
  16  1           1  1  0 1.0315  -2.65     0.00     0.00     0.00    0.00 345.00 0.0000    0.00    0.00 0.0000 0.0000    0   16
  17  1           1  1  0 1.0649 -13.10   561.00   220.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   17
  19  1           1  1  0 0.9820   1.08     0.00     0.00     0.00    0.00 230.00 0.0000    0.00    0.00 0.0000 0.0000    0   18
  20  1           1  1  2 1.0010  -2.46   595.00   120.00   -10.00    0.00 115.00 1.0010   20.00  -20.00 0.0000 0.0000   20   19
  21  1           1  1  0 0.9752   1.62    77.00     1.00     0.00    0.00 230.00 0.0000    0.00    0.00 0.0000 0.0000    0   20
  22  1           1  1  0 0.9963  -1.97    81.00    23.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   21
  23  1           1  1  0 1.0501   3.94    21.00     7.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   22
  24  1           1  1  0 1.0057   6.02     0.00     0.00     0.00    0.00 230.00 0.0000    0.00    0.00 0.0000 0.0000    0   23
  25  1           1  1  0 1.0234   1.44    45.00    12.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   24
  26  1           1  1  0 0.9986  -1.73    28.00     9.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   25
  27  1           1  1  0 0.9750  -4.90    69.00    13.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   26
  33  1           1  1  0 1.0244 -12.02    55.00     6.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   27
  34  1           1  1  0 1.0414  -7.94     0.00     0.00     0.00    0.00 345.00 0.0000    0.00    0.00 0.0000 0.0000    0   28
  35  1           1  1  0 0.9757 -25.72     0.00     0.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   29
  36  1           1  1  0 1.0011 -22.59     0.00     0.00     0.00    0.00 230.00 0.0000    0.00    0.00 0.0000 0.0000    0   30
  37  1           1  1  0 1.0201 -11.23    85.00    32.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   31
  38  1           1  1  0 1.0202 -12.56   155.00    18.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   32
  39  1           1  1  0 1.0535  -5.81     0.00     0.00     0.00    0.00 345.00 0.0000    0.00    0.00 0.0000 0.0000    0   33
  40  1           1  1  0 1.0216 -12.78    46.00   -21.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   34
  41  1           1  1  0 1.0292 -10.45    86.00     0.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   35
  42  1           1  1  0 1.0448  -7.44     0.00     0.00     0.00    0.00 345.00 0.0000    0.00    0.00 0.0000 0.0000    0   36
  43  1           1  1  0 1.0006 -16.79    39.00     9.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   37
  44  1           1  1  0 1.0086 -17.47   195.00    29.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   38
  45  1           1  1  0 1.0215 -14.74     0.00     0.00     0.00    0.00 230.00 0.0000    0.00    0.00 0.0000 0.0000    0   39
  46  1           1  1  0 1.0344 -11.75     0.00     0.00     0.00    0.00 345.00 0.0000    0.00    0.00 0.0000 0.0000    0   40
  47  1           1  1  0 0.9777 -23.17    58.00    11.80     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   41
  48  1           1  1  0 1.0019 -16.09    41.00    19.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   42
  49  1           1  1  0 1.0475  -2.95    92.00    26.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   43
  51  1           1  1  0 1.0253  -8.15    -5.00     5.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   44
  52  1           1  1  0 0.9979 -11.86    61.00    28.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   45
  53  1           1  1  0 0.9959 -17.60    69.00     3.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   46
  54  1           1  1  0 1.0050 -16.25    10.00     1.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   47
  55  1           1  1  0 1.0150 -12.21    22.00    10.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   48
  57  1           1  1  0 1.0335  -8.00    98.00    20.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   49
  58  1           1  1  0 0.9918  -5.99    14.00     1.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   50
  59  1           1  1  0 0.9789  -5.29   218.00   106.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   51
  60  1           1  1  0 1.0246  -9.56     0.00     0.00     0.00    0.00 230.00 0.0000    0.00    0.00 0.0000 0.0000    0   52
  61  1           1  1  0 0.9906  -3.47   227.00   110.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   53
  62  1           1  1  0 1.0160  -1.10     0.00     0.00     0.00    0.00 230.00 0.0000    0.00    0.00 0.0000 0.0000    0   54
  63  1           1  1  2 0.9583 -17.62    70.00    30.00     0.00    0.00 115.00 0.9583   25.00  -25.00 0.0000 0.0000   63   55
  64  1           1  1  0 0.9480 -12.97     0.00     0.00     0.00    0.00 230.00 0.0000    0.00    0.00 0.0000 0.0000    0   56
  69  1           1  1  0 0.9630 -25.66     0.00     0.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   57
  70  1           1  1  0 0.9513 -35.16    56.00    20.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   58
  71  1           1  1  0 0.9793 -29.88   116.00    38.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   59
  72  1           1  1  0 0.9696 -27.48    57.00    19.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   60
  73  1           1  1  0 0.9775 -25.77   224.00    71.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   61
  74  1           1  1  0 0.9964 -22.00     0.00     0.00     0.00    0.00 230.00 0.0000    0.00    0.00 0.0000 0.0000    0   62
  76  1           1  1  2 0.9632 -26.54   208.00   107.00     0.00    0.00 115.00 0.9632   35.00   12.00 0.0000 0.0000   76   63
  77  1           1  1  0 0.9837 -24.94    74.00    28.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   64
  78  1           1  1  0 0.9900 -24.05     0.00     0.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   65
  79  1           1  1  0 0.9820 -24.97    48.00    14.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   66
  80  1           1  1  0 0.9872 -24.97    28.00     7.00     0.00    0.00 115.00 0.0000    0.00    0.00 0.0000 0.0000    0   67
  81  1           1  1  0 1.0340 -18.89     0.00     0.00     0.00    0.00 345.00 0.0000    0.00    0.00 0.0000 0.0000    0   68
  84  1           1  1  2 1.0250 -17.16    37.00    13.00   375.00    0.00 115.00 1.0250  240.00 -240.00 0.0000 0.0000   84   69
  85  1           1  1  0 0.9872 -17.68     0.00     0.00     0.00    0.00 230.00 0.0000    0.00    0.00 0.0000 0.0000    0   70
```

86	1		1	1	0	0.9909	-14.19	0.00	0.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	71
87	1		1	1	0	0.9921	-7.77	0.00	0.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	72
88	1		1	1	0	1.0151	-20.96	0.00	0.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	73
89	1		1	1	0	1.0317	-11.13	44.20	0.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	74
90	1		1	1	0	1.0272	-11.23	66.00	0.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	75
91	1		1	1	2	1.0520	-9.40	17.40	0.00	155.00	0.00	115.00	1.0520	96.00	-11.00	0.0000	0.0000	91	76
92	1		1	1	2	1.0520	-6.20	15.80	0.00	290.00	0.00	115.00	1.0520	153.00	-153.00	0.0000	0.0000	92	77
94	1		1	1	0	0.9930	-9.42	60.30	0.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	78
97	1		1	1	0	1.0183	-13.24	39.90	0.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	79
98	1		1	1	2	1.0000	-14.60	66.70	0.00	68.00	0.00	115.00	1.0000	56.00	-30.00	0.0000	0.0000	98	80
99	1		1	1	0	0.9894	-20.27	83.50	0.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	81
100	1		1	1	0	1.0060	-14.45	0.00	0.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	82
102	1		1	1	0	1.0008	-15.23	77.80	0.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	83
103	1		1	1	0	1.0288	-12.06	32.00	0.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	84
104	1		1	1	0	0.9958	-17.33	8.60	0.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	85
105	1		1	1	0	1.0223	-12.94	49.60	0.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	86
107	1		1	1	0	1.0095	-16.03	4.60	0.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	87
108	1		1	1	2	0.9900	-20.26	112.10	0.00	117.00	0.00	115.00	0.9900	77.00	-24.00	0.0000	0.0000	108	88
109	1		1	1	0	0.9749	-26.06	30.70	0.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	89
110	1		1	1	0	0.9730	-24.72	63.00	0.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	90
112	1		1	1	0	0.9725	-28.69	19.60	0.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	91
113	1		1	1	0	0.9700	-25.38	26.20	0.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	92
114	1		1	1	0	0.9747	-28.59	18.20	0.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	93
115	2		1	2	0	0.9603	-13.57	0.00	0.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	94
116	2		1	2	0	1.0249	-12.69	0.00	0.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	95
117	2		1	2	0	0.9348	-4.72	0.00	0.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	3.2500	0	96
118	2		1	2	0	0.9298	-4.12	14.10	650.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	97
119	2		1	2	2	1.0435	5.17	0.00	0.00	1930.00	0.00	115.00	1.0435	1500.00	-500.00	0.0000	0.0000	119	98
120	2		1	2	0	0.9584	-8.77	777.00	215.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.5500	0	99
121	2		1	2	0	0.9871	-12.64	535.00	55.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	100
122	2		1	2	0	0.9728	-14.36	229.10	11.80	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	101
123	2		1	2	0	1.0006	-17.64	78.00	1.40	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	102
124	2		1	2	2	1.0233	-13.49	276.40	59.30	240.00	0.00	115.00	1.0233	120.00	-60.00	0.0000	0.0000	124	103
125	2		1	2	2	1.0103	-18.43	514.80	82.70	0.00	0.00	115.00	1.0103	200.00	-25.00	0.0000	0.0000	125	104
126	2		1	2	0	0.9978	-12.86	57.90	5.10	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	105
127	2		1	2	0	1.0001	-10.52	380.80	37.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	106
128	2		1	2	0	1.0024	-4.78	0.00	0.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	107
129	2		1	2	0	1.0028	-4.40	0.00	0.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	108
130	2		1	2	0	1.0191	5.56	0.00	0.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	109
131	2		1	2	0	0.9861	6.06	0.00	0.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	110
132	2		1	2	0	1.0045	3.04	0.00	0.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	111
133	2		1	2	0	1.0020	-5.46	0.00	0.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	112
134	2		1	2	0	1.0220	-8.04	0.00	0.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	113
135	2		1	2	0	1.0193	-6.76	169.20	41.60	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	114
136	2		1	2	0	1.0476	1.54	55.20	18.20	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	115
137	2		1	2	0	1.0471	-1.45	273.60	99.80	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	116
138	2		1	2	2	1.0550	-6.35	826.70	135.20	-192.50	0.00	230.00	1.0550	350.00	-125.00	0.0000	0.0000	138	117
139	2		1	2	0	1.0117	-3.57	595.00	83.30	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	118
140	2		1	2	0	1.0430	-3.44	387.70	114.70	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	119
141	2		1	2	2	1.0510	0.05	145.00	58.00	281.00	0.00	230.00	1.0510	75.00	-50.00	0.0000	0.0000	141	120
142	2		1	2	0	1.0155	-2.77	56.50	24.50	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	121
143	2		1	2	2	1.0435	4.03	89.50	35.50	696.00	0.00	230.00	1.0435	300.00	-100.00	0.0000	0.0000	143	122
144	2		1	2	0	1.0160	-0.70	0.00	0.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	123
145	2		1	2	0	1.0081	-0.16	24.00	14.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	124
146	2		1	2	2	1.0528	4.32	0.00	0.00	84.00	0.00	230.00	1.0528	35.00	-15.00	0.0000	0.0000	146	125
147	2		1	2	2	1.0528	8.36	0.00	0.00	217.00	0.00	230.00	1.0528	100.00	-50.00	0.0000	0.0000	147	126
148	2		1	2	0	1.0577	0.28	63.00	25.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	127
149	2		1	2	2	1.0735	5.23	0.00	0.00	103.00	0.00	230.00	1.0735	50.00	-25.00	0.0000	0.0000	149	128
150	2		1	2	0	0.9869	6.34	0.00	0.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	129
151	2		1	2	0	1.0048	4.13	0.00	0.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	130
152	2		1	2	2	1.0535	9.24	17.00	9.00	372.00	0.00	230.00	1.0535	175.00	-50.00	0.0000	0.0000	152	131
153	2		1	2	2	1.0435	10.46	0.00	0.00	216.00	0.00	230.00	1.0435	90.00	-50.00	0.0000	0.0000	153	132
154	2		1	2	0	0.9663	-1.80	70.00	5.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.3450	0	133
155	2		1	2	0	1.0177	6.75	200.00	50.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	134
156	2		1	2	2	0.9630	5.15	75.00	50.00	0.00	0.00	115.00	0.9630	15.00	-10.00	0.0000	0.0000	156	135
157	2		1	2	0	0.9845	-11.93	123.50	-24.30	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	136
158	2		1	2	0	0.9987	-11.40	0.00	0.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	137
159	2		1	2	0	0.9867	-9.82	33.00	16.50	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	138
160	2		1	2	0	0.9998	-12.55	0.00	0.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	139
161	2		1	2	0	1.0360	8.85	35.00	15.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	140
162	2		1	2	0	0.9918	18.50	85.00	24.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	141
163	2		1	2	0	1.0410	2.91	0.00	0.40	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	142
164	2		1	2	0	0.9839	9.66	0.00	0.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	-2.1200	0	143
165	2		1	2	0	1.0002	26.31	0.00	0.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	144
166	2		1	2	0	0.9973	30.22	0.00	0.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	-1.0300	0	145
167	2		1	2	0	0.9715	-6.91	299.90	95.70	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	146
168	2		1	2	0	1.0024	-4.80	0.00	0.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	147
169	2		1	2	0	0.9879	-6.68	0.00	0.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	148
170	2		1	2	2	0.9290	0.09	481.80	205.00	205.00	0.00	115.00	0.9290	90.00	-40.00	0.0000	0.0000	170	149
171	2		1	2	2	0.9829	-9.94	763.60	291.10	0.00	0.00	115.00	0.9829	150.00	-50.00	0.0000	0.0000	171	150
172	2		1	2	0	1.0244	-6.22	26.50	0.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	151
173	2		1	2	0	0.9837	-12.75	163.50	43.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.5300	0	152
174	2		1	2	0	1.0622	-2.69	0.00	0.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	153
175	2		1	2	0	0.9730	-7.21	176.00	83.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	154
176	2		1	2	2	1.0522	4.67	5.00	4.00	228.00	0.00	115.00	1.0522	90.00	-45.00	0.0000	0.0000	176	155
177	2		1	2	2	1.0077	0.62	28.00	12.00	84.00	0.00	115.00	1.0077	35.00	-15.00	0.0000	0.0000	177	156

178	2	1	2	0	0.9397	-6.56	427.40	173.60	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	157
179	2	1	2	0	0.9699	-9.37	74.00	29.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.4500	0	158
180	2	1	2	0	0.9793	-3.09	69.50	49.30	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	159
181	2	1	2	0	1.0518	-1.33	73.40	0.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	160
182	2	1	2	0	1.0447	-4.19	240.70	89.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	161
183	2	1	2	0	0.9717	7.12	40.00	4.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	162
184	2	1	2	0	1.0386	-6.85	136.80	16.60	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	163
185	2	1	2	2	1.0522	-4.33	0.00	0.00	200.00	0.00	230.00	1.0522	80.00	-50.00	0.0000	0.0000	185	164
186	2	1	2	2	1.0650	2.17	59.80	24.30	1200.00	0.00	230.00	1.0650	400.00	-100.00	0.0000	0.0000	186	165
187	2	1	2	2	1.0650	1.40	59.80	24.30	1200.00	0.00	230.00	1.0650	400.00	-100.00	0.0000	0.0000	187	166
188	2	1	2	0	1.0533	-0.72	182.60	43.60	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	167
189	3	1	3	0	0.9975	-25.84	7.00	2.00	0.00	0.00	66.00	0.0000	0.00	0.00	0.0000	0.0000	0	168
190	3	1	3	2	1.0551	-20.62	0.00	0.00	475.00	0.00	345.00	1.0551	300.00	-300.00	0.0000	-1.5000	190	169
191	3	1	3	2	1.0435	12.25	489.00	53.00	1973.00	0.00	230.00	1.0435	1000.00	-1000.00	0.0000	0.0000	191	170
192	3	1	3	0	0.9374	-11.18	800.00	72.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	171
193	3	1	3	0	0.9897	-26.09	0.00	0.00	0.00	0.00	66.00	0.0000	0.00	0.00	0.0000	0.0000	0	172
194	3	1	3	0	1.0489	-19.21	0.00	0.00	0.00	0.00	345.00	0.0000	0.00	0.00	0.0000	0.0000	0	173
195	3	1	3	0	1.0357	-20.79	0.00	0.00	0.00	0.00	345.00	0.0000	0.00	0.00	0.0000	0.0000	0	174
196	3	1	3	0	0.9695	-25.32	10.00	3.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	175
197	3	1	3	0	0.9907	-23.72	43.00	14.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	176
198	3	1	3	2	1.0150	-20.58	64.00	21.00	424.00	0.00	115.00	1.0150	260.00	-260.00	0.0000	0.0000	198	177
199	3	1	3	0	0.9528	-26.05	35.00	12.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	178
200	3	1	3	0	0.9550	-25.93	27.00	12.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	179
201	1	1	1	0	0.9692	-27.49	41.00	14.00	0.00	0.00	66.00	0.0000	0.00	0.00	0.0000	0.0000	0	180
202	3	1	3	0	0.9908	-25.33	38.00	13.00	0.00	0.00	66.00	0.0000	0.00	0.00	0.0000	0.0000	0	181
203	3	1	3	0	1.0033	-22.35	42.00	14.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	182
204	3	1	3	0	0.9718	-25.70	72.00	24.00	0.00	0.00	66.00	0.0000	0.00	0.00	0.0000	0.0000	0	183
205	3	1	3	0	0.9838	-26.07	0.00	-5.00	0.00	0.00	66.00	0.0000	0.00	0.00	0.0000	0.0000	0	184
206	3	1	3	0	0.9992	-27.41	12.00	2.00	0.00	0.00	66.00	0.0000	0.00	0.00	0.0000	0.0000	0	185
207	1	1	1	0	1.0137	-27.44	-21.00	-14.20	0.00	0.00	66.00	0.0000	0.00	0.00	0.0000	0.0000	0	186
208	3	1	3	0	0.9929	-26.28	7.00	2.00	0.00	0.00	66.00	0.0000	0.00	0.00	0.0000	0.0000	0	187
209	3	1	3	0	0.9999	-25.66	38.00	13.00	0.00	0.00	66.00	0.0000	0.00	0.00	0.0000	0.0000	0	188
210	3	1	3	0	0.9788	-24.22	0.00	0.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	189
211	3	1	3	0	1.0017	-23.31	96.00	7.00	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	190
212	3	1	3	0	1.0132	-22.51	0.00	0.00	0.00	0.00	138.00	0.0000	0.00	0.00	0.0000	0.0000	0	191
213	3	1	3	2	1.0100	-11.67	0.00	0.00	272.00	0.00	16.50	1.0100	150.00	-150.00	0.0000	0.0000	213	192
214	3	1	3	0	0.9919	-17.53	22.00	16.00	0.00	0.00	138.00	0.0000	0.00	0.00	0.0000	0.0000	0	193
215	3	1	3	0	0.9866	-20.23	47.00	26.00	0.00	0.00	138.00	0.0000	0.00	0.00	0.0000	0.0000	0	194
216	3	1	3	0	0.9751	-22.53	176.00	105.00	0.00	0.00	138.00	0.0000	0.00	0.00	0.0000	0.0000	0	195
217	3	1	3	0	1.0215	-22.20	100.00	75.00	0.00	0.00	138.00	0.0000	0.00	0.00	0.0000	0.0000	0	196
218	3	1	3	0	1.0075	-22.63	131.00	96.00	0.00	0.00	138.00	0.0000	0.00	0.00	0.0000	0.0000	0	197
219	3	1	3	0	1.0554	-21.15	0.00	0.00	0.00	0.00	345.00	0.0000	0.00	0.00	0.0000	0.0000	0	198
220	3	1	3	2	1.0080	-21.73	285.00	100.00	100.00	0.00	138.00	1.0080	60.00	-60.00	0.0000	0.0000	220	199
221	3	1	3	2	1.0000	-22.49	171.00	70.00	450.00	0.00	138.00	1.0000	320.00	-320.00	0.0000	0.0000	221	200
222	3	1	3	2	1.0500	-23.17	328.00	188.00	250.00	0.00	20.00	1.0500	300.00	-300.00	0.0000	0.0000	222	201
223	3	1	3	0	0.9965	-22.70	428.00	232.00	0.00	0.00	138.00	0.0000	0.00	0.00	0.0000	0.0000	0	202
224	3	1	3	0	1.0002	-21.55	173.00	99.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	203
225	3	1	3	0	0.9453	-11.34	410.00	40.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	204
226	3	1	3	0	1.0180	-21.61	0.00	0.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	205
227	3	1	3	2	1.0000	-27.22	538.00	369.00	303.00	0.00	27.00	1.0000	300.00	-300.00	0.0000	0.0000	227	206
228	3	1	3	0	1.0423	-20.94	223.00	148.00	0.00	0.00	138.00	0.0000	0.00	0.00	0.0000	0.0000	0	207
229	3	1	3	0	1.0496	-19.94	96.00	46.00	0.00	0.00	138.00	0.0000	0.00	0.00	0.0000	0.0000	0	208
230	3	1	3	2	1.0400	-13.82	0.00	0.00	345.00	0.00	20.00	1.0400	250.00	-250.00	0.0000	0.0000	230	209
231	3	1	3	0	1.0535	-21.22	159.00	107.00	0.00	0.00	345.00	0.0000	0.00	0.00	0.0000	-3.0000	0	210
232	3	1	3	0	1.0414	-23.19	448.00	143.00	0.00	0.00	138.00	0.0000	0.00	0.00	0.0000	0.0000	0	211
233	3	1	3	2	1.0000	-25.90	404.00	212.00	300.00	0.00	66.00	1.0000	500.00	-500.00	0.0000	0.0000	233	212
234	3	1	3	0	1.0387	-20.89	572.00	244.00	0.00	0.00	138.00	0.0000	0.00	0.00	0.0000	0.0000	0	213
235	3	1	3	0	1.0095	-21.03	269.00	157.00	0.00	0.00	138.00	0.0000	0.00	0.00	0.0000	0.0000	0	214
236	3	1	3	2	1.0165	-15.40	0.00	0.00	600.00	0.00	20.00	1.0165	300.00	-300.00	0.0000	0.0000	236	215
237	3	1	3	0	1.0558	-21.10	0.00	0.00	0.00	0.00	345.00	0.0000	0.00	0.00	0.0000	0.0000	0	216
238	3	1	3	2	1.0100	-20.94	255.00	149.00	250.00	0.00	138.00	1.0100	200.00	-200.00	0.0000	-1.5000	238	217
239	3	1	3	2	1.0000	-15.86	0.00	0.00	550.00	0.00	138.00	1.0000	400.00	-400.00	0.0000	0.0000	239	218
240	3	1	3	0	1.0237	-20.14	0.00	0.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	-1.4000	0	219
241	3	1	3	2	1.0500	-16.50	0.00	0.00	575.43	0.00	20.00	1.0500	600.00	-600.00	0.0000	0.0000	241	220
242	3	1	3	2	0.9930	-17.53	0.00	0.00	170.00	0.00	138.00	0.9930	100.00	40.00	0.0000	0.0000	242	221
243	3	1	3	2	1.0100	-19.27	8.00	3.00	84.00	0.00	66.00	1.0100	80.00	40.00	0.0000	0.0000	243	222
244	3	1	3	0	0.9921	-20.21	0.00	0.00	0.00	0.00	66.00	0.0000	0.00	0.00	0.0000	0.0000	0	223
245	3	1	3	0	0.9711	-20.90	61.00	30.00	0.00	0.00	66.00	0.0000	0.00	0.00	0.0000	0.0000	0	224
246	3	1	3	0	0.9651	-21.74	77.00	33.00	0.00	0.00	66.00	0.0000	0.00	0.00	0.0000	0.0000	0	225
247	3	1	3	0	0.9688	-21.67	61.00	30.00	0.00	0.00	66.00	0.0000	0.00	0.00	0.0000	0.0000	0	226
248	3	1	3	0	0.9760	-25.23	29.00	14.00	0.00	0.00	66.00	0.0000	0.00	0.00	0.0000	0.4560	0	227
249	3	1	3	0	0.9752	-25.65	29.00	14.00	0.00	0.00	66.00	0.0000	0.00	0.00	0.0000	0.0000	0	228
250	3	1	3	0	1.0196	-23.80	-23.00	-17.00	0.00	0.00	66.00	0.0000	0.00	0.00	0.0000	0.0000	0	229
281	3	1	3	0	1.0251	-20.06	-33.10	-29.40	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	230
319	1	1	1	0	1.0152	1.48	115.80	-24.00	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	231
320	1	1	1	0	1.0146	-2.23	2.40	-12.60	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	232
322	1	1	1	0	1.0005	-17.61	2.40	-3.90	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	233
323	1	1	1	0	0.9810	-13.69	-14.90	26.50	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	234
324	1	1	1	0	0.9750	-23.42	24.70	-1.20	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	235
526	1	1	1	0	0.9429	-34.31	145.30	-34.90	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	236
528	1	1	1	0	0.9723	-37.58	28.10	-20.50	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	237
531	1	1	1	0	0.9604	-29.10	14.00	2.50	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	238
552	1	1	1	0	1.0009	-23.36	-11.10	-1.40	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	239
562	1	1	1	0	0.9777	-28.00	50.50	17.40	0.00	0.00	230.00	0.0000	0.00	0.00	0.0000	0.0000	0	240
609	1	1	1	0	0.9583	-28.79	29.60	0.60	0.00	0.00	115.00	0.0000	0.00	0.00	0.0000	0.0000	0	241
664	3	1	3	0	1.0309	-17.00	-113.70	76.70	0.00	0.00	345.00	0.0000	0.00	0.00	0.0000	0.0000	0	242

```
1190  2              1  2  0 1.0128   3.90   100.31    29.17      0.00     0.00    86.00 0.0000      0.00     0.00 0.0000 0.0000      0  243
1200  2              1  2  0 1.0244  -7.52  -100.00    34.17      0.00     0.00    86.00 0.0000      0.00     0.00 0.0000 0.0000      0  244
1201  2              1  2  0 1.0122 -15.18     0.00     0.00      0.00     0.00   115.00 0.0000      0.00     0.00 0.0000 0.0000      0  245
2040  3              1  3  0 0.9653 -14.94     0.00     0.00      0.00     0.00   115.00 0.0000      0.00     0.00 0.0000 0.0000      0  246
7001  1              1  1  2 1.0507  10.79     0.00     0.00    467.00     0.00    13.80 1.0507    210.00 -210.00 0.0000 0.0000 7001  247
7002  1              1  1  2 1.0507  12.48     0.00     0.00    623.00     0.00    13.80 1.0507    280.00 -280.00 0.0000 0.0000 7002  248
7003  1              1  1  2 1.0323  13.76     0.00     0.00   1210.00     0.00    13.80 1.0323    420.00 -420.00 0.0000 0.0000 7003  249
7011  1              1  1  2 1.0145   4.99     0.00     0.00    234.00     0.00    13.80 1.0145    100.00 -100.00 0.0000 0.0000 7011  250
7012  1              1  1  2 1.0507  11.57     0.00     0.00    372.00     0.00    13.80 1.0507    224.00 -224.00 0.0000 0.0000 7012  251
7017  1              1  1  2 1.0507 -10.47     0.00     0.00    330.00     0.00    13.80 1.0507    350.00    0.00 0.0000 0.0000 7017  252
7023  1              1  1  2 1.0507   6.15     0.00     0.00    185.00     0.00    13.80 1.0507    120.00    0.00 0.0000 0.0000 7023  253
7024  1              1  1  2 1.0290  12.60     0.00     0.00    410.00     0.00    13.80 1.0290    224.00 -224.00 0.0000 0.0000 7024  254
7039  1              1  1  2 1.0500   2.11     0.00     0.00    500.00     0.00    20.00 1.0500    200.00 -200.00 0.0000 0.0000 7039  255
7044  1              1  1  2 1.0145 -13.92     0.00     0.00     37.00     0.00    13.80 1.0145     42.00    0.00 0.0000 0.0000 7044  256
7049  1              1  1  3 1.0507   0.00     0.00     0.00      0.00     0.00    13.80 1.0507      0.00    0.00 0.0000 0.0000      0  257
7055  1              1  1  2 0.9967  -7.50     0.00     0.00     45.00     0.00    13.80 0.9967     25.00    0.00 0.0000 0.0000 7055  258
7057  1              1  1  2 1.0212  -3.44     0.00     0.00    165.00     0.00    13.80 1.0212     90.00  -90.00 0.0000 0.0000 7057  259
7061  1              1  1  2 1.0145   1.97     0.00     0.00    400.00     0.00    13.80 1.0145    150.00 -150.00 0.0000 0.0000 7061  260
7062  1              1  1  2 1.0017   5.80     0.00     0.00    400.00     0.00    13.80 1.0017    150.00    0.00 0.0000 0.0000 7062  261
7071  1              1  1  2 0.9893 -25.35     0.00     0.00    116.00     0.00    13.80 0.9893     87.00    0.00 0.0000 0.0000 7071  262
7130  2              1  2  2 1.0507  19.02     0.00     0.00   1292.00     0.00    13.80 1.0507    600.00 -100.00 0.0000 0.0000 7130  263
7139  2              1  2  2 1.0507   2.75     0.00     0.00    700.00     0.00    13.80 1.0507    325.00 -125.00 0.0000 0.0000 7139  264
7166  2              1  2  2 1.0145  35.05     0.00     0.00    553.00     0.00    13.80 1.0145    300.00 -200.00 0.0000 0.0000 7166  265
9001  1              1  9  0 1.0117 -11.25     0.00     0.00      0.00     0.00   115.00 0.0000      0.00     0.00 0.0000 0.0000      0  266
9002  1              1  9  2 0.9945 -18.86     0.00     0.00     -4.20     0.00     6.60 0.9945      2.00    -2.00 0.0000 0.0000 9002  267
9003  1              1  9  0 0.9833 -19.68     2.71     0.94      0.00     0.00     6.60 0.0000      0.00     0.00 0.0014 0.0240      0  268
9004  1              1  9  0 0.9768 -19.82     0.86     0.28      0.00     0.00     6.60 0.0000      0.00     0.00 0.0000 0.0000      0  269
9005  1              1  9  0 1.0117 -11.32     0.00     0.00      0.00     0.00   115.00 0.0000      0.00     0.00 0.0000 0.0000      0  270
9006  1              1  9  0 1.0029 -17.42     0.00     0.00      0.00     0.00     6.60 0.0000      0.00     0.00 0.0000 0.0000      0  271
9007  1              1  9  0 0.9913 -18.69     0.00     0.00      0.00     0.00     6.60 0.0000      0.00     0.00 0.0000 0.0000      0  272
9012  1              1  9  0 1.0023 -17.27     0.00     0.00      0.00     0.00     6.60 0.0000      0.00     0.00 0.0000 0.0000      0  273
9021  1              1  9  0 0.9887 -19.09     4.75     1.56      0.00     0.00     6.60 0.0000      0.00     0.00 0.0000 0.0000      0  274
9022  1              1  9  0 0.9648 -21.67     1.53     0.53      0.00     0.00     0.60 0.0000      0.00     0.00 0.0008 0.0000      0  275
9023  1              1  9  0 0.9747 -19.41     0.00     0.00      0.00     0.00     6.60 0.0000      0.00     0.00 0.0000 0.0000      0  276
9024  1              1  9  0 0.9706 -21.43     1.35     0.47      0.00     0.00     0.60 0.0000      0.00     0.00 0.0007 0.0000      0  277
9025  1              1  9  0 0.9649 -20.48     0.45     0.16      0.00     0.00     0.60 0.0000      0.00     0.00 0.0002 0.0000      0  278
9026  1              1  9  0 0.9657 -20.39     0.45     0.16      0.00     0.00     0.60 0.0000      0.00     0.00 0.0002 0.0000      0  279
9031  1              1  9  0 0.9318 -25.03     1.84     0.64      0.00     0.00     0.60 0.0000      0.00     0.00 0.0010 0.0000      0  280
9032  1              1  9  0 0.9441 -23.84     1.39     0.48      0.00     0.00     0.60 0.0000      0.00     0.00 0.0007 0.0000      0  281
9033  1              1  9  0 0.9286 -25.33     1.89     0.65      0.00     0.00     0.60 0.0000      0.00     0.00 0.0010 0.0000      0  282
9034  1              1  9  0 0.9973 -21.10     1.55     0.54      0.00     0.00     0.60 0.0000      0.00     0.00 0.0008 0.0172      0  283
9035  1              1  9  0 0.9506 -23.19     1.66     0.58      0.00     0.00     0.60 0.0000      0.00     0.00 0.0009 0.0000      0  284
9036  1              1  9  0 0.9598 -22.67     3.03     1.00      0.00     0.00     2.30 0.0000      0.00     0.00 0.0000 0.0000      0  285
9037  1              1  9  0 0.9570 -22.58     1.86     0.64      0.00     0.00     0.60 0.0000      0.00     0.00 0.0010 0.0000      0  286
9038  1              1  9  0 0.9391 -24.41     2.58     0.89      0.00     0.00     0.60 0.0000      0.00     0.00 0.0014 0.0000      0  287
9041  1              1  9  0 0.9636 -21.33     1.01     0.35      0.00     0.00     0.60 0.0000      0.00     0.00 0.0005 0.0000      0  288
9042  1              1  9  0 0.9501 -22.50     0.81     0.28      0.00     0.00     0.60 0.0000      0.00     0.00 0.0004 0.0000      0  289
9043  1              1  9  0 0.9646 -21.42     1.60     0.52      0.00     0.00     2.30 0.0000      0.00     0.00 0.0000 0.0000      0  290
9044  1              1  9  0 0.9790 -19.78     0.00     0.00      0.00     0.00     6.60 0.0000      0.00     0.00 0.0000 0.0000      0  291
9051  1              1  9  2 1.0000 -19.40     0.00     0.00    -35.81     0.00    13.80 1.0000     17.35  -17.35 0.0000 0.0000 9051  292
9052  1              1  9  0 0.9786 -17.25    30.00    23.00      0.00     0.00    13.80 0.0000      0.00     0.00 0.0000 0.0000      0  293
9053  1              1  9  2 1.0000 -17.68     0.00     0.00    -26.48     0.00    13.80 1.0000     12.83  -12.80 0.0000 0.0000 9053  294
9054  1              1  9  2 1.0000  -6.83     0.00     0.00     50.00     0.00    13.80 1.0000     38.00  -38.00 0.0000 0.0000 9054  295
9055  1              1  9  2 1.0000  -7.54     0.00     0.00      8.00     0.00    13.80 1.0000      6.00   -6.00 0.0000 0.0000 9055  296
9071  1              1  9  0 0.9752 -20.48     1.02     0.35      0.00     0.00     0.60 0.0000      0.00     0.00 0.0005 0.0000      0  297
9072  1              1  9  0 0.9803 -19.92     1.02     0.35      0.00     0.00     0.60 0.0000      0.00     0.00 0.0005 0.0000      0  298
9121  1              1  9  0 0.9799 -19.30     3.80     1.25      0.00     0.00     6.60 0.0000      0.00     0.00 0.0000 0.0000      0  299
9533  1              1  9  0 1.0402 -18.24     1.19     0.41      0.00     0.00     2.30 0.0000      0.00     0.00 0.0010 0.0000      0  300
-999 1
BRANCH DATA FOLLOWS                                  411 ITEMS
  37 9001  1  9 1 2  0.000060  0.000460  0.00000     0     0    75    0 0  1.0082    0.00 0.90431.10435 .00400     0.0   15.0      1
9001 9005  1  9 1 0  0.000800  0.003480  0.00000     0     0     0    0 0  0.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000      2
9001 9006  1  9 1 2  0.024390  0.436820  0.00000     0     0     0 9006 0  0.9668    0.00 0.9391 1.1478 .00417  0.9900 1.0100      3
9001 9012  1  9 1 2  0.036240  0.648980  0.00000     0     0     0 9012 0  0.9796    0.00 0.9391 1.1478 .00417  0.9900 1.0100      4
9005 9051  1  9 1 1  0.015780  0.374860  0.00000     0     0     0 9051 0  1.0435    0.00 0.9391 1.1478 .00417  0.9900 1.0100      5
9005 9052  1  9 1 2  0.015780  0.374860  0.00000     0     0     0 9052 0  0.9391    0.00 0.9391 1.1478 .00417  0.9900 1.0100      6
9005 9053  1  9 1 1  0.016020  0.380460  0.00000     0     0     0 9053 0  1.0435    0.00 0.9391 1.1478 .00417  0.9900 1.0100      7
9005 9054  1  9 1 1  0.000000  0.152000  0.00000     0     0     0    0 0  1.0435    0.00 0.0000 0.0000 .00000  0.0000 0.0000      8
9005 9055  1  9 1 1  0.000000  0.800000  0.00000     0     0     0    0 0  1.0435    0.00 0.0000 0.0000 .00000  0.0000 0.0000      9
9006 9007  1  9 1 0  0.055580  0.246660  0.00000     0     0     0    0 0  0.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000     10
9006 9003  1  9 1 0  0.111180  0.493320  0.00000     0     0     0    0 0  0.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000     11
9006 9003  1  9 2 0  0.111180  0.493320  0.00000     0     0     0    0 0  0.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000     12
9012 9002  1  9 1 0  0.076220  0.432860  0.00000     0     0     0    0 0  0.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000     13
9012 9002  1  9 2 0  0.076220  0.432860  0.00000     0     0     0    0 0  0.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000     14
9002 9021  1  9 1 0  0.053700  0.070260  0.00000     0     0     0    0 0  0.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000     15
9021 9023  1  9 1 0  1.106800  0.952780  0.00000     0     0     0    0 0  0.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000     16
9021 9022  1  9 1 1  0.443640  2.815200  0.00000     0     0     0    0 0  1.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000     17
9002 9024  1  9 1 1  0.507480  3.220200  0.00000     0     0     0    0 0  1.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000     18
9023 9025  1  9 1 1  0.666880  3.944000  0.00000     0     0     0    0 0  1.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000     19
9023 9026  1  9 1 1  0.611300  3.615200  0.00000     0     0     0    0 0  1.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000     20
9007 9071  1  9 1 1  0.441200  2.966800  0.00000     0     0     0    0 0  1.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000     21
9007 9072  1  9 1 1  0.307920  2.057000  0.00000     0     0     0    0 0  1.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000     22
9007 9003  1  9 1 0  0.055800  0.246660  0.00000     0     0     0    0 0  0.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000     23
9003 9031  1  9 1 1  0.736330  4.672400  0.00000     0     0     0    0 0  1.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000     24
9003 9032  1  9 1 1  0.769780  4.884600  0.00000     0     0     0    0 0  1.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000     25
9003 9033  1  9 1 1  0.757320  4.805600  0.00000     0     0     0    0 0  1.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000     26
```

9003	9044	1	9	1	0	0.073780	0.063520	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	27
9044	9004	1	9	1	0	0.038320	0.028940	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	28
9004	9041	1	9	1	1	0.366140	2.456000	0.00000	0	0	0	0	0	1.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	29
9004	9042	1	9	1	1	1.059300	5.453600	0.00000	0	0	0	0	0	1.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	30
9004	9043	1	9	1	1	0.156700	1.699400	0.00000	0	0	0	0	0	1.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	31
9003	9034	1	9	1	1	0.130060	1.391200	0.00000	0	0	0	0	0	1.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	32
9003	9035	1	9	1	1	0.544840	3.457200	0.00000	0	0	0	0	0	1.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	33
9003	9036	1	9	1	1	0.154260	1.672900	0.00000	0	0	0	0	0	1.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	34
9003	9037	1	9	1	1	0.384900	2.571200	0.00000	0	0	0	0	0	1.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	35
9003	9038	1	9	1	1	0.441200	2.966800	0.00000	0	0	0	0	0	1.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	36
9012	9121	1	9	1	0	0.235520	0.990360	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	37
9053	9533	1	9	1	1	0.000000	0.750000	0.00000	0	0	0	0	0	0.9583	0.00	0.0000	0.0000	.00000	0.0000	0.0000	38
1	5	1	1	1	0	0.001000	0.006000	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	39
2	6	1	1	1	0	0.001000	0.009000	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	40
2	8	1	1	1	0	0.006000	0.027000	0.05400	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	41
3	7	1	1	1	0	0.000000	0.003000	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	42
3	19	1	1	1	0	0.008000	0.069000	0.13900	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	43
3	150	1	2	1	0	0.001000	0.007000	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	44
4	16	1	1	1	0	0.002000	0.019000	1.12700	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	45
5	9	1	1	1	0	0.006000	0.029000	0.01800	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	46
7	12	1	1	1	0	0.001000	0.009000	0.07000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	47
7	131	1	2	1	0	0.001000	0.007000	0.01400	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	48
8	11	1	1	1	0	0.013000	0.059500	0.03300	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	49
8	14	1	1	1	0	0.013000	0.042000	0.08100	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	50
9	11	1	1	1	0	0.006000	0.027000	0.01300	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	51
11	13	1	1	1	0	0.008000	0.034000	0.01800	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	52
12	21	1	1	1	0	0.002000	0.015000	0.11800	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	53
13	20	1	1	1	0	0.006000	0.034000	0.01600	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	54
14	15	1	1	1	0	0.014000	0.042000	0.09700	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	55
15	37	1	1	1	0	0.065000	0.248000	0.12100	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	56
15	89	1	1	1	0	0.099000	0.248000	0.03500	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	57
15	90	1	1	1	0	0.096000	0.363000	0.04800	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	58
16	42	1	1	1	0	0.002000	0.022000	1.28000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	59
19	21	1	1	1	0	0.002000	0.018000	0.03600	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	60
19	87	1	1	1	0	0.013000	0.080000	0.15100	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	61
20	22	1	1	1	0	0.016000	0.033000	0.01500	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	62
20	27	1	1	1	0	0.069000	0.186000	0.09800	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	63
21	24	1	1	1	0	0.004000	0.034000	0.28000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	64
22	23	1	1	1	0	0.052000	0.111000	0.05000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	65
23	25	1	1	1	0	0.019000	0.039000	0.01800	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	66
24	319	1	1	1	0	0.007000	0.068000	0.13400	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	67
25	26	1	1	1	0	0.036000	0.071000	0.03400	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	68
26	27	1	1	1	0	0.045000	0.120000	0.06500	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	69
26	320	1	1	1	0	0.043000	0.130000	0.01400	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	70
33	34	1	1	1	0	0.000000	0.063000	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	71
33	38	1	1	1	0	0.002500	0.012000	0.01300	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	72
33	40	1	1	1	0	0.006000	0.029000	0.02000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	73
33	41	1	1	1	0	0.007000	0.043000	0.02600	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	74
34	42	1	1	1	0	0.001000	0.008000	0.04200	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	75
35	72	1	1	1	0	0.012000	0.060000	0.00800	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	76
35	76	1	1	1	0	0.006000	0.014000	0.00200	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	77
35	77	1	1	1	0	0.010000	0.029000	0.00300	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	78
36	88	1	1	1	0	0.004000	0.027000	0.04300	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	79
37	38	1	1	1	0	0.008000	0.047000	0.00800	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	80
37	40	1	1	1	0	0.022000	0.064000	0.00700	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	81
37	41	1	1	1	0	0.010000	0.036000	0.02000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	82
37	49	1	1	1	0	0.017000	0.081000	0.04800	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	83
37	89	1	1	1	0	0.102000	0.254000	0.03300	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	84
37	90	1	1	1	0	0.047000	0.127000	0.01600	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	85
38	41	1	1	1	0	0.008000	0.037000	0.02000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	86
38	43	1	1	1	0	0.032000	0.087000	0.04000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	87
39	42	1	1	1	0	0.000600	0.006400	0.40400	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	88
40	48	1	1	1	0	0.026000	0.154000	0.02200	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	89
41	42	1	1	1	0	0.000000	0.029000	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	90
41	49	1	1	1	0	0.065000	0.191000	0.02000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	91
41	51	1	1	1	0	0.031000	0.089000	0.03600	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	92
42	46	1	1	1	0	0.002000	0.014000	0.80600	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	93
43	44	1	1	1	0	0.026000	0.072000	0.03500	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	94
43	48	1	1	1	0	0.095000	0.262000	0.03200	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	95
43	53	1	1	1	0	0.013000	0.039000	0.01600	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	96
44	47	1	1	1	0	0.027000	0.084000	0.03900	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	97
44	54	1	1	1	0	0.028000	0.084000	0.03700	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	98
45	60	1	1	1	0	0.007000	0.041000	0.31200	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	99
45	74	1	1	1	0	0.009000	0.054000	0.41100	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	100
46	81	1	1	1	0	0.005000	0.042000	0.69000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	101
47	73	1	1	1	0	0.052000	0.145000	0.07300	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	102
47	113	1	1	1	0	0.043000	0.118000	0.01300	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	103
48	107	1	1	1	0	0.025000	0.062000	0.00700	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	104
49	51	1	1	1	0	0.031000	0.094000	0.04300	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	105
51	52	1	1	1	0	0.037000	0.109000	0.04900	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	106
52	55	1	1	1	0	0.027000	0.080000	0.03600	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	107
53	54	1	1	1	0	0.025000	0.073000	0.03500	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	108
54	55	1	1	1	0	0.035000	0.103000	0.04700	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	109
55	57	1	1	1	0	0.065000	0.169000	0.08200	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	110
57	58	1	1	1	0	0.046000	0.080000	0.03600	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	111
57	63	1	1	1	0	0.159000	0.537000	0.07100	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	112

58	59	1	1	1	0	0.009000	0.026000	0.00500	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	113
59	61	1	1	1	0	0.002000	0.013000	0.01500	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	114
60	62	1	1	1	0	0.009000	0.065000	0.48500	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	115
62	64	1	1	1	0	0.016000	0.105000	0.20300	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	116
62	144	1	2	1	0	0.001000	0.007000	0.01300	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	117
63	526	1	1	1	0	0.026500	0.172000	0.02600	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	118
69	211	1	3	1	0	0.051000	0.232000	0.02800	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	119
69	79	1	1	1	0	0.051000	0.157000	0.02300	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	120
70	71	1	1	1	0	0.032000	0.100000	0.06200	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	121
70	528	1	1	1	0	0.020000	0.123400	0.02800	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	122
71	72	1	1	1	0	0.036000	0.131000	0.06800	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	123
71	73	1	1	1	0	0.034000	0.099000	0.04700	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	124
72	77	1	1	1	0	0.018000	0.087000	0.01100	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	125
72	531	1	1	1	0	0.025600	0.193000	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	126
73	76	1	1	1	0	0.021000	0.057000	0.03000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	127
73	79	1	1	1	0	0.018000	0.052000	0.01800	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	128
74	88	1	1	1	0	0.004000	0.027000	0.05000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	129
74	562	1	1	1	0	0.028600	0.201300	0.37900	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	130
76	77	1	1	1	0	0.016000	0.043000	0.00400	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	131
77	78	1	1	1	0	0.001000	0.006000	0.00700	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	132
77	80	1	1	1	0	0.014000	0.070000	0.03800	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	133
77	552	1	1	1	0	0.089100	0.267600	0.02900	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	134
77	609	1	1	1	0	0.078200	0.212700	0.02200	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	135
78	79	1	1	1	0	0.006000	0.022000	0.01100	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	136
78	84	1	1	1	0	0.000000	0.036000	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	137
79	211	1	3	1	0	0.099000	0.375000	0.05100	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	138
80	211	1	3	1	0	0.022000	0.107000	0.05800	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	139
81	194	1	3	1	0	0.003500	0.033000	0.53000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	140
81	195	1	3	1	0	0.003500	0.033000	0.53000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	141
85	86	1	1	1	0	0.008000	0.064000	0.12800	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	142
86	87	1	1	1	0	0.012000	0.093000	0.18300	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	143
86	323	1	1	1	0	0.006000	0.048000	0.09200	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	144
89	91	1	1	1	0	0.047000	0.119000	0.01400	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	145
90	92	1	1	1	0	0.032000	0.174000	0.02400	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	146
91	94	1	1	1	0	0.100000	0.253000	0.03100	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	147
91	97	1	1	1	0	0.022000	0.077000	0.03900	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	148
92	103	1	1	1	0	0.019000	0.144000	0.01700	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	149
92	105	1	1	1	0	0.017000	0.092000	0.01200	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	150
94	97	1	1	1	0	0.278000	0.427000	0.04300	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	151
97	100	1	1	1	0	0.022000	0.053000	0.00700	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	152
97	102	1	1	1	0	0.038000	0.092000	0.01200	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	153
97	103	1	1	1	0	0.048000	0.122000	0.01500	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	154
98	100	1	1	1	0	0.024000	0.064000	0.00700	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	155
98	102	1	1	1	0	0.034000	0.121000	0.01500	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	156
99	107	1	1	1	0	0.053000	0.135000	0.01700	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	157
99	108	1	1	1	0	0.002000	0.004000	0.00200	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	158
99	109	1	1	1	0	0.045000	0.354000	0.04400	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	159
99	110	1	1	1	0	0.050000	0.174000	0.02200	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	160
100	102	1	1	1	0	0.016000	0.038000	0.00400	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	161
102	104	1	1	1	0	0.043000	0.064000	0.02700	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	162
103	105	1	1	1	0	0.019000	0.062000	0.00800	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	163
104	108	1	1	1	0	0.076000	0.130000	0.04400	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	164
104	322	1	1	1	0	0.044000	0.124000	0.01500	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	165
105	107	1	1	1	0	0.012000	0.088000	0.01100	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	166
105	110	1	1	1	0	0.157000	0.400000	0.04700	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	167
108	324	1	1	1	0	0.074000	0.208000	0.02600	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	168
109	110	1	1	1	0	0.070000	0.184000	0.02100	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	169
109	113	1	1	1	0	0.100000	0.274000	0.03100	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	170
109	114	1	1	1	0	0.109000	0.393000	0.03600	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	171
110	112	1	1	1	0	0.142000	0.404000	0.05000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	172
112	114	1	1	1	0	0.017000	0.042000	0.00600	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	173
115	122	1	2	1	0	0.003600	0.019900	0.00400	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	174
116	120	1	2	1	0	0.002000	0.104900	0.00100	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	175
117	118	1	2	1	0	0.000100	0.001800	0.01700	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	176
118	119	1	2	1	0	0.000000	0.027100	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	177
118	1201	1	2	1	0	0.000000	0.616300	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	178
1201	120	1	2	1	0	0.000000	-0.369700	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	179
118	121	1	2	1	0	0.002200	0.291500	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	180
119	120	1	2	1	0	0.000000	0.033900	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	181
119	121	1	2	1	0	0.000000	0.058200	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	182
122	123	1	2	1	0	0.080800	0.234400	0.02900	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	183
122	125	1	2	1	0	0.096500	0.366900	0.05400	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	184
123	124	1	2	1	0	0.036000	0.107600	0.11700	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	185
123	125	1	2	1	0	0.047600	0.141400	0.14900	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	186
125	126	1	2	1	0	0.000600	0.019700	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	187
126	127	1	2	1	0	0.005900	0.040500	0.25000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	188
126	129	1	2	1	0	0.011500	0.110600	0.18500	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	189
126	132	1	2	1	0	0.019800	0.168800	0.32100	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	190
126	157	1	2	1	0	0.005000	0.050000	0.33000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	191
126	158	1	2	1	0	0.007700	0.053800	0.33500	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	192
126	169	1	2	1	0	0.016500	0.115700	0.17100	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	193
127	128	1	2	1	0	0.005900	0.057700	0.09500	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	194
127	134	1	2	1	0	0.004900	0.033600	0.20800	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	195
127	168	1	2	1	0	0.005900	0.057700	0.09500	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	196
128	130	1	2	1	0	0.007800	0.077300	0.12600	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	197
128	133	1	2	1	0	0.002600	0.019300	0.03000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	198

```
129  130  1  2 1 0  0.007600  0.075200  0.12200   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  199
129  133  1  2 1 0  0.002100  0.018600  0.03000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  200
130  132  1  2 1 0  0.001600  0.016400  0.02600   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  201
130  151  1  2 1 0  0.001700  0.016500  0.02600   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  202
130  167  1  2 1 0  0.007900  0.079300  0.12700   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  203
130  168  1  2 1 0  0.007800  0.078400  0.12500   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  204
133  137  1  2 1 0  0.001700  0.011700  0.28900   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  205
133  168  1  2 1 0  0.002600  0.019300  0.03000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  206
133  169  1  2 1 0  0.002100  0.018600  0.03000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  207
133  171  1  2 1 0  0.000200  0.010100  0.00000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  208
134  135  1  2 1 0  0.004300  0.029300  0.18000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  209
134  184  1  2 1 0  0.003900  0.038100  0.25800   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  210
135  136  1  2 1 0  0.009100  0.062300  0.38500   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  211
136  137  1  2 1 0  0.012500  0.089000  0.54000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  212
136  152  1  2 1 0  0.005600  0.039000  0.95300   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  213
137  140  1  2 1 0  0.001500  0.011400  0.28400   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  214
137  181  1  2 1 0  0.000500  0.003400  0.02100   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  215
137  186  1  2 1 0  0.000700  0.015100  0.12600   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  216
137  188  1  2 1 0  0.000500  0.003400  0.02100   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  217
139  172  1  2 1 0  0.056200  0.224800  0.08100   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  218
140  141  1  2 1 0  0.012000  0.083600  0.12300   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  219
140  142  1  2 1 0  0.015200  0.113200  0.68400   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  220
140  145  1  2 1 0  0.046800  0.336900  0.51900   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  221
140  146  1  2 1 0  0.043000  0.303100  0.46300   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  222
140  147  1  2 1 0  0.048900  0.349200  0.53800   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  223
140  182  1  2 1 0  0.001300  0.008900  0.11900   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  224
141  146  1  2 1 0  0.029100  0.226700  0.34200   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  225
142  143  1  2 1 0  0.006000  0.057000  0.76700   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  226
143  145  1  2 1 0  0.007500  0.077300  0.11900   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  227
143  149  1  2 1 0  0.012700  0.090900  0.13500   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  228
145  146  1  2 1 0  0.008500  0.058800  0.08700   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  229
145  149  1  2 1 0  0.021800  0.151100  0.22300   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  230
146  147  1  2 1 0  0.007300  0.050400  0.07400   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  231
148  178  1  2 1 0  0.052300  0.152600  0.07400   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  232
148  179  1  2 1 0  0.137100  0.391900  0.07600   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  233
152  153  1  2 1 0  0.013700  0.095700  0.14100   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  234
153  161  1  2 1 0  0.005500  0.028800  0.19000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  235
154  156  1  2 1 0  0.174600  0.316100  0.04000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  236
154  183  1  2 1 0  0.080400  0.305400  0.04500   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  237
155  161  1  2 1 0  0.011000  0.056800  0.38800   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  238
157  159  1  2 1 0  0.000800  0.009800  0.06900   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  239
158  159  1  2 1 0  0.002900  0.028500  0.19000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  240
158  160  1  2 1 0  0.006600  0.044800  0.27700   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  241
162  164  1  2 1 0  0.002400  0.032600  0.23600   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  242
162  165  1  2 1 0  0.001800  0.024500  1.66200   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  243
163  164  1  2 1 0  0.004400  0.051400  3.59700   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  244
165  166  1  2 1 0  0.000200  0.012300  0.00000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  245
167  169  1  2 1 0  0.001800  0.017800  0.02900   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  246
172  173  1  2 1 0  0.066900  0.484300  0.06300   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  247
172  174  1  2 1 0  0.055800  0.221000  0.03100   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  248
173  174  1  2 1 0  0.080700  0.333100  0.04900   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  249
173  175  1  2 1 0  0.073900  0.307100  0.04300   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  250
173  176  1  2 1 0  0.179900  0.501700  0.06900   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  251
175  176  1  2 1 0  0.090400  0.362600  0.04800   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  252
175  179  1  2 1 0  0.077000  0.309200  0.05400   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  253
176  177  1  2 1 0  0.025100  0.082900  0.04700   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  254
177  178  1  2 1 0  0.022200  0.084700  0.05000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  255
178  179  1  2 1 0  0.049800  0.185500  0.02900   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  256
178  180  1  2 1 0  0.006100  0.029000  0.08400   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  257
181  138  1  2 1 0  0.000400  0.020200  0.00000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  258
181  187  1  2 1 0  0.000400  0.008300  0.11500   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  259
184  185  1  2 1 0  0.002500  0.024500  0.16400   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  260
186  188  1  2 1 0  0.000700  0.008600  0.11500   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  261
187  188  1  2 1 0  0.000700  0.008600  0.11500   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  262
188  138  1  2 1 0  0.000400  0.020200  0.00000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  263
189  208  1  3 1 0  0.033000  0.095000  0.00000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  264
189  209  1  3 1 0  0.046000  0.069000  0.00000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  265
190  231  1  3 1 0  0.000400  0.002200  6.20000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  266
190  240  1  3 1 0  0.000000  0.027500  0.00000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  267
191  192  1  3 1 0  0.003000  0.048000  0.00000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  268
192  225  1  3 1 0  0.002000  0.009000  0.00000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  269
193  205  1  3 1 0  0.045000  0.063000  0.00000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  270
193  208  1  3 1 0  0.048000  0.127000  0.00000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  271
194  219  1  3 1 0  0.003100  0.028600  0.50000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  272
194  664  1  3 1 0  0.002400  0.035500  0.36000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  273
195  219  1  3 1 0  0.003100  0.028600  0.50000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  274
196  197  1  3 1 0  0.014000  0.040000  0.00400   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  275
196  210  1  3 1 0  0.030000  0.081000  0.01000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  276
197  198  1  3 1 0  0.010000  0.060000  0.00900   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  277
197  211  1  3 1 0  0.015000  0.040000  0.00600   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  278
198  202  1  3 1 0  0.332000  0.688000  0.00000   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  279
198  203  1  3 1 0  0.009000  0.046000  0.02500   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  280
198  210  1  3 1 0  0.020000  0.073000  0.00800   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  281
198  211  1  3 1 0  0.034000  0.109000  0.03200   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  282
199  200  1  3 1 0  0.076000  0.135000  0.00900   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  283
199  210  1  3 1 0  0.040000  0.102000  0.00500   0   0   0   0 0  0.0000   0.00 0.0000 0.0000 .00000  0.0000 0.0000  284
```

200	210	1	3	1	0	0.081000	0.128000	0.01400	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	285
201	204	1	3	1	0	0.124000	0.183000	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	286
203	211	1	3	1	0	0.010000	0.059000	0.00800	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	287
204	205	1	3	1	0	0.046000	0.068000	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	288
205	206	1	3	1	0	0.302000	0.446000	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	289
206	207	1	1	1	0	0.073000	0.093000	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	290
206	208	1	3	1	0	0.240000	0.421000	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	291
212	215	1	3	1	0	0.013900	0.077800	0.08600	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	292
213	214	1	3	1	1	0.002500	0.038000	0.00000	0	0	0	0	0	1.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	293
214	215	1	3	1	0	0.001700	0.018500	0.02000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	294
214	242	1	3	1	0	0.001500	0.010800	0.00200	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	295
215	216	1	3	1	0	0.004500	0.024900	0.02600	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	296
216	217	1	3	1	0	0.004000	0.049700	0.01800	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	297
217	218	1	3	1	0	0.000000	0.045600	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	298
217	219	1	3	1	0	0.000500	0.017700	0.02000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	299
217	220	1	3	1	0	0.002700	0.039500	0.83200	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	300
219	237	1	3	1	0	0.000300	0.001800	5.20000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	301
220	218	1	3	1	0	0.003700	0.048400	0.43000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	302
220	221	1	3	1	0	0.001000	0.029500	0.50300	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	303
220	238	1	3	1	0	0.001600	0.004600	0.40200	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	304
221	223	1	3	1	0	0.000300	0.001300	1.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	305
222	237	1	3	1	1	0.001400	0.051400	0.33000	0	0	0	0	0	1.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	306
224	225	1	3	1	0	0.010000	0.064000	0.48000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	307
224	226	1	3	1	0	0.001900	0.008100	0.86000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	308
225	191	1	3	1	0	0.001000	0.061000	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	309
226	231	1	3	1	0	0.000500	0.021200	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	310
227	231	1	3	1	1	0.000900	0.047200	0.18600	0	0	0	0	0	1.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	311
228	229	1	3	1	0	0.001900	0.008700	1.28000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	312
228	231	1	3	1	0	0.002600	0.091700	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	313
228	234	1	3	1	0	0.001300	0.028800	0.81000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	314
229	190	1	3	1	0	0.000000	0.062600	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	315
231	232	1	3	1	0	0.000200	0.006900	1.36400	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	316
231	237	1	3	1	0	0.000100	0.000600	3.57000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	317
232	233	1	3	1	0	0.001700	0.048500	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	318
234	235	1	3	1	0	0.000200	0.025900	0.14400	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	319
234	237	1	3	1	0	0.000600	0.027200	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	320
235	238	1	3	1	0	0.000200	0.000600	0.80000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	321
241	237	1	3	1	1	0.000500	0.015400	0.00000	0	0	0	0	0	1.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	322
240	281	1	3	1	0	0.000300	0.004300	0.00900	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	323
242	245	1	3	1	0	0.008200	0.085100	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	324
242	247	1	3	1	0	0.011200	0.072300	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	325
243	244	1	3	1	0	0.012700	0.035500	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	326
243	245	1	3	1	0	0.032600	0.180400	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	327
244	246	1	3	1	0	0.019500	0.055100	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	328
245	246	1	3	1	0	0.015700	0.073200	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	329
245	247	1	3	1	0	0.036000	0.211900	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	330
246	247	1	3	1	0	0.026800	0.128500	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	331
247	248	1	3	1	0	0.042800	0.121500	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	332
248	249	1	3	1	0	0.035100	0.100400	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	333
249	250	1	3	1	0	0.061600	0.185700	0.00000	0	0	0	0	0	0.0000	0.00	0.0000	0.0000	.00000	0.0000	0.0000	334
3	1	1	1	1	2	0.000000	0.052000	0.00000	0	0	0	1	0	0.9470	0.00	0.9000	1.1000	.00200	0.9000	1.1000	335
3	2	1	1	1	2	0.000000	0.052000	0.00000	0	0	0	2	0	0.9560	0.00	0.9000	1.1000	.00200	0.9000	1.1000	336
3	4	1	1	1	2	0.000000	0.005000	0.00000	0	0	0	4	0	0.9710	0.00	0.9000	1.1000	.00200	0.9000	1.1000	337
7	5	1	1	1	2	0.000000	0.039000	0.00000	0	0	0	5	0	0.9480	0.00	0.9000	1.1000	.00200	0.9000	1.1000	338
7	6	1	1	1	2	0.000000	0.039000	0.00000	0	0	0	6	0	0.9590	0.00	0.9000	1.1000	.00200	0.9000	1.1000	339
10	11	1	1	1	2	0.000000	0.089000	0.00000	0	0	0	11	0	1.0460	0.00	0.9000	1.1000	.00200	0.9000	1.1000	340
12	10	1	1	1	1	0.000000	0.053000	0.00000	0	0	0	10	0	0.9850	0.00	0.9000	1.1000	.00200	0.9000	1.1000	341
15	17	1	1	1	2	0.019400	0.031100	0.00000	0	0	0	17	0	0.9561	0.00	0.9000	1.1000	.00200	0.9000	1.1000	342
16	15	1	1	1	2	0.001000	0.038000	0.00000	0	0	0	15	0	0.9710	0.00	0.9000	1.1000	.00200	0.9000	1.1000	343
21	20	1	1	1	1	0.000000	0.014000	0.00000	0	0	0	20	0	0.9520	0.00	0.9000	1.1000	.00200	0.9000	1.1000	344
24	23	1	1	1	2	0.000000	0.064000	0.00000	0	0	0	23	0	0.9430	0.00	0.9000	1.1000	.00200	0.9000	1.1000	345
36	35	1	1	1	2	0.000000	0.047000	0.00000	0	0	0	35	0	1.0100	0.00	0.9000	1.1000	.00200	0.9000	1.1000	346
45	44	1	1	1	2	0.000000	0.020000	0.00000	0	0	0	44	0	1.0080	0.00	0.9000	1.1000	.00200	0.9000	1.1000	347
45	46	1	1	1	2	0.000000	0.021000	0.00000	0	0	0	46	0	1.0000	0.00	0.9000	1.1000	.00200	0.9000	1.1000	348
62	61	1	1	1	2	0.000000	0.059000	0.00000	0	0	0	61	0	0.9750	0.00	0.9000	1.1000	.00200	0.9000	1.1000	349
63	64	1	1	1	2	0.000000	0.038000	0.00000	0	0	0	64	0	1.0170	0.00	0.9000	1.1000	.00200	0.9000	1.1000	350
73	74	1	1	1	2	0.000000	0.024400	0.00000	0	0	0	74	0	1.0000	0.00	0.9000	1.1000	.00200	0.9000	1.1000	351
81	88	1	1	1	2	0.000000	0.020000	0.00000	0	0	0	88	0	1.0000	0.00	0.9000	1.1000	.00200	0.9000	1.1000	352
85	99	1	1	1	2	0.000000	0.048000	0.00000	0	0	0	99	0	1.0000	0.00	0.9000	1.1000	.00200	0.9000	1.1000	353
86	102	1	1	1	2	0.000000	0.048000	0.00000	0	0	0	102	0	1.0000	0.00	0.9000	1.1000	.00200	0.9000	1.1000	354
87	94	1	1	1	2	0.000000	0.046000	0.00000	0	0	0	94	0	1.0150	0.00	0.9000	1.1000	.00200	0.9000	1.1000	355
114	207	1	1	1	2	0.000000	0.149000	0.00000	0	0	0	207	0	0.9670	0.00	0.9000	1.1000	.00200	0.9000	1.1000	356
116	124	1	2	1	1	0.005200	0.017400	0.00000	0	0	0	124	0	1.0100	0.00	0.9000	1.1000	.00200	0.9000	1.1000	357
121	115	1	2	1	2	0.000000	0.028000	0.00000	0	0	0	115	0	1.0500	0.00	0.9000	1.1000	.00200	0.9000	1.1000	358
122	157	1	2	1	2	0.000500	0.019500	0.00000	0	0	0	157	0	1.0000	0.00	0.9000	1.1000	.00200	0.9000	1.1000	359
130	131	1	2	1	2	0.000000	0.018000	0.00000	0	0	0	131	0	1.0522	0.00	0.9000	1.1000	.00200	0.9000	1.1000	360
130	150	1	2	1	2	0.000000	0.014000	0.00000	0	0	0	150	0	1.0522	0.00	0.9000	1.1000	.00200	0.9000	1.1000	361
132	170	1	2	1	1	0.001000	0.040200	0.00000	0	0	0	170	0	1.0500	0.00	0.9000	1.1000	.00200	0.9000	1.1000	362
141	174	1	2	1	2	0.002400	0.060300	0.00000	0	0	0	174	0	0.9750	0.00	0.9000	1.1000	.00200	0.9000	1.1000	363
142	175	1	2	1	2	0.002400	0.049800	-0.08700	0	0	0	175	0	1.0000	0.00	0.9000	1.1000	.00200	0.9000	1.1000	364
143	144	1	2	1	2	0.000000	0.083300	0.00000	0	0	0	144	0	1.0350	0.00	0.9000	1.1000	.00200	0.9000	1.1000	365
143	148	1	2	1	2	0.001300	0.037100	0.00000	0	0	0	148	0	0.9565	0.00	0.9000	1.1000	.00200	0.9000	1.1000	366
145	180	1	2	1	2	0.000500	0.018200	0.00000	0	0	0	180	0	1.0000	0.00	0.9000	1.1000	.00200	0.9000	1.1000	367
151	170	1	2	1	1	0.001000	0.039200	0.00000	0	0	0	170	0	1.0500	0.00	0.9000	1.1000	.00200	0.9000	1.1000	368
153	183	1	2	1	2	0.002700	0.063900	0.00000	0	0	0	183	0	1.0730	0.00	0.9000	1.1000	.00200	0.9000	1.1000	369
155	156	1	2	1	1	0.000800	0.025600	0.00000	0	0	0	156	0	1.0500	0.00	0.9000	1.1000	.00200	0.9000	1.1000	370

```
 159  117  1  2 1 2  0.000000  0.016000   0.00000      0     0     0  117 0  1.0506    0.00 0.9000 1.1000 .00200  0.9000 1.1000   371
 160  124  1  2 1 1  0.001200  0.039600   0.00000      0     0     0  124 0  0.9750    0.00 0.9000 1.1000 .00200  0.9000 1.1000   372
 163  137  1  2 1 2  0.001300  0.038400  -0.05700      0     0     0  137 0  0.9800    0.00 0.9000 1.1000 .00200  0.9000 1.1000   373
 164  155  1  2 1 2  0.000900  0.023100  -0.03300      0     0     0  155 0  0.9560    0.00 0.9000 1.1000 .00200  0.9000 1.1000   374
 182  139  1  2 1 2  0.000300  0.013100   0.00000      0     0     0  139 0  1.0500    0.00 0.9000 1.1000 .00200  0.9000 1.1000   375
 189  210  1  3 1 2  0.000000  0.252000   0.00000      0     0     0  210 0  1.0300    0.00 0.9000 1.1000 .00200  0.9000 1.1000   376
 193  196  1  3 1 2  0.000000  0.237000   0.00000      0     0     0  196 0  1.0300    0.00 0.9000 1.1000 .00200  0.9000 1.1000   377
 195  212  1  3 1 2  0.000800  0.036600   0.00000      0     0     0  212 0  0.9850    0.00 0.9000 1.1000 .00200  0.9000 1.1000   378
 200  248  1  3 1 2  0.000000  0.220000   0.00000      0     0     0  248 0  1.0000    0.00 0.9000 1.1000 .00200  0.9000 1.1000   379
 201   69  1  1 2 2  0.000000  0.098000   0.00000      0     0     0   69 0  1.0300    0.00 0.9000 1.1000 .00200  0.9000 1.1000   380
 202  211  1  3 1 2  0.000000  0.128000   0.00000      0     0     0  211 0  1.0100    0.00 0.9000 1.1000 .00200  0.9000 1.1000   381
 204 2040  1  3 1 2  0.020000  0.204000  -0.01200      0     0     0  196    1.0500    0.00 0.9000 1.1000 .00200  0.9000 1.1000   382
 209  198  1  3 1 1  0.026000  0.211000   0.00000      0     0     0  198 0  1.0300    0.00 0.9000 1.1000 .00200  0.9000 1.1000   383
 211  212  1  3 1 2  0.003000  0.012200   0.00000      0     0     0  212 0  1.0000    0.00 0.9000 1.1000 .00200  0.9000 1.1000   384
 218  219  1  3 1 2  0.001000  0.035400  -0.01000      0     0     0  219 0  0.9700    0.00 0.9000 1.1000 .00200  0.9000 1.1000   385
 223  224  1  3 1 2  0.001200  0.019500  -0.36400      0     0     0  224 0  1.0000    0.00 0.9000 1.1000 .00200  0.9000 1.1000   386
 229  230  1  3 1 1  0.001000  0.033200   0.00000      0     0     0  230 0  1.0200    0.00 0.9000 1.1000 .00200  0.9000 1.1000   387
 234  236  1  3 1 1  0.000500  0.016000   0.00000      0     0     0  236 0  1.0700    0.00 0.9000 1.1000 .00200  0.9000 1.1000   388
 238  239  1  3 1 1  0.000500  0.016000   0.00000      0     0     0  239 0  1.0200    0.00 0.9000 1.1000 .00200  0.9000 1.1000   389
 196 2040  1  3 1 4  0.000100  0.020000   0.00000      0     0     0    0 0  1.0000  -11.40 -15.00    0.00   0.30    80.0    85.0   390
 119 1190  1  2 1 2  0.001000  0.023000   0.00000      0     0     0 1190 0  1.0223    0.00 0.8435 1.1565 .00313  1.0107 1.0145   391
 120 1200  1  2 1 2  0.000000  0.023000   0.00000      0     0     0 1200 0  0.9284    0.00 0.8435 1.1565 .00313  1.0225 1.0263   392
7002    2  1  1 1 1  0.001000  0.014600   0.00000      0     0     0    0 0  1.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000   393
7003    3  1  1 1 1  0.000000  0.010540   0.00000      0     0     0    0 0  1.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000   394
7061   61  1  1 1 1  0.000000  0.023800   0.00000      0     0     0    0 0  1.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000   395
7062   62  1  1 1 1  0.000000  0.032140   0.00000      0     0     0    0 0  0.9500    0.00 0.0000 0.0000 .00000  0.0000 0.0000   396
7166  166  1  2 1 1  0.000000  0.015400   0.00000      0     0     0    0 0  1.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000   397
7024   24  1  1 1 1  0.000000  0.028900   0.00000      0     0     0    0 0  1.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000   398
7001    1  1  1 1 1  0.000000  0.019530   0.00000      0     0     0    0 0  1.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000   399
7130  130  1  2 1 1  0.000000  0.019300   0.00000      0     0     0    0 0  1.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000   400
7011   11  1  1 1 1  0.000000  0.019230   0.00000      0     0     0    0 0  1.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000   401
7023   23  1  1 1 1  0.000000  0.023000   0.00000      0     0     0    0 0  1.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000   402
7049   49  1  1 1 1  0.000000  0.012400   0.00000      0     0     0    0 0  1.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000   403
7139  139  1  2 1 1  0.000000  0.016700   0.00000      0     0     0    0 0  1.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000   404
7012   12  1  1 1 1  0.000000  0.031200   0.00000      0     0     0    0 0  1.0000    0.00 0.0000 0.0000 .00000  0.0000 0.0000   405
7017   17  1  1 1 1  0.000000  0.016540   0.00000      0     0     0    0 0  0.9420    0.00 0.0000 0.0000 .00000  0.0000 0.0000   406
7039   39  1  1 1 1  0.000000  0.031590   0.00000      0     0     0    0 0  0.9650    0.00 0.0000 0.0000 .00000  0.0000 0.0000   407
7057   57  1  1 1 1  0.000000  0.053470   0.00000      0     0     0    0 0  0.9500    0.00 0.0000 0.0000 .00000  0.0000 0.0000   408
7044   44  1  1 1 1  0.000000  0.181810   0.00000      0     0     0    0 0  0.9420    0.00 0.0000 0.0000 .00000  0.0000 0.0000   409
7055   55  1  1 1 1  0.000000  0.196070   0.00000      0     0     0    0 0  0.9420    0.00 0.0000 0.0000 .00000  0.0000 0.0000   410
7071   71  1  1 1 1  0.000000  0.068960   0.00000      0     0     0    0 0  0.9565    0.00 0.0000 0.0000 .00000  0.0000 0.0000   411
-999 1
LOSS ZONES FOLLOWS                              0 ITEMS
-99
END OF DATA
```

La sécurisation des infrastructures critiques : recherche d'une méthodologie d'identification des vulnérabilités et modélisation des interdépendances

Résumé Les travaux de cette thèse portent sur la sécurisation des infrastructures critiques. Celles-ci sont constituées de l'ensemble des grands réseaux indispensables au bon fonctionnement d'une société. Ce travail s'attache particulièrement aux réseaux électriques et de télécommunications associés. Les interdépendances entre ces derniers amènent à l'apparition de nouvelles vulnérabilités. Pour progresser dans la compréhension de ces vulnérabilités afin de les réduire, deux approches complémentaires ont été explorées. La première est la création d'un outil de simulation comportementale pour systèmes multi-infrastructures. La seconde est la proposition d'une modélisation multi-infrastructures inspirée par la théorie des réseaux complexes. Grâce à cette modélisation, diverses études, en particulier sur l'évaluation de l'influence du réseau de communication sur l'impact des pannes généralisées dans les réseaux électriques ont été réalisées.

Mots clés *Interdépendances, sécurisation, infrastructures critiques, réseau électrique, réseau de communication, technologies de l'information et de la communication, systèmes couplés, vulnérabilités, cosimulateur, théorie des réseaux complexes.*

Critical Infrastructures Protection : a methodology for vulnerabilities identification and interdependencies modelling

Abstract The research work presented in this PhD thesis deals with Critical Infrastructure Protection. Critical infrastructures are defined as the set of essential networks for the normal functioning of our modern society. This work is particularly focused on the electrical grid and the communication and information networks. Interdependencies between these networks create new vulnerabilities. In order to understand and reduce them, two different approaches were explored. The first one is the building of a multi-infrastructure combined simulator. The second one is the proposal of an original multi-infrastructure model based on the complex networks theory. Thanks to this modelling, dedicated studies were accomplished, principally on the evaluation of the communication network impact on blackouts in power systems.

Keywords *Interdependencies, Critical Infrastructures Protection, power grid, communication systems, Information and Communication Technologies, coupled systems, vulnerabilities, combined simulator, complex network theory.*

Laboratoire de Génie Électrique de Grenoble – G2Elab
UMR 5269 – Grenoble INP / UJF / CNRS
961 rue de la Houille Blanche
BP 46
38 402 St Martin d'Hères CEDEX
FRANCE