POLYPUBLIE
Polytechnique Montréal

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Titre: Title:	Le partage d'informations confidentielles sur une plateforme web dédiée aux interdépendances entre les infrastructures essentielles
Auteur: Author:	Dona-Maria Awedikian
Date:	2013
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Awedikian, D.-M. (2013). Le partage d'informations confidentielles sur une plateforme web dédiée aux interdépendances entre les infrastructures essentielles [Mémoire de maîtrise, École Polytechnique de Montréal]. PolyPublie. https://publications.polymtl.ca/1160/

Document en libre accès dans PolyPublie
Open Access document in PolyPublie

URL de PolyPublie: PolyPublie URL:	https://publications.polymtl.ca/1160/
Directeurs de recherche: Advisors:	Benoît Robert
Programme: Program:	Génie industriel

Ce fichier a été téléchargé à partir de PolyPublie, le dépôt institutionnel de Polytechnique Montréal
This file has been downloaded from PolyPublie, the institutional repository of Polytechnique Montréal

https://publications.polymtl.ca

UNIVERSITÉ DE MONTRÉAL

LE PARTAGE D'INFORMATIONS CONFIDENTIELLES SUR UNE PLATEFORME WEB DÉDIÉE AUX INTERDÉPENDANCES ENTRE LES INFRASTRUCTURES ESSENTIELLES

DONA-MARIA AWEDIKIAN

DÉPARTEMENT DE MATHÉMATIQUES ET DE GÉNIE INDUSTRIEL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION

DU DIPLÔME DE MAITRÎSE ÈS SCIENCES APPLIQUÉES

(GÉNIE INDUSTRIEL)

AOÛT 2013

© Dona-Maria Awedikian, 2013.

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé :

LE PARTAGE D'INFORMATIONS CONFIDENTIELLES SUR UNE PLATEFORME WEB DÉDIÉE AUX INTERDÉPENDANCES ENTRE LES INFRASTRUCTURES ESSENTIELLES

présenté par : AWEDIKIAN Dona-Maria

en vue de l'obtention du diplôme de : Maîtrise ès sciences appliquées
a été dûment accepté par le jury d'examen constitué de :

M. TRÉPANIER Martin, ing, Ph.D., président

M. ROBERT Benoît, ing, Ph.D., membre et directeur de recherche

M. SABOURIN Jean-Pierre, M.A., membre

« People who say it cannot be done should not interrupt those who are doing it. »

George Bernard Shaw

« Ceux qui disent que c'est infaisable ne doivent pas interrompre ceux qui le font. »

George Bernard Shaw (Traduction Libre)

REMERCIEMENTS

En premier lieu, je tiens à remercier mon directeur de recherche et directeur du *Centre risque & performance* (CRP) de l'École Polytechnique de Montréal, le professeur Benoît Robert, de m'avoir accepté et encadré pour travailler sur l'un des projets du CRP. Sa confiance m'a donné l'opportunité d'effectuer une maîtrise recherche en génie industriel.

Je tiens à remercier Luciano Morabito avec qui j'ai eu énormément le plaisir de collaborer au CRP. Ses connaissances poussées et ses conseils continus et pertinents m'ont permis de surmonter tous les défis et d'atteindre mes objectifs.

Je tiens aussi à remercier les autres membres du CRP avec qui j'ai eu le plaisir de partager d'agréables moments.

Je remercie ma sœur Zeina et son mari Paul, qui ont toujours été prêts pour m'aider quand j'en avais besoin. Merci de m'avoir reçue pour plusieurs mois chez vous. Je remercie aussi la famille de mon oncle Elias, la famille Karam et la famille de Mme Flynn, qui m'ont traité comme une de leurs enfants et m'ont donné la chance de passer avec eux de beaux moments.

Je remercie mes parents, Avedis et Souraya, et ma sœur Ghenwa. Merci d'avoir toujours cru en moi et de m'avoir supportée tout le long de ces deux années passées à Montréal, malgré la distance et le décalage horaire. Ce mémoire, c'est avant tout à vous que je le dois.

Je tiens à remercier mon grand amour, Jean Pierre, mon très grand soutien quotidien, même à distance. Merci du fond du cœur pour ta patience, ta générosité et ton support. Merci de m'avoir toujours relevé le moral dans les moments difficiles. La conclusion heureuse de toute cette histoire, c'est à toi que je la dois.

Je voudrais aussi remercier les nombreuses personnes avec lesquelles j'ai eu la chance de passer des moments inoubliables à Montréal. Je ne vais jamais oublier cette expérience bien enrichissante d'une culture aussi riche et pleine de belles surprises. Je tiens à mentionner Stéphanie qui a été une amie très proche de moi.

Enfin, je souhaite remercier les membres de mon jury pour le temps précieux qu'ils m'ont accordé pour juger mes travaux de recherche.

RÉSUMÉ

Les infrastructures essentielles sont des systèmes complexes qui ont pour but de fournir à la société les ressources essentielles à son bon fonctionnement (eau, gaz naturel, électricité, liens téléphoniques, etc.). Ces infrastructures sont dépendantes les unes des autres en raison des ressources qu'elles s'échangent. Ainsi, lorsqu'une infrastructure essentielle devient défaillante, elle peut entraîner la défaillance des autres infrastructures qui utilisent la ressource qu'elle produit. Cela peut entraîner des défaillances en cascade se propageant de réseau en réseau que l'on appelle des effets domino. Ces effets domino peuvent avoir des conséquences néfastes sur l'ensemble des activités économiques et sur le bien-être de la population. Dans le but de diminuer la vulnérabilité de nos sociétés face à ces phénomènes, il est important d'élargir les connaissances concernant les interdépendances entre les infrastructures essentielles.

Dans ce contexte, le *Centre risque & performance* de l'École Polytechnique de Montréal a développé, depuis une dizaine d'années, une approche simple, mais efficace, qui permet l'identification des interdépendances entre les infrastructures essentielles. Cette méthodologie a permis le développement de DOMINO, un outil qui permet l'anticipation d'effets domino potentiels suite à la défaillance de l'une de ces infrastructures. Actuellement à l'état de prototype, le déploiement opérationnel de cet outil est soumis à une contrainte majeure. Pour pouvoir être utilisable, il doit nécessairement être accessible par les différents gestionnaires d'infrastructures essentielles et par les responsables du centre de sécurité civile. Cette question de l'accessibilité représente un défi puisqu'elle demande d'abord une réponse technique, c'est-à-dire le développement d'un système accessible, mais aussi organisationnelle, c'est-à-dire le développement d'un cadre de fonctionnement permettant le partage d'informations confidentielles entre des organisations multiples.

L'objectif des travaux présentés dans ce mémoire a donc été d'aborder ces deux questions en développant une plateforme informatique accessible via l'Internet qui permet aux organisations d'échanger des informations permettant une meilleure gestion de leurs interdépendances tout en respectant le caractère confidentiel de ces informations. Dans un premier temps, il a été nécessaire d'étudier les besoins des futurs utilisateurs du système (qui sont en quelque sorte le

client) et d'établir l'analyse fonctionnelle du système, c'est-à-dire de dresser l'ensemble des fonctionnalités que le système devra réaliser. Ensuite, il a été nécessaire d'aborder la question de la confidentialité des informations en intégrant au système un volet permettant la gestion des accès. Ces travaux ont permis de créer une version web du prototype DOMINO qui répond aux deux principales contraintes soulevées précédemment, soit l'accessibilité et la confidentialité.

Une phase de test était nécessaire pour s'assurer du bon fonctionnement du prototype développé et pour valider son utilisation. Une première phase de validation, à l'interne du CRP, a permis de valider la justesse des résultats qu'il produit. Une deuxième phase de validation, auprès des partenaires, a permis de soulever quelques-uns des nombreux défis qui devront être soulevés avant de rendre une telle application réellement opérationnelle sur une municipalité.

Rendre l'information accessible tout en conservant la confidentialité, est l'un des principaux défis de la mise en œuvre de tels systèmes d'information. Donc, l'accessibilité et la confidentialité de l'information doivent être abordées en parallèle. Un équilibre à rechercher entre accessibilité et confidentialité constitue un défi principal car l'échec de chacun de ceux-ci peut influencer négativement l'utilisation du système. Finalement, quelques modèles de sécurité existants pour tels outils ont été présentés dans ce mémoire en mettant l'appui sur la nécessité d'en créer un pour le Canada.

ABSTRACT

Critical infrastructures (CI) are complex systems that are placed to respond to people's needs (water, natural gas, electricity, telephone links, etc.), to ensure proper functioning of industrialized societies. CI are dependent from each other and our societies depend on the resources provided by these CI.

Thus, when a CI fails, it can cause failure of another CI that uses its resources. This can cause cascading failures from network to another called Domino Effect (ED) and then the total socio-economic environment will be paralysed. In order to reduce the vulnerability of our societies and to protect the CI, it is important to broaden the knowledge of their interdependencies and the ED they generate.

In this context, the *Centre risque & performance* (CRP) of the École Polytechnique de Montréal has been working in this domain for the last decade and was able to develop a simple and effective methodology for the identification of ED between the CI. However, this methodology should be automated and computerized to generate results. Also, information sharing between CI and managers responsible for the civil security can ensure coordination between the different stakeholders and result in proper management of these risks.

The objective of the work presented in this thesis is the sharing of confidential information related to interdependencies between CI and simulation of ED of 3rd order. To achieve this it was necessary to find an IT-related platform that will ensure the availability of partners to access such tool. For this reason, DOMINO web version was created. This tool generates curves dependencies that simulate interdependencies between CI and that simulate ED. It also generates analysis reports of data related to CI, their resources and their interdependencies.

At first, it was necessary to study the requirements of the clients who are the future users of the system and to determine the functional analysis and the access management of the system.

Thereafter, based on the concept of the database from previous projects, it was necessary to modify this database to suit the needs of future users of the system and optimize it for better analysis. Once the new database designed and established, the prototype of DOMINO web was designed and developed too.

To ensure proper functioning of the developed prototype and validate its use and the problems that are related, the third chapter was created. It has the internal testing phase done by the CRP based on several already known simulations. Thereafter, it was possible to present the tool to the partners of the CRP. The challenges of the system availability versus confidentiality were presented and the various issues arising from such tool were addressed to the partners to withdraw their recommendations as it is for them that the system is created.

Making such system accessible while maintaining its confidentiality is one of the main challenges that arises during the implementation. So, accessibility and confidentiality of information must be addressed in parallel because the failure of one of these can adversely affect the system use. Finally, some existing models of security for such tools were presented in this thesis with special support on the need to create one for Canada.

TABLE DES MATIÈRES

REMERCIEMENTS IV

RÉSUMÉ VI

ABSTRACT VIII

TABLE DES MATIÈRES X

LISTE DES TABLEAUX XIII

LISTE DES FIGURES XIV

LISTE DES SIGLES ET ABRÉVIATIONS XV

LISTE DES ANNEXES XVII

INTRODUCTION 1

CHAPITRE 1 MISE EN CONTEXTE 4

1.1 Projets précédents 4

1.1.1 Subventions obtenues par le CRP 4

1.1.2 Courbes de dépendances et cartographie floue 5

1.1.3 DOMINO 10

1.2 Problématiques 15

1.2.1 Problématique liée à l'outil 16

1.2.2 Problématique liée au partage d'information 17

1.3 Projet actuel 17

1.3.1 Objectifs 18

1.3.2 Résultats attendus 20

1.3.3 Originalité des travaux 21

1.3.4 Contraintes 23

CHAPITRE 2 DÉVELOPPEMENT DU PROTOTYPE WEB 25

2.1 Analyse des requis 26
2.2 Analyse fonctionnelle 28
2.3 Gestion des accès 30
2.4 Conception 32
2.4.1 Conception de la base de données 32
2.4.2 Améliorations apportées à la BD 41
2.4.3 Conception de l'application 45
2.4.4 Identification des ED du troisième ordre 49
2.5 Développement 53
CHAPITRE 3 TESTS ET VALIDATIONS 61
3.1 Validation à l'interne du CRP 61
3.2 Validation auprès des partenaires 63
3.2.1 Identification de la problématique de sécurité 64
3.2.1.1 Connectivité Internet 65
3.2.1.2 Hébergement des serveurs 66
3.2.1.3 Gestion des accès et des informations 68
3.2.2 Recommandations des partenaires 69
3.2.3 Accessibilité versus sécurité 71
3.3 Cadre de partage d'information entre les IE 73
3.3.1 Modèle américain 75
3.3.2 Modèle australien 78
3.3.3 Modèle canadien 82
CHAPITRE 4 DISCUSSION 86
CONCLUSION 89

RÉFÉRENCES 92

ANNEXES 98

LISTE DES TABLEAUX

Tableau 1.1 - Indicateurs du niveau de fonctionnement des IE 6

Tableau 1.2 - Simulation des ED suivant une panne d'eau dans un secteur donné.....14

Tableau 2.1 - Spécifications techniques du serveur de l'application web DOMINO 57

Tableau 3.1 - Connectivités possibles pour DOMINO 65

Tableau 3.2 - Types d'hébergements possibles pour DOMINO 67

Tableau 3.3 - Échelle de sécurité *versus* accessibilité.....73

LISTE DES FIGURES

Figure 1.1 - Exemple de courbes de dépendances.....6

Figure 1.2 - Exemple de découpage en secteurs d'une zone géographique.....7

Figure 1.3 - Exemple de découpage en zones d'alimentation d'une zone géographique 8

Figure 1.4 - Exemple de courbe d'ED et de visualisation de la propagation d'un ED 9

Figure 1.5 - Rapports générés à la suite d'une analyse d'ED.....12

Figure 2.1 - *Entity Relationship Diagram* de la BD du prototype web DOMINO 34

Figure 2.2 - *Entity Relationship Diagram* de la BD du prototype Access de DOMINO.....42

Figure 2.3 - Diagramme du prototype web DOMINO.....46

Figure 2.4 - Courbes d'ED du premier ordre suite à une panne d'eau dans un secteur 51

Figure 2.5 - Courbes d'ED du deuxième ordre suite à une panne d'eau dans un secteur.....52

Figure 2.6 - Courbes d'ED du troisième ordre suite à une panne d'eau dans un secteur.....53

Figure 3.1 - Simulation d'un ED réalisée par DOMINO version Access 62

Figure 3.2 - Simulation d'un ED réalisée par DOMINO version web.....63

Figure 3.3 - Structure du *U.S. Department of Homeland Security*.....76

Figure 3.4 - Structure du *National Protection & Programs Directorate*.....77

Figure 3.5 - Organisations et divisions du *Infrastructure Protection* 78

Figure 3.6 - *Trusted Information Sharing Network* du gouvernement australien 80

Figure 3.7 - Composition du FNI 83

Figure 3.8 - Diagramme du plan d'action sur les IE 84

LISTE DES SIGLES ET ABRÉVIATIONS

AGD	Attorney General's Department
AMT	Agence Métropolitaine de Transport
ASP	Active Server Pages
BD	Base de Données
CSC	Centre de Sécurité Civile
CSS	Cascading Style Sheets
CI	Critical Infrastructure
CIIS	Complex Interdependent Integrated Systems
CIMS	Critical Infrastructure Modelling Simulation
CIPMA	Critical Infrastructure Protection Modelling and Analysis
CIR	Critical Infrastructure Resilience
CoI	Communities of Interest
CRP	Centre risque & perfomance
CRSNG	Conseil de Recherches en Sciences Naturelles et en Génie
CS&C	Cyber-Security and Communications
DCSC	Développement des Connaissances, Sensibilisation et Communication
DHS	Department of Homeland Security
DNS	Domain Name System
DRSCSI	Direction Régionale de la Sécurité Civile et de la Sécurité Incendie
EAG	Expert Advisory Groups
ED	Effet domino
ERD	Entity Relationship Diagram
FPS	Federal Protective Service

GPU	General Public License
Https	HyperText Transfer Protocol Secure
ID	Identifiant
IE	Infrastructure Essentielle
IICD	Infrastructure Information Collection Division
IIS	Internet Information Server
IP	Infrastructure Protection
MSP	Ministère de la Sécurité Publique
MTQ	Ministère des Transports du Québec
NATEC	Risques Naturels et Technologiques
NCCIC	National Cyber-security and Communications Integration Center
NCTC	Comité national de lutte contre le terrorisme
NPPD	National Protection and Programs Directorate
PCII	Protected Critical Infrastructure Information
PCRII	Programme Conjoint de Recherche sur les Interdépendances entre les Infrastructures
PHP	Hypertext Preprocessor
PSCD	Protective Security Coordination Division
RDC	Recherche et Développement Coopérative
SCADA	Supervisory Control And Data Acquisition
SGBDR	Système de Gestion de Bases de Données Relationnelles
SPC	Sécurité Publique Canada
SQL	Structured Query Language
TISN	Trusted Information Sharing Network
VPN	Virtual Private Network

LISTE DES ANNEXES

ANNEXE – INTERFACE DU SYSTÈME DOMINO WEB……...…….98

INTRODUCTION

Le fonctionnement normal d'une société industrialisée dépend grandement de la qualité des ressources et des services fournis par les Infrastructures Essentielles (IE). Aussi connues sous le nom d'infrastructures critiques, de systèmes essentiels ou de réseaux de support à la vie, les IE contribuent à la santé et au bien-être de la population en lui fournissant les ressources indispensables à ses activités quotidiennes telles que l'électricité, le gaz naturel, l'eau potable, les télécommunications, etc. Il est donc primordial que ces infrastructures fournissent un service fiable et sans interruption (*The President's Commission on Critical Infrastructure Protection* [PCCIP], 1997 ; Sécurité Publique Canada [SPC], 2004).

Au Canada, les IE sont regroupées en 10 secteurs : l'énergie et les services publics, les communications et technologies de l'information, la finance, les soins de santé, l'alimentation, l'eau, les transports, la sécurité, le gouvernement et la fabrication (Bureau de la Protection des Infrastructures Essentielles et de la Protection Civile [BPIEPC], 2003). Pour fonctionner adéquatement, ces infrastructures ont besoin l'une de l'autre. Par exemple, pour produire et distribuer de l'eau potable, le réseau d'eau a besoin d'électricité pour le fonctionnement de ses divers équipements. De manière analogue, le réseau d'électricité a besoin d'eau pour ses infrastructures pour la protection contre les incendies ou pour le refroidissement de certains équipements tels que les serveurs informatiques ou les appareils de climatisation. Il existe donc, au sein des IE, une forte interdépendance en raison des ressources qui sont échangées.

Les multiples liens entre les réseaux font en sorte que les IE forment pratiquement un grand système hautement complexe et enchevêtré d'éléments (infrastructures ou équipements) interreliés (Robert, Morabito & Debernard, 2012). Par conséquent, la défaillance d'un seul élément de ce système, soit une infrastructure ou un équipement, peut engendrer une réaction en cascade (ou en chaîne) communément appelé effet domino (ED). De nature parfois imprévisible, ces ED peuvent affecter, avec le temps, un grand nombre d'IE entraînant ainsi des conséquences de plus en plus importantes sur les activités socio-économiques, la population et l'environnement (Boin, Lagadec, Michel-Kerjan et Overdijk, 2003; Parfomak, 2005). Ces constatations expliquent

les investissements faits par les gouvernements dans les domaines de recherche liés à la protection des IE et à la mise en place de stratégies visant à accroître cette protection. Cela représente de nombreux défis et concerne à la fois les organisations publiques et les organisations privées qui en sont souvent propriétaires.

Plusieurs événements des dernières décennies ont été d'importants déclencheurs d'ED ayant eu des conséquences néfastes sur la population. L'un de ces événements est certainement la tempête de verglas qui a frappé le Québec en 1998. La tempête a causé d'importants dommages au réseau électrique entraînant des coupures de courant jusqu'à un mois et demi pour certains habitants. Cette défaillance du réseau électrique a eu des répercussions sur l'ensemble des autres réseaux, principalement le réseau d'eau potable (Nicolet, Trudeau, Denis, Bernier, Cloutier, Dicaire et al., 1999). L'enchaînement des défaillances qui ont résulté de cet événement démontrent la vulnérabilité de l'ensemble des IE face aux phénomènes d'ED.

Un autre exemple, plus récent cette fois, est sans doute l'épisode de l'ouragan Sandy ayant touché l'Amérique du Sud et les États-Unis en 2012. Fin octobre, l'ouragan Sandy frappe de plein fouet les Caraïbes ainsi que la côte Est et le Nord-est des États-Unis. L'ouragan a affecté directement des centaines de milliers de personnes et a généré des ED privant des milliers de personnes de ressources essentielles comme l'électricité, l'eau, les communications et les transports. Le coût des dégâts a été estimé à 65,6 milliards de dollars américains (Mufson, 2012 ; Barron et Goodman, 2012 ; Goldstein et Hauser, 2012 ; Serino, 2013).

D'autres exemples, tout aussi éloquents, tels que les pannes électriques en Ontario et aux États-Unis en 2003 (*Department of Energy* [DOE] et Ressources Naturelles Canada [RNC] 2004 ; SPC, 2006) et le tsunami de Fukushima au Japon en 2011 (Associated Press, 2011 ; Chossudovsky, 2012 ; Macchia 2012), font prendre conscience de l'importance de s'attarder aux IE et aux interdépendances entre elles et de développer de nouveaux outils dans le but de mieux anticiper les ED et leurs conséquences néfastes.

Les travaux du *Centre risque & performance* (CRP) de l'École Polytechnique de Montréal, s'inscrivent dans ce contexte. Ils ont permis le développement de DOMINO, un prototype d'outils qui permet d'anticiper les ED entre les IE. Or, ce prototype est actuellement disponible sur un seul poste de travail au CRP (dans ce document, on y référera par l'expression « DOMINO version Access »). Il est donc très peu accessible pour l'ensemble des partenaires du CRP. En contrepartie, le fait que ce prototype soit uniquement accessible par les personnes autorisées (trois personnes au CRP) fait en sorte qu'il est très sécuritaire et qu'il ne soulève pas de grandes questions relatives à la confidentialité des informations. L'objectif des travaux faisant l'objet de ce mémoire est de rendre DOMINO accessible aux partenaires du CRP par l'entremise du web. Concrètement, il s'agit de développer un prototype d'une plateforme web d'échange d'informations dédiée aux interdépendances entre les IE tout en tenant compte des contraintes liées à la confidentialité et à la sécurité des informations et de voir comment une telle plateforme pourrait être implémentée réellement dans une ou plusieurs municipalités. Dans ce document, on utilisera l'expression « DOMINO version web » pour désigner cette nouvelle version de l'outil.

Ce mémoire est divisé en quatre chapitres. Le premier chapitre présentera les travaux menés par le CRP pour en arriver au développement du prototype DOMINO version Access ainsi que certains modèles de partage d'information et d'outils dédiés aux IE. Le deuxième chapitre aborde la méthodologie utilisée pour parvenir au développement du prototype web : l'analyse des requis (autant les requis du CRP que ceux des partenaires). L'analyse fonctionnelle, la gestion des accès, la conception et le développement de la base de données (BD) et du prototype web seront détaillés dans ce chapitre. Le troisième chapitre porte sur la phase de tests et la validation qui suivra le développement du prototype. Ce chapitre aborde également les questions relatives à l'accessibilité et à la confidentialité des informations. Le dernier chapitre présentera quant à lui une discussion générale sur le sujet et présentera les différentes recommandations concernant les améliorations à apporter au système.

CHAPITRE 1 MISE EN CONTEXTE

Les travaux présentés dans ce mémoire ont débuté en 2012. Ils s'inscrivent dans la continuité d'une suite de projets menés par le CRP depuis 2005 concernant la modélisation des interdépendances entre les IE et le développement d'outils capables d'anticiper les ED. Deux projets principaux ont été réalisés par le CRP dans le passé. Le premier, de septembre 2005 à septembre 2008, visait le développement d'une méthodologie permettant l'identification et la caractérisation des interdépendances entre les IE. Le deuxième, initialement prévu de septembre 2008 à septembre 2012, a été reconduit pour une période de 1 an, soit jusqu'en septembre 2013, et visait le développement de DOMINO : un prototype d'outil permettant la modélisation spatio-temporelle des ED. Dans ce chapitre, il sera question de présenter brièvement les projets précédents réalisés par le CRP ainsi que les principales motivations ayant conduits au projet de maîtrise présenté dans ce document et de présenter différents modèles de partage d'information instauré par les gouvernements et d'outils dédiés aux IE.

1.1 Projets précédents

1.1.1 Subventions obtenues par le CRP

De 2005 à 2008, le CRP a obtenu deux subventions successives dans le but de développer une méthodologie de gestion des interdépendances entre les IE. La première de ces subventions a été obtenue dans le cadre du Programme Conjoint de Recherche sur les Interdépendances entre les Infrastructures (PCRII). Le projet visait le développement de la méthodologie (projet réalisé sur la ville de Montréal). La deuxième subvention a été obtenue dans le cadre du programme Développement des Connaissances, Sensibilisation et Communication (DCSC) d'Infrastructures Canada. Cette fois, le projet consistait à valider la méthodologie développée en l'appliquant sur une ville autre que celle où elle fut développée (projet réalisé sur la ville de Québec). Les travaux de recherche menés par le CRP dans le cadre de ces programmes de financement ont permis de développer une méthodologie relativement simple, mais très efficace, permettant d'identifier et de caractériser les interdépendances entre les IE et de comprendre les conséquences de leur défaillance en terme de propagation des ED. Appelée « Approche par conséquences », cette

méthodologie consiste à évaluer les conséquences potentielles de la dégradation d'une ressource sur le fonctionnement des IE qui utilisent cette ressource. Cette approche tire son originalité du fait qu'elle se concentre sur les conséquences de la défaillance des systèmes et non sur les causes ayant menées à cette défaillance (Robert, Morabito & Quenneville, 2007; Robert et Morabito, 2008 ; Robert et Morabito, 2010). De plus, cette méthodologie présente l'avantage de fournir des informations pertinentes pour la gestion d'une situation d'urgence en écartant toute notion de calculs probabilistes reliés à des aléas (Robert et Morabito, 2010).

Fort de ces résultats, le CRP a obtenu un nouveau financement de 2008 à 2012 dans le cadre du programme subvention de Recherche et Développement Coopérative (RDC) du Conseil de Recherches en Sciences Naturelles et en Génie du Canada (CRSNG). Reconduit pour une année supplémentaire (jusqu'en septembre 2013), le projet prévoit le développement d'un prototype d'outil permettant d'anticiper et de simuler les ED entre les IE suite à la panne d'une ressource dans une municipalité : DOMINO.

Parmi les quatre types d'interdépendances existants entre les IE (fonctionnelles, géographiques, cybernétiques et logiques (Rinaldi, Peerenboom et Kelly 2001 ; Robert et Morabito, 2008)), DOMINO n'aborde présentement que deux d'entre elles. Il s'agit des interdépendances fonctionnelles qui sont dues aux échanges de ressources entre les IE (relations de type clients/fournisseurs), et des interdépendances géographiques, qui sont dues à la proximité géographique des infrastructures. Les interdépendances cybernétiques (dues aux transferts d'informations entre les IE) et les interdépendances logiques (dues à des réalités conjoncturelles, politiques ou financières) ne sont pas prises en compte par DOMINO.

1.1.2 Courbes de dépendances et cartographie floue

Dans le but de visualiser comment la défaillance d'une ressource fournie par une infrastructure peut affecter les infrastructures qui utilisent cette ressource, le CRP a développé un code formé de quatre indicateurs de couleurs correspondant chacun à un niveau de conséquences (Tableau 1.1).

Tableau 1.1 - Indicateurs du niveau de fonctionnement des IE
(Robert & Morabito, 2008)

Indicateur	Couleur	Description
Vert		Le réseau fonctionne normalement avec les ressources qu'il utilise de manière courante ou sans l'apport d'une ou plusieurs ressources courantes.
Jaune		Le réseau utilise une ressource dégradée à l'une ou plusieurs de ses infrastructures et met en place des moyens ou des ressources alternatives pour compenser la dégradation de la ressource de sorte qu'on ne craint pas pour la mission du réseau (à court terme).
Orange		Le réseau utilise une ressource déficiente à l'une ou plusieurs de ses infrastructures. Les moyens palliatifs mis en place pour compenser la dégradation de la ressource ne sont pas suffisants de sorte que l'on craint pour la mission du réseau (à court terme).
Rouge		La mission du réseau est affectée à un endroit sur la zone d'étude. Une infrastructure d'une autre IE est privée de cette ressource.

En fonction de ces indicateurs, il a été possible de développer un premier outil pour exprimer l'évolution des conséquences sur les infrastructures privées d'une ressource en fonction du temps : les courbes de dépendances (Robert & Morabito, 2008). La figure 1.1 présente un exemple théorique de courbes de dépendances à la ressource « Eau » pour 5 réseaux différents.

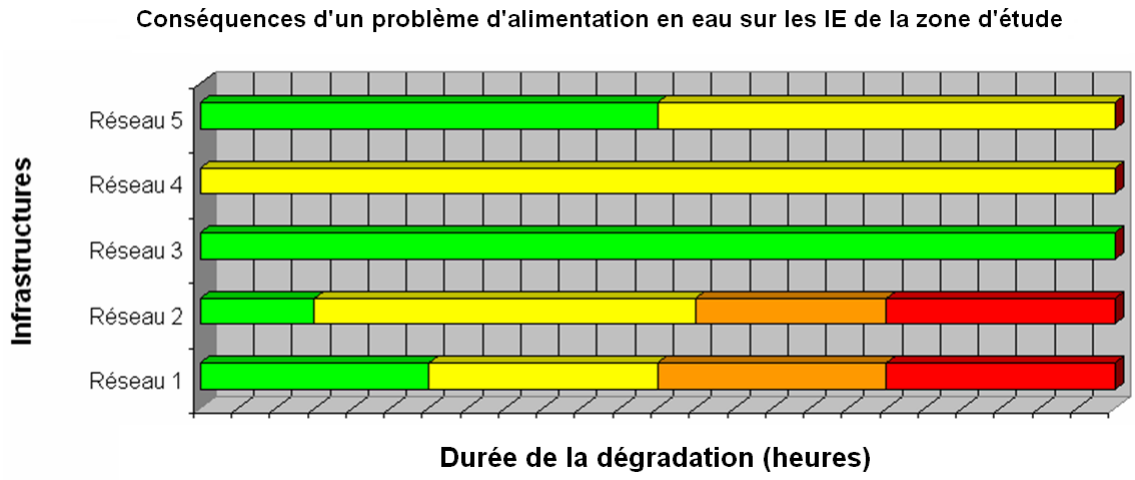


Figure 1.1 - Exemple de courbes de dépendances
(Robert & Morabito, 2008)

Sur cette figure, on remarque que les réseaux ne dépendent pas tous de la même manière de la ressource « Eau ». Ainsi, le réseau 3 n'est pas du tout affecté par la panne de la ressource, alors que les réseaux 4 et 5 le sont faiblement. Par contre, les réseaux 1 et 2 dépendent fortement la ressource « Eau », si bien qu'une panne de cette ressource peut compromettre la fourniture de leur propre ressource après seulement quelques heures.

Le deuxième outil développé par le CRP est la cartographie floue (ou souple). Cette cartographie consiste à diviser la zone d'étude de deux manières différentes. La première manière est une division de la zone d'étude en secteurs (Figure 1.2). Ces secteurs, dont la dimension peut varier selon le territoire d'étude, servent à localiser les infrastructures des réseaux. Selon le niveau de confidentialité que les responsables des différentes IE désirent conserver, la localisation d'une infrastructure peut se faire ponctuellement (par une adresse ou un point) ou en identifiant le secteur dans lequel l'infrastructure est située (Robert, de Calan & Morabito, 2008 ; Robert & Morabito, 2010).

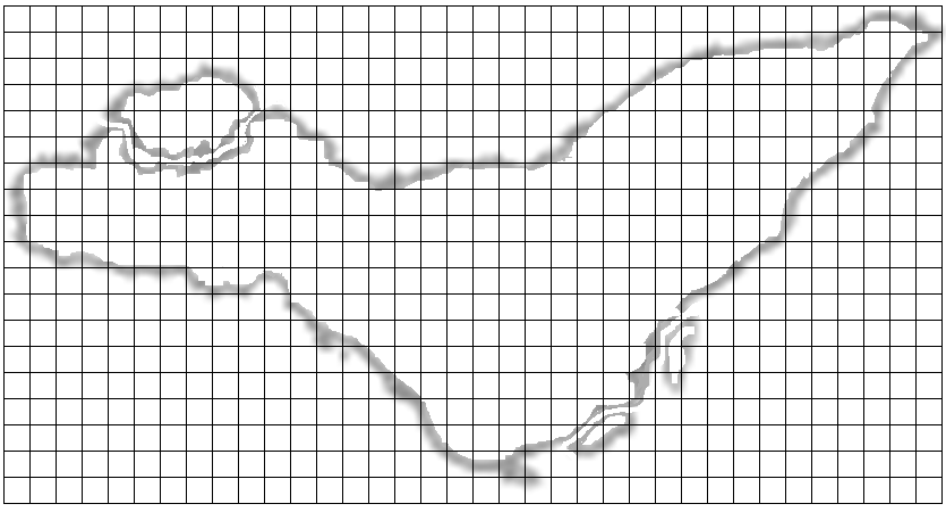


Figure 1.2 - Exemple de découpage en secteurs d'une zone géographique (Robert et Morabito, 2008)

La deuxième manière consiste à diviser la zone d'étude en plusieurs zones d'alimentation spécifiques aux IE (Figure 1.3). Ces zones correspondent aux zones alimentées en ressource par les différents éléments (équipements ou infrastructures) des IE et servent à connaître les zones

impactées par une panne de ressource après la défaillance d'un de ces éléments. Par exemple, pour le réseau électrique, ces zones peuvent être celles alimentées en électricité par les grandes centrales de production électrique ou par les postes de transformation ; pour le réseau de télécommunications, elles peuvent correspondre aux zones alimentées par les centraux téléphoniques ou par les tours cellulaires, etc. La détermination de ces zones est donc critique puisque ce sont elles qui permettent de déterminer les liens de dépendances entre les réseaux. Il incombe au responsable de chaque IE de préciser les zones d'alimentation de son réseau.

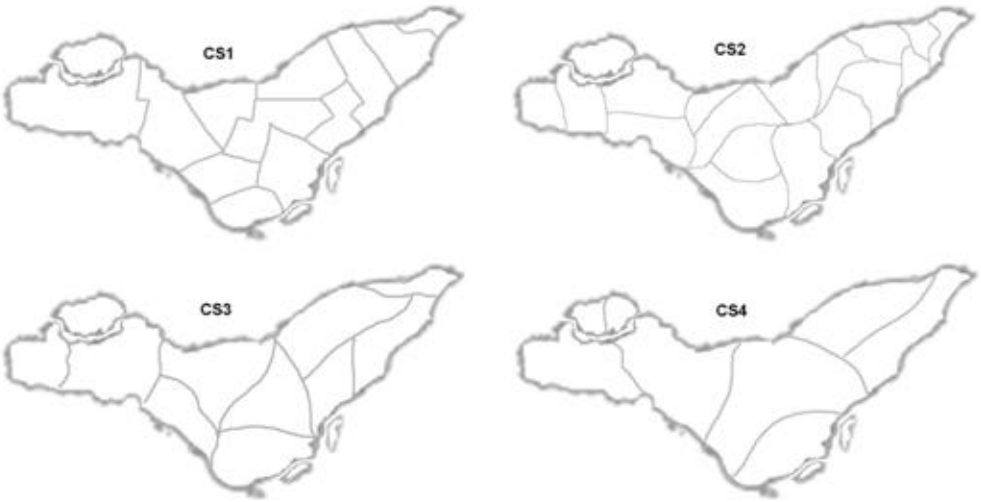
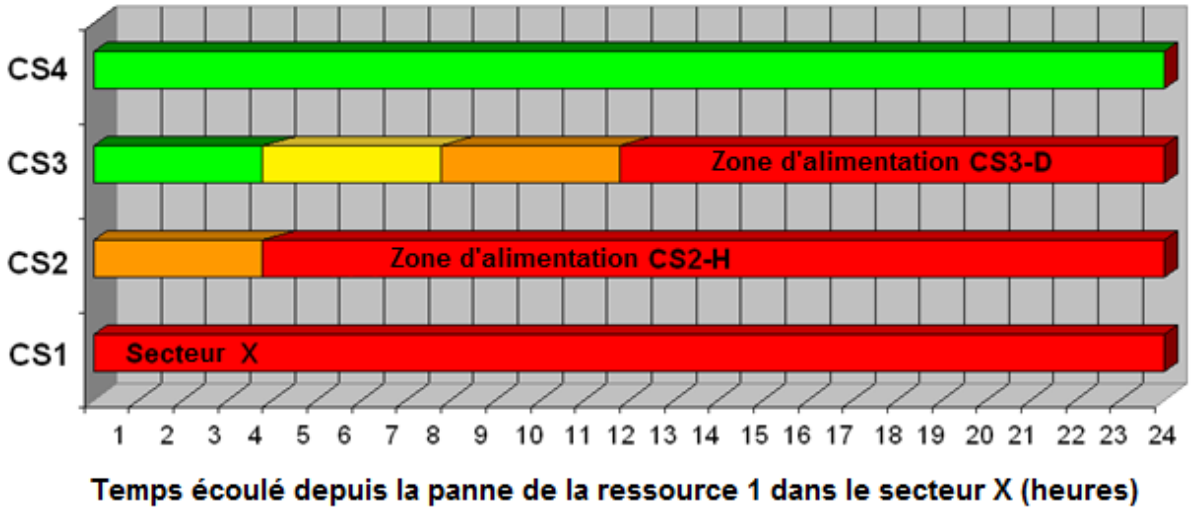


Figure 1.3 - Exemple de découpage en zones d'alimentation d'une zone géographique (Robert et Morabito, 2008)

La combinaison judicieuse des courbes de dépendances nous permet de tracer les courbes d'ED qui, associées à la cartographie floue (secteurs et zones d'alimentation) rendent possible la simulation de la propagation spatio-temporelle des ED déclenchés par la défaillance d'une ressource. La figure 1.4 illustre un exemple de courbe d'ED et de propagation spatio-temporelle associée à cette courbe.



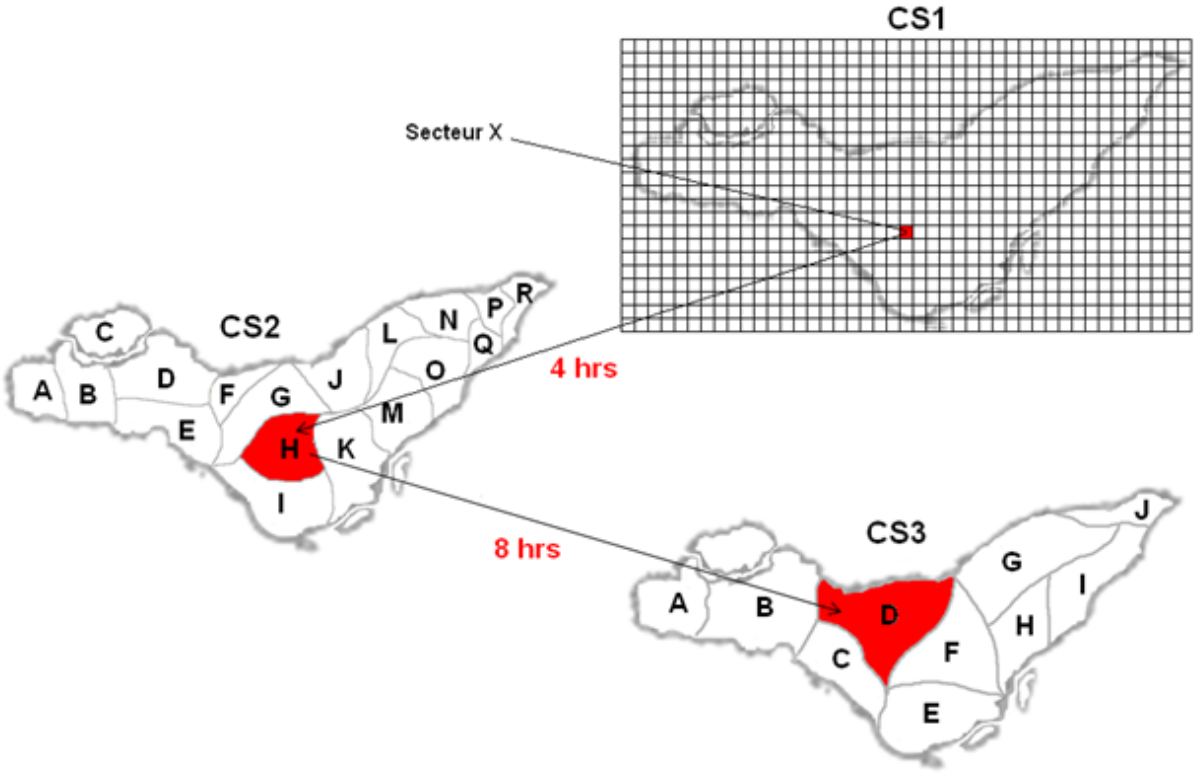


Figure 1.4 - Exemple de courbe d'ED et de visualisation de la propagation d'un ED (Robert et Morabito, 2012, Traduction libre)

Sur cette figure, on remarque que la panne de la ressource fournie par le réseau CS1 dans le secteur X de la zone d'étude à l'instant T_0 résulte en la panne de la ressource fournie par le réseau CS2 sur la zone d'alimentation H après 4 heures, qui à son tour engendre la panne de la ressource fournie par le réseau CS3 sur la zone d'alimentation D après 8 heures, soit 12 heures après la panne initiale de la ressource fournie par le réseau CS1.

1.1.3 DOMINO

Les outils présentés précédemment ont permis de développer le prototype DOMINO. Cet outil est constitué d'une BD (créée avec le logiciel Microsoft Access) qui contient l'ensemble des connaissances et des expertises concernant les interdépendances entre les IE. Un ensemble de requêtes permettent de combiner ces informations afin de déterminer les ED potentiellement générés par une panne de ressource dans un secteur. Cette BD est liée à un système d'information géographique ArcGIS[1]. Basé sur l'approche par conséquences développée par le CRP, l'outil fournit des informations pertinentes relatives à la propagation des ED très utiles pour les responsables des IE en situation d'urgence (Robert et al., 2007; Robert & Morabito, 2008, 2010). Les informations sont stockées dans différentes tables de la BD qui présente deux modules distincts : un module de données et un module d'analyse. Le module de données, réservé aux propriétaires des IE, leur permet de générer des rapports d'informations à propos de leurs propres infrastructures tels que les vulnérabilités connues par rapport aux interdépendances fonctionnelles et géographiques (dépendances face aux ressources utilisées, vulnérabilité face aux fuites d'eau, fuites de gaz naturel, etc.), les secteurs de la zone géographique où ils sont présents et où ils utilisent des ressources et certaines autres informations relatives à la dépendance des autres réseaux face à la ressource qu'eux-mêmes fournissent. Ces connaissances permettent aux propriétaires de réseaux d'évaluer la nécessité de mettre en place des mesures de prévention ou de protection afin de rendre leurs infrastructures moins vulnérables à la perte d'une ressource,

---

[1] ArcGIS d'Esri est un système d'information géographique (SIG) pour travailler sur des cartes et des informations géographiques. Il est utilisé pour créer et utiliser des cartes, compiler des données géographiques, analyser de l'information cartographique, gérer de l'information géographique dans une BD. http://www.esri.com/software/arcgis

selon que les conséquences sont jugées acceptables ou non. Ces informations sont très pertinentes, surtout en phase de prévention/planification. De plus, ces informations permettent d'identifier rapidement les infrastructures critiques affectées par une panne de ressource dans un secteur, de diffuser des messages d'alerte ciblés et de prioriser certaines activités de rétablissement. Donc, ces informations peuvent aussi être pertinentes en phase d'intervention/rétablissement. Pour assurer la confidentialité des informations, chaque IE possède un accès distinct et protégé qui lui permet d'accéder à ses informations.

Le second module de DOMINO est le module d'analyse qui permet au centre de sécurité civile (CSC) et au CRP d'exécuter des requêtes visant à analyser les dépendances entre les IE et à simuler les ED. Il faut bien noter que les niveaux de sécurité civile qui peuvent théoriquement s'y chevaucher sont : le niveau provincial présenté par le ministère de la sécurité publique (MSP), la direction régionale de la sécurité civile et de la sécurité incendie (DRSCSI) et le CSC de la ville de Montréal. Par contre, seuls les niveaux MSP et CSC sont concernés dans ces travaux. Le module répond au besoin de ces responsables en situation d'urgence, mais aussi en planification. En situation d'urgence, les responsables au CSC ont besoin de connaître dans les plus brefs délais l'évolution possible d'une situation afin de mettre en place les moyens nécessaires pour atténuer les conséquences néfastes potentielles. Ils veulent également être en mesure de pouvoir identifier rapidement les zones affectées et les éléments vulnérables qui y sont situés afin de pouvoir alerter les bonnes personnes. En situation de planification, les responsables du CSC ont besoin d'informations pertinentes leur permettant d'organiser des exercices de préparation, mais aussi pour faire de la prévention et de la sensibilisation (Robert et al., 2012). Les options programmées dans DOMINO pour les responsables du CSC ont donc été définies en tenant compte de ces besoins.

Pour la simulation des ED, DOMINO prend en entrée 2 paramètres : la ressource défaillante et le secteur où cette défaillance est observée. Pour préserver la confidentialité des données, l'outil ne fournit que le résultat de la requête ainsi que tous les éléments pertinents permettant une prise de décision éclairée en fonction de la situation simulée. La figure 1.5 présente un exemple de résultat d'une telle requête qui se décline en quatre rapports.

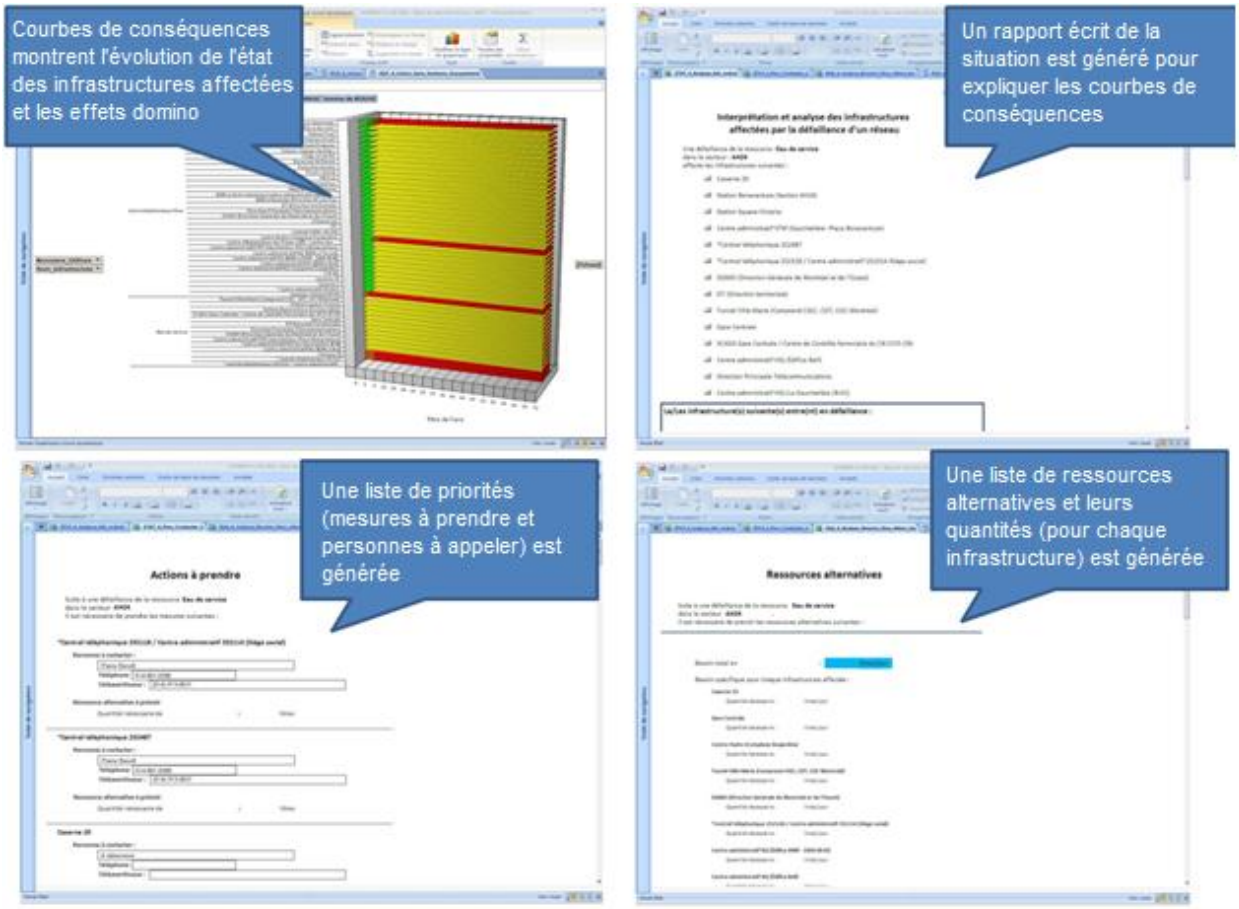


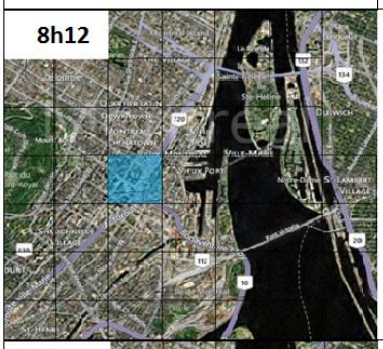
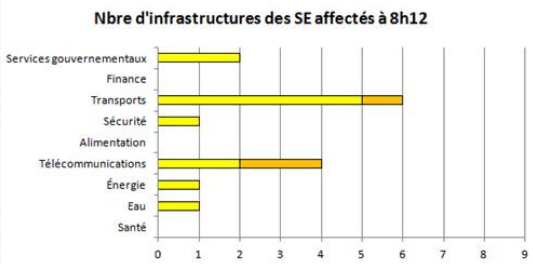
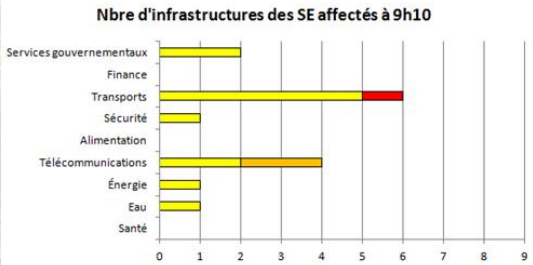
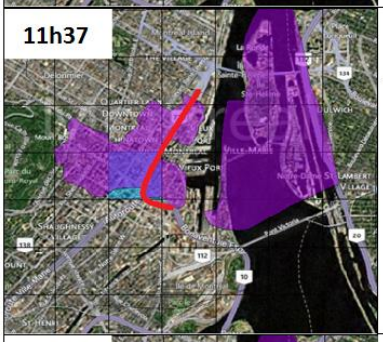
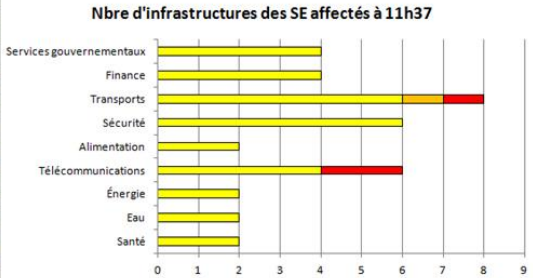
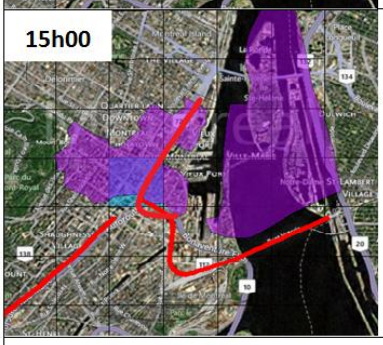
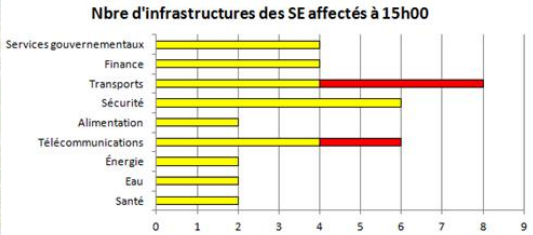
Figure 1.5 - Rapports générés à la suite d'une analyse d'ED
(Robert et al., 2012, Traduction libre)

Le premier rapport présente la courbe des ED potentiellement générés par cette panne selon les 5 indicateurs de couleurs préalablement définis. Ce rapport permet alors en un coup d'œil de savoir quelles infrastructures sont affectées par la panne, comment leur état évoluera en fonction du temps et de constater lesquelles de ces infrastructures tomberont possiblement en défaillance à l'intérieur des 72 heures. Pour des raisons techniques liées à la programmation des requêtes dans Access, la version bureau de DOMINO s'arrête aux ED d'ordre 2. Le deuxième rapport explique textuellement la courbe obtenue afin de laisser le moins de place possible à l'interprétation. Le troisième rapport consiste en une liste des actions prioritaires à poser. Cette liste inclus le nom des organisations et des personnes à contacter ainsi que toute autre action jugée pertinente pour la situation et qui auront été préalablement entrées dans le système par les gestionnaires des SE.

Cette liste permet alors de diffuser des messages d'alertes pertinents et clairs aux bonnes personnes et aux bons moments et de poser certaines actions prioritaires. Finalement, le dernier rapport concerne les ressources alternatives à prévoir. Ce dernier rapport permet aux gestionnaires du CSC de connaître les besoins en ressources alternatives pour chaque secteur de la zone d'étude pour éventuellement gérer et prioriser les approvisionnements en ressources alternatives advenant une pénurie de ces ressources.

Le résultat de la requête illustré sur la courbe de la figure 1.5 peut ensuite être simulé sur une carte géographique par l'intermédiaire du logiciel ArcGIS. Un curseur temporel permet aux utilisateurs de déplacer le curseur pour faire défiler le temps. Ceci permet d'illustrer la propagation dans le temps et sur la zone géographique des ED. Le tableau 1.2 représente le résultat d'une simulation générée par DOMINO version « bureau ».

Tableau 1.2 - Simulation des ED suivant une panne d'eau dans un secteur donné (Robert, Morabito & Cloutier 2012)

Simulation Domino	Identification des SE affectés	Notes
8h12 		• Interruption de l'alimentation en eau dans un secteur géographique donné (carré bleu). • 15 infrastructures affectées par la panne d'eau dont 3 ont un potentiel de défaillance à court terme.
9h10		• Défaillance d'une infrastructure d'un réseau de transport. • Perturbation du trafic routier.
11h37 		• Interruption de certains services de télécommunications. • Augmentation de la zone d'impact (couleur violet).
15h00 		**<u>État de la situation après 7 heures</u>** • Perte d'alimentation en eau. • Perturbation du trafic routier. • Perturbation des télécommunications. • Affectation de plusieurs réseaux de transport.

<u>Légende</u> : ○ Infrastructure perturbée - ○ Infrastructure perturbée avec un potentiel de défaillance - ● Infrastructure défaillante

Cette simulation illustre la propagation potentielle d'un ED due à la perte de la ressource « Eau » dans un secteur de la ville de Montréal. Dans cette table sont illustrées la carte associée aux zones impactées par la perte des différentes ressources, l'information concernant les infrastructures affectées par ces pannes et la description du résultat obtenu à chaque étape.

Ce genre de simulations permet aux responsables des IE d'avoir un aperçu des ED potentiels dans les premières heures qui suivent la panne d'une ressource dans un secteur de la ville. Par contre, il faut préciser que ce n'est pas certain que ces ED auront lieu. En effet, les conditions réelles (saison, période de la journée, autres circonstances aggravantes, etc.) peuvent affecter ces résultats ou les changer. Mais, au moins, les responsables des ED ont une idée de ce qui peut se passer et peuvent prioriser certaines tâches et actions à prendre comme se préparer à envoyer des messages de prévention aux autres organisations qui peuvent être affectées.

DOMINO se veut donc une forme de support permettant aux gestionnaires des IE de partager et mettre en commun de l'information pertinente dans le but d'en retirer des bénéfices certains concernant la réduction de leurs vulnérabilités par rapport aux ressources qu'elles utilisent, la planification et la préparation aux situations d'urgence et la mobilisation et l'alerte en situation d'intervention.

1.2 Problématiques

Deux problématiques entourent l'implémentation de DOMINO et son opérationnalisation. La première est purement technique et liée à l'outil lui-même. La seconde est liée au cadre mis de l'avant pour régir le partage d'information entre les IE. Les sections suivantes visent à expliciter davantage ces deux problématiques.

1.2.1 Problématique liée à l'outil

La problématique majeure qui entoure l'utilisation de DOMINO par les partenaires est son accessibilité. Tel qu'il l'a été mentionné plus tôt, DOMINO en est encore au stade de prototype. Il s'agit essentiellement d'un fichier de type Access qui est disponible sur un seul poste de travail au CRP. L'outil n'est donc pas directement accessible par les gestionnaires des IE. Lorsqu'un gestionnaire veut simuler une requête dans l'outil, il doit en faire la demande au CRP qui prend en charge de lancer la simulation et de retourner le résultat de cette simulation au gestionnaire qui en a fait la demande. Cette manière de procéder n'est pas optimale puisque l'outil n'est alors disponible que durant les heures de bureau. Donc, si un sinistre survient le soir ou la fin de semaine, les gestionnaires ne peuvent avoir accès à aucune information ou analyse que pourrait leur fournir l'outil. Installer un fichier DOMINO sur chacun des postes de travail des partenaires n'est pas une solution envisageable : la mise à jour des données serait beaucoup trop complexe et il n'y aurait aucune interaction entre les différents gestionnaires si bien qu'on perdrait l'essence-même de DOMINO qui est de mettre les réseaux en relation et les faire partager des informations. Une autre limitation de DOMINO version Access est le fait qu'il ne modélise que les 2 premiers ordres des ED. En fait, la complexité des requêtes permettant de simuler les ED d'ordre supérieur à 2 et les limitations induites par l'utilisation du logiciel Microsoft Access ne permettent pas de simuler les ED au-delà du second ordre. Ainsi, le prototype DOMINO n'est pas encore entièrement automatisé : certaines opérations sont encore réalisées « intellectuellement et manuellement » afin que l'outil puisse fournir des résultats complets qui incluent les ED de troisième ordre et les simulations cartographiques sur ArcGIS. L'outil ne peut pas être directement transféré aux partenaires puisque ceux-ci ne seront pas à même de produire des résultats d'ED tel que le fait le CRP.

1.2.2 Problématique liée au partage d'information

L'autre problématique entourant l'implémentation de DOMINO est liée au cadre régissant le partage d'information entre les IE. Il n'existe pas au Québec, ni même au Canada, à l'heure actuelle, un cadre bien précis régissant et encadrant le partage d'information entre les IE, si bien qu'il y a en quelque sorte un vide dans lequel les gestionnaires des IE se retrouvent lorsque vient le temps d'échanger de l'information entre elles ou avec les autorités gouvernementales. Tous s'entendent pour dire qu'il est impératif de partager de l'information dans le but de réduire la vulnérabilité des IE, mais le cadre formel pour le faire n'existant pas, la plupart du temps ces échanges se font sur une base volontaire et sur un principe de confiance mutuelle.

L'espace de coopération que le CRP a établi entre les différents partenaires repose précisément sur ce concept de confiance mutuelle. Il a permis de créer un processus de communication qui permet aux différentes entités de s'échanger des informations pertinentes qui les amène à mieux se préparer vis-à-vis des risques reliés aux interdépendances entre leurs réseaux sur une base volontaire. Lorsqu'un responsable de l'une des IE anticipe un dysfonctionnement de son réseau qui pourrait avoir des conséquences sur la fourniture de sa ressource, il peut aviser les utilisateurs de cette ressource pour les prévenir qu'une défaillance de la ressource en question pourrait les affecter. À partir de ces informations, les IE qui utilisent la ressource en question peuvent se préparer à intervenir (Robert et al., 2007). DOMINO permet cela. Néanmoins, amener DOMINO du stade du prototype au stade opérationnel demande un peu plus que du bon vouloir et de la confiance. Il demande en effet qu'un cadre plus formel de collaboration soit défini.

1.3 Projet actuel

Dans le contexte des limites mentionnées à la section précédente et suite à l'avancement des projets de recherche menés antérieurement par le CRP, la solution que le CRP propose pour rendre DOMINO accessible est de développer le prototype web de DOMINO et de proposer des pistes de solutions visant la définition d'un cadre pour le partage d'information confidentielles sur une plateforme web. Les travaux présentés dans ce mémoire porteront principalement sur ces deux objectifs.

1.3.1 Objectifs

Le choix d'une plateforme web pour faciliter l'accès à DOMINO va de soi. En effet, la principale raison qui motive ce choix est l'accessibilité. DOMINO web pourra être accessible de n'importe où, 24 heures par jour et 7 jours par semaine : l'Internet ne présentant pas les contraintes liées aux frontières géographiques, à la distance ou à la période de la journée. Cet avantage répond à une réalité concrète puisque les gestionnaires impliqués dans la gestion d'un sinistre sont, la plupart du temps, répartis sur le territoire (bien que des centres de coordination de mesures d'urgence puissent être ouverts dans certaines situations) et que les situations d'urgence peuvent se produire à n'importe quel moment. D'autres avantages justifient également ce choix. Premièrement, contrairement à une application bureau, une application web ne demande aucune installation au niveau des clients (les partenaires du CRP). Ceci élimine donc les problèmes engendrés par les licences, les vérifications des droits d'administrateur sur les postes de travail ainsi que tous les problèmes reliés à la mise à jour des données. La plupart des applications web sont beaucoup plus compatibles sur toutes les plateformes informatiques que les logiciels traditionnels installés. En général, le minimum requis sur les postes de travail est un navigateur web tels qu'Internet Explorer, Firefox et Netscape, pour ne citer que ceux-là. Ces navigateurs sont disponibles pour une multitude de systèmes d'exploitation, que ce soit Windows, Linux ou Mac OS, de sorte qu'il est toujours possible d'exécuter l'application web même sur des ordinateurs aux performances plutôt faibles ou ordinaires en autant qu'une connexion internet soit disponible. Ceci parce que l'application ne s'exécute pas localement sur les postes de travail, mais plutôt sur un serveur assez performant et dont la vitesse permettra de générer des résultats rapidement. La troisième raison d'utiliser une application web est la réduction du temps perdu à échanger des demandes de requêtes et des résultats de simulation entre les partenaires du CRP et le CRP lui-même. De plus, puisque les données seront centralisées dans un seul endroit, soit la BD sur laquelle est basée l'application web, les mises à jour seront beaucoup plus rapides et cohérentes et tous les utilisateurs auront accès aux informations les plus récentes : pas de problème lié aux versions obsolètes à devoir mettre à jour sur chacun des postes de travail tel qu'il incombe dans le cas des logiciels installés. Finalement, l'introduction de nouvelles fonctionnalités compatibles avec les

nouvelles applications mobiles comme notification d'alertes via courriel, réseaux sociaux, web-conférence, etc. sera plus facile dans le futur.

Donc, afin de répondre au besoin essentiel de rendre DOMINO accessible aux partenaires et en fonction des avantages reliés à l'utilisation d'une application web, le CRP propose de développer un prototype d'application web qui permettra un accès en tout temps à DOMINO. Cet outil offrira une interface d'aide à la décision aux intervenants impliqués dans les mesures d'urgence et permettra un accès en tout temps à DOMINO. Cette application permettra aux gestionnaires des différentes IE de se connecter à l'outil et de lancer des simulations à distance. Dans ce projet, uniquement deux types d'interdépendances seront considérées : les interdépendances fonctionnelles et géographiques. Évidemment, pour assurer la confidentialité des informations, l'accès à DOMINO sera strictement réservé aux personnes autorisées et sera modulé en fonction des utilisateurs.

Cette application permettra aux gestionnaires des différentes IE de se connecter à l'outil depuis leurs postes et de lancer des simulations à leur guise. De cette façon, le CRP pourra tester l'outil avec ses utilisateurs finaux, les partenaires, et voir leur interaction avec cet outil pour finalement implanter dans un prochain projet la première version de DOMINO web. De nouveaux modules concernant, par exemple, l'adaptation aux changements climatiques, les risques naturels et technologiques (NATEC), l'aménagement du territoire ou le développement durable, pourront lui être ajoutés dans le futurs. De plus, et dû à la limitation en temps de ce projet de maîtrise, la simulation sur une carte géographique ne sera pas abordée.

Afin de parvenir à atteindre cet objectif, 4 sous-objectifs spécifiques ont dû être formulés:

1. Apporter des améliorations à la BD développée sous Access pour la rendre plus dynamique, normalisée et optimisée ;
2. Développer le prototype DOMINO version web qui sera accessible aux partenaires du CRP ;
3. Préparer le système pour éventuellement y intégrer un volet cartographique et y ajouter des modules complémentaires ;

4. Tester et valider le système.

1.3.2 Résultats attendus

L'objectif principal de ce projet est le développement d'une plateforme web permettant le partage d'informations confidentielles reliées aux interdépendances entre les IE. Cet objectif se traduit concrètement par la création du prototype web de DOMINO qui devra être accessible à l'ensemble des partenaires du CRP et aux responsables du CSC de la ville de Montréal.

Pour atteindre l'objectif principal de ce projet, le projet sera divisé en deux phases principales et plusieurs sous-activités réparties sur une année et demie.

1. **Développement de l'application DOMINO web**
    1. Analyse des requis ;
    2. Analyse fonctionnelle ;
    3. Gestion des accès ;
    4. Conception de la BD ;
    5. Conception de l'application ;
    6. Développement.
2. **Tests et validation**
    1. Test et validation à l'interne des résultats ;
    2. Validation auprès des partenaires.

Le développement de l'application web de DOMINO reposera en grande partie sur les travaux qui ont mené au développement de la version bureau de DOMINO. Une adaptation devra être effectuée au niveau de la structure de la BD pour s'assurer qu'elle soit normalisée et optimisée en vue d'une application web. Cela inclut entre autre la transformation de la BD de sa version Access vers sa version MySQL. Aussi, des niveaux d'accès devront être définis pour les différents utilisateurs pour s'assurer de respecter les contraintes liées à la confidentialité des informations.

La validation du système sera faite sur la zone de la ville de Montréal. Ce choix est justifié par le fait que les données pour cette zone sont déjà disponibles au CRP et que les experts du CRP possèdent une très bonne connaissance des interdépendances sur cette zone géographique. La validation consistera donc à s'assurer que le prototype fournit les bons résultats de simulation. Cette validation sera faite en deux temps. D'abord, différentes simulations seront effectuées à l'interne par le CRP pour valider les résultats fournis par l'outil. Ensuite, une validation auprès des partenaires sera effectuée pour s'assurer que les paramètres liés à la gestion des accès qui auront été intégrés au système correspondent bien à leurs attentes en termes de confidentialité des informations et de sécurité des accès. Cette validation permettra aussi d'ouvrir les discussions sur la stratégie à élaborer pour l'implémentation future de DOMINO et ouvrira la discussion sur le cadre à mettre en place pour formaliser le partage d'information entre les IE.

1.3.3 Originalité des travaux

L'originalité de ces travaux découle du fait qu'il n'existe encore aucun outil en ligne qui modélise les interdépendances entre les IE utilisant des approches par conséquences (du moins, nous n'en n'avons recensé aucun dans la littérature) et qui permette aux gestionnaires des IE de partager de l'information sur les interdépendances en temps réel lors de sinistres. En fait, la plupart des systèmes existants sont des *Supervisory Control And Data Acquisition* (SCADA) utilisés par les IE pour contrôler leur propre réseau. Les SCADA permettent de collecter des informations provenant d'unités distantes et de contrôler et opérer ces unités à distance (Krutz, 2006). Ce ne sont donc pas réellement des outils qui permettent une gestion multi-organisationnelle des réseaux et de leurs interdépendances. Deux outils correspondent davantage à DOMINO. Il s'agit de l'outil *I2Sim* développé à l'Université de la Colombie-Britannique et de l'outil *Critical Infrastructure Modelling Simulation* (CIMS) développé par l'*Idaho National Laboratory* aux États-Unis.

I2Sim

Dans le but de partager des données entre les infrastructures privées et les institutions publiques, le groupe de recherche *Complex Interdependent Integrated Systems* (CIIS) de l'Université de la

Colombie-Britannique a élaboré un cadre d'intégration conceptuelle (appelé *I2Sim*) qui vise à aider les multiples opérateurs d'IE à mieux coordonner leurs efforts de planification, d'intervention et de rétablissement lors de grandes catastrophes. L'environnement de simulation fonctionne en temps réel en y intégrant des informations au fur et à mesure de l'évolution d'une situation. Théoriquement, le système permet de coordonner autant la réponse des couches physiques et humaines impliquées dans la réponse aux catastrophes. Des prototypes de l'environnement *I2Sim* ont été construits et sont actuellement opérationnels. Le campus principal de l'Université de la Colombie-Britannique a été utilisé comme un cas réaliste pour tester les concepts de modélisation et de l'environnement opérationnel. Le projet continue d'évoluer dans un certain nombre de directions. Parmi celles-ci, le développement d'un réseau intégré d'intervenants en cas de catastrophe à l'aide des technologies compatibles avec les réseaux, l'incorporation des facteurs psychologiques, anthropologiques et culturels dans la caractérisation des couches de l'homme au niveau des victimes et des intervenants et la promotion de l'intelligence artificielle et des bases de données distribuées pour fournir une aide "ciblée" (sans surcharge d'informations) aux intervenants et aux décideurs en cas de catastrophe (Marti et al., 2007). Un des inconvénients majeurs de cet outil est qu'il a d'abord été développé en laboratoire sans réellement tenir compte des contraintes liées à l'obtention de certaines données critiques de la part des grands opérateurs d'IE ce qui limite grandement son opérationnalisation.

***Critical Infrastructure Modelling Simulation* (CIMS)**

Une autre approche intéressante pour simuler les perturbations associées à la défaillance des IE a été développée par l'Idaho *National Laboratory* des États-Unis. Soutenu par l'American *Department of Energy* (DOE), le logiciel (développé en 2005) vise à fournir aux décideurs un outil d'aide à la décision concernant les menaces et les catastrophes naturelles. Il est important de mentionner que l'ouragan Katrina a été un important incitatif pour le développement de cet outil. Les principales caractéristiques de cet outil est qu'il dépeint visuellement l'interopérabilité de nombreuses infrastructures et qu'il offre la possibilité de créer des modèles à partir d'informations de type *open source*. Ainsi, il est possible, dans le cas d'un événement destructeur, de « capturer » la dynamique des effets en cascade engendrés par l'événement et la façon dont cela affecte les opérations des équipes d'urgence (Dudenhoeffer & Permann, 2006).

Contrairement à DOMINO, cet outil fonctionne à partir d'une approche causale souvent associée à un événement naturel de grande ampleur, si bien qu'on simule davantage les effets de la défaillance de l'ensemble des réseaux que les effets en cascades d'un réseau sur l'autre.

1.3.4 Contraintes

Le fait de rendre DOMINO accessible par le web engendre des contraintes qui, si elles ne sont pas correctement saisies, peuvent constituer un obstacle majeur à l'implémentation de DOMINO dans une municipalité.

En premier lieu, le fait qu'une application soit accessible par l'Internet demande obligatoirement de prendre en compte des critères de sécurité qui peuvent différer dépendamment du niveau de sécurité que l'administrateur désire avoir. En effet, une application web peut subir un acte de *hacking* (acte de malveillance) constitué d'un ensemble de techniques relevant de failles et de vulnérabilités d'un élément ou d'un groupe d'éléments matériels ou humains du système (*social engineering*) (Gomez-Urbina, 2007). Le *hacking* peut être appliqué par plusieurs techniques : attaque par force brute, dépassement de tampon (*stacks overflows* et *heap overflows*), écriture de code malveillant (*shellcode*), s*niffing*, *hijacking*, f*ingerprinting*, détournement et utilisation de données WEB (*cookies*, *Cascading Style Sheets* (CSS), vulnérabilités concernant les langages *Hypertext Preprocessor* (PHP), *Active Server Pages* (ASP), *Structured Query Language* (SQL), etc.); attaques réseaux qui regroupe le déni de service distribué, l'attaque de l'homme du milieu, l'*IP spoofing*, le *TCP session hijacking*, le *DNS spoofing*, le *DNS cache poisoning* (empoisonnement du cache DNS) et bien d'autres (Gomez-Urbina, 2007).

L'objet des travaux de ce mémoire n'est pas d'aborder toutes ces techniques de corruption des systèmes, mais plutôt d'aborder la question de la sécurité selon trois points de discussion qui devront être abordés avec les partenaires du CRP dans le but de définir un cadre de sécurité qui puisse convenir à l'ensemble de ces partenaires. Le premier de ces points de discussion est l'hébergement du serveur sur lequel va reposer l'application. Qui hébergera le serveur et, par le fait-même, l'application et les données est une question importante puisque la sécurité entourant

le serveur sera aussi garante de la sécurité de l'application. Le deuxième point de discussion concerne le type de lien à privilégier entre le serveur et les utilisateurs. Parmi les possibilités envisagés, accès entièrement libre (de type *Hypertext Transfer Protocol* (http)), accès sécurisé encrypté (*Hypertext Transfer Protocol Secure* (https)), accès complètement privé (de type *Virtual Private Network* (VPN)[2]), création d'un intranet multi-organisationnel, etc., les partenaires devront opter pour la solution qui soit la plus pratique possible compte tenu du niveau de sécurité souhaité. Finalement, le troisième de ces points de discussion concerne l'identité de l'administrateur du système. L'administrateur étant celui qui aura accès à l'ensemble des informations des organisations et à l'ensemble des fonctionnalités du système, incluant le code, il importe que le choix de l'identité de cet administrateur convienne à tous. Ces points de discussion seront abordés plus en détail dans le chapitre 3 de ce mémoire.

---

[2] Un réseau privé virtuel (VPN) s'étend à un réseau privé à travers un l'Internet. Il permet à un ordinateur d'envoyer et de recevoir des données à travers des réseaux partagés ou publics, comme s'il était directement connecté au réseau privé, tout en bénéficiant de la fonctionnalité, les politiques de sécurité et de gestion du réseau privé. Le canal est totalement encrypté.

CHAPITRE 2 DÉVELOPPEMENT DU PROTOTYPE WEB

La réalisation d'un prototype web demande de passer par quatre étapes : l'identification des requis du système, la conception du système (BD et application web), le développement du système (BD et application) et la phase de tests et de validation.

La première étape est l'identification des requis du système (besoins des utilisateurs et fonctionnalités du système). Cette étape sera réalisée par le CRP en collaboration avec ses partenaires. Elle est primordiale puisqu'elle vise à définir les besoins des clients et les fonctionnalités qui devront être intégrées à l'application. Essentiellement, le but est que le programmeur et le client s'entendent sur le produit final. Une analyse fonctionnelle suivra cette étape. Elle consistera à définir les fonctionnalités du système en termes de contenu, de conception visuelle, de requêtes à exécuter et de gestion des accès.

La deuxième étape est la conception du système. Celle-ci doit permettre de traduire visuellement les fonctionnalités et la structure du système. Il faut s'y référer continuellement au cours du développement et veiller à ce que rien ne soit oublié. Toute modification souhaitée devant être apportée au système doit être mentionnée à cette étape pour éviter les problèmes au moment de la programmation. Après avoir obtenu la confirmation finale du client relativement aux requis du système, il est possible de passer à la phase de programmation.

La troisième étape concerne le développement de la BD et du système. Il s'agit d'une étape technique de programmation qui se fera en utilisant les plateformes informatiques qui seront mentionnées plus tard dans ce chapitre. Puisqu'il s'agit d'une étape purement technique, elle ne sera pas largement abordée dans ce document.

La quatrième et dernière étape consiste en une phase de tests visant à valider le produit. Il s'agit d'une étape importante qui vise à vérifier que le système et la base de donnée forment un produit

fonctionnel et conforme aux requis du système étudié en premier lieu. Cette phase de tests sera accomplie d'abord à l'interne par les experts du CRP pour s'assurer que le système rencontre bien toutes les spécifications souhaitées et qu'il fournit les bons résultats puis par l'ensemble des partenaires pour valider que les contraintes liées aux accès et à la gestion de la confidentialité des informations ont bien été intégrée lors du développement du système. Cette dernière validation est importante puisque c'est seulement après avoir validé ces points que les discussions sur l'hébergement, le type de connexion souhaité et l'identité du gestionnaire de l'application pourront être abordées. Il faut également mentionner que tant pour ce prototype que pour le produit final envisagé dans les années prochaines, la phase de tests n'est jamais une phase qui possède une fin bien déterminée. Il faut bien distinguer la phase de tests qui doit être faite pour n'importe quelle application avant d'être implémentée et la phase maintenance qui suit le lancement de l'application et qui est normalement continuelle. Cette dernière vise à effectuer les mises à jour requises au niveau de l'application pour s'assurer que la version est toujours compatible avec l'avancement de la technologie et aussi au niveau des changements sociaux ou géographiques concernant les IE qui sont appelées à évoluer dans le temps. En effet, Antoniol *et al.* (2007) affirment que les systèmes logiciels, qui ont tendance à être grands et complexes, doivent être flexibles, dynamiques et capables d'évoluer avec les besoins des consommateurs. Ils doivent être construits d'une manière qui rend le changement le moins coûteux et le moins risqué possible puisque les changements imprévus et indisciplinés dans un système dégradent la qualité du logiciel et produisent des effets secondaires indésirables ou inattendus. Cette dernière étape sera abordée plus en détail au chapitre 3.

2.1 Analyse des requis

L'analyse des requis consiste à décomposer le grand livrable du prototype en étapes plus faciles à gérer. Il faut envisager les besoins des utilisateurs, ce qu'ils voudront accomplir dans le système et la procédure à suivre pour accomplir une tâche dans le système. Il faut aussi prendre en compte le contexte d'urgence dans lequel le système peut être utilisé. La structure doit être ciblée et claire.

Il est important de définir les fonctionnalités qui doivent être absolument implémentées dans l'application et de prioriser les tâches afin de favoriser une implémentation fluide du système. Le tout sans dédoubler le travail à effectuer et sans incohérences. À force de changer la structure plusieurs fois durant le développement on pourrait corrompre le système, ce qui n'est pas conseillé. Ensuite, il faut définir les nouvelles fonctionnalités qui devront être implémentées. Finalement, il faut préciser les fonctionnalités que l'on aimerait éventuellement (dans le futur) intégrer au système pour pouvoir développer la version courante d'une façon qui permette facilement leur implémentation au moment souhaité.

La liste finale des requis doit comprendre les fonctionnalités que le prototype devra avoir. Des sessions de *brainstorming* ont eu lieu à chaque semaine au sein du CRP pour discuter chaque idée, bonne ou mauvaise, faisable ou non. Les besoins des utilisateurs finaux, qui sont en fait les partenaires du CRP, ont été pris en compte lors de ces sessions.

La liste des requis finale est la suivante :

1. L'interface doit être simple et conviviale. Un outil trop compliqué pourrait être difficilement utilisable en situation d'urgence. Surtout étant donné le fait qu'il ne sera pas utilisé quotidiennement ;
2. L'outil doit être accessible par internet. Il doit donc être sécurisé afin d'éviter que n'importe qui puisse s'y connecter. Cela implique donc que les utilisateurs devront s'identifier par un mot de passe pour accéder à l'outil. La procédure pour demander un mot de passe prévoit que les utilisateurs envoient une requête par courriel au CRP qui fournira un nom d'usager ainsi qu'un mot de passe après avoir fait les vérifications qui s'imposent ;
3. Le CRP est le seul à détenir les droits de modification et de mise à jour des données dans le système (pour l'instant pour des raisons de sécurité afin d'éviter de compromettre la base de données) ;
4. Tous les utilisateurs enregistrés au système doivent avoir accès à l'analyse des ED mais les informations détaillées sur les infrastructures affectées par les ED ne doivent être disponibles que pour les réseaux propriétaires des infrastructures ;

5. L’administrateur doit pouvoir importer des données à la BD via des fichiers Excel ;
6. Les résultats des simulations doivent être accessibles à tous les partenaires selon le niveau d’accès autorisé à chaque utilisateur ;
7. L’interface devra être personnalisée en fonction de la session ouverte par l’utilisateur et du niveau d’accès permis spécifiquement à chaque utilisateur ;
8. Les résultats doivent être générés sous forme de rapports qui peuvent être imprimés et envoyés par courriel ;
9. Les rapports doivent être cohérents dans leur format et avoir une interface claire, organisée et optimisée en fonction de leur utilisation ;
10. Le système doit permettre le retour à une version antérieure de l’outil advenant une corruption des données et/ou de l’outil lui-même ;
11. Le système doit traiter les interdépendances fonctionnelles et géographiques et doit avoir une structure dynamique qui permet de changer, modifier ou ajouter d’autres modules (exemple : interdépendances logiques, interdépendances cybernétiques, Aléas naturels et technologiques, etc.) ;
12. Le système doit pouvoir simuler les ED d’ordre 3.

2.2 Analyse fonctionnelle

L’analyse fonctionnelle sert à déterminer les fonctions que devra permettre l’outil dans sa version web. Ces fonctions découlent à la fois de la liste des requis, mais également des requêtes actuellement disponibles dans DOMINO et qui correspondent à des informations que les utilisateurs veulent pouvoir être en mesure de générer à partir de l’outil.

Les fonctionnalités dans DOMINO doivent être divisées en quatre types différents :

- **Caractérisation floue des équipements** : accès limité aux propriétaires des réseaux pour valider leurs propres informations ;
- **Analyse des dépendances** : accès limité aux propriétaires des réseaux pour valider leurs propres informations et connaître leurs dépendances face aux ressources qu’ils utilisent ;

- **Analyse des ressources alternatives** : accès aux propriétaires des réseaux pour valider leurs propres informations et planifier leurs interventions ainsi qu'aux responsables du CSC pour gérer des pénuries éventuelles ;
- **Analyse des ED** : accès à l'ensemble des propriétaires des réseaux et aux responsables du CSC.

Voici les grandes fonctions que le système devra être en mesure de réaliser.

- Le système sera divisé en deux grandes sections : (1) les pages statiques qui contiennent des informations générales sur l'outil et le CRP et (2) l'outil lui-même ;
- Les utilisateurs autorisés détiennent un mot de passe pour ouvrir une session de l'outil ;
- Selon l'identifiant, le système ouvre une session correspondante au niveau d'accès autorisé à l'utilisateur ;
- Les interdépendances géographiques sont accessibles pour tous les niveaux d'accès.

Les informations sur les interdépendances fonctionnelles sont divisées en quatre catégories :

- **Informations sur les infrastructures** : informations sur les infrastructures localisées dans un secteur, celles appartenant à un réseau et celles des autres réseaux qui utilisent la ressource fournie par le réseau (dans un secteur ou une zone d'alimentation) ;
- **Informations sur les ressources** : informations sur les ressources utilisées par une infrastructure d'un réseau dans un secteur ainsi que la dépendance d'un réseau face à une ressource dans un secteur ou dans une zone d'alimentation ;
- **Analyse de dépendances et vulnérabilités** : informations sur la criticité des secteurs face à la panne d'une ressource ainsi que les analyse des besoins en ressources alternatives par secteur ou par zone d'alimentation ;
- **Analyse des ED :** informations sur la propagation spatio-temporelle des ED sous forme de courbes de conséquences et de rapports explicatifs de la situation anticipée.

Les informations sur les interdépendances géographiques sont divisées en deux catégories :

- **Criticité des secteurs face à un évènement donné :** informations sur la vulnérabilité des secteurs de la zone d'étude face à des événements tels que des fuites de gaz naturel, des inondations et des fuites d'eau ;
- **Infrastructures affectées par un évènement dans un secteur de la ville** : informations sur la vulnérabilité des infrastructures des réseaux face à des événements tels que des fuites de gaz naturel, des inondations et des fuites d'eau.

Deux autres modules figurent dans DOMINO, mais ne font pas partie de ce projet. Il s'agit du module sur les interdépendances logiques et celui sur les NATEC.

2.3 Gestion des accès

Une liste de critères concernant les accès a été préparée par le CRP en prenant en compte les contraintes de confidentialité exigées par les partenaires. Les critères établis sont les suivants :

1. L'accès aux différentes données est strictement réservés aux propriétaires de ces données ;
2. Le système doit prévoir un code de connexion unique composé d'un identifiant et d'un mot de passe pour chaque usager. Selon l'usager, le système permet des options différentes. Par exemple, deux usagers d'un même réseau pourraient ne pas avoir accès aux mêmes options (accès en mode gestionnaire, accès en mode utilisateur, etc.) ;
3. Le système doit permettre à un gestionnaire de réseau de donner une autorisation à une personne quelconque pour accéder en totalité ou en partie à ses informations (accès en mode invité). Cet accès peut être temporaire et révoqué en tout temps ;
4. Le CSC a accès uniquement aux analyses des données des réseaux, à moins qu'elle ait obtenue une autorisation particulière de la part d'un réseau (accès en mode invité) ;
5. Le CRP, en tant qu'administrateur, a accès à toutes les options et toutes les informations des réseaux.

Dans le but de rendre l'application plus dynamique et plus cohérente, les interfaces d'accès sont uniques aux différents utilisateurs et changent de contenu selon la session ouverte. Pour cette raison, il est nécessaire de catégoriser les utilisateurs en différents groupes ayant chacun un niveau d'accès prédéterminé à certaines fonctions de l'outil.

Les utilisateurs de l'outil sont divisés en 5 catégories. À chaque catégorie un niveau d'accès a été assigné :

- **Niveau 1** : accès absolu à toutes les fonctionnalités de DOMINO incluant le code source. Cet accès est octroyé seulement à l'administrateur du système puisque ce dernier est responsable de gérer la partie technique du système et de la BD ainsi que toutes les informations et données contenues dans la BD. Ce niveau est appelé « CRP Admin » ;
- **Niveau 2** : accès octroyé à l'équipe de recherche du CRP. Ce niveau permet l'accès général à l'ensemble des requêtes permises par l'outil sauf les privilèges liés à la modification des données et à l'accès au code de programmation du système (privilèges qui sont strictement réservés à l'administrateur). Ce niveau est appelé « CRP Équipe » ;
- **Niveau 3** : accès réservé aux gestionnaires des IE. Ce niveau permet l'accès à toutes les requêtes qui permettent à un réseau d'avoir de l'information sur son propre système comme les vulnérabilités des infrastructures et les dépendances face aux ressources utilisées. Ce niveau est appelé « Partenaires IE » ;
- **Niveau 4** : accès réservé aux personnes employées par une IE partenaire du CRP qui pourraient se voir accorder un accès temporaire au système (accès en mode invité). Il s'agit d'un accès de base qui peut être octroyé à une tierce personne à la demande d'un gestionnaire d'IE. Ce niveau est appelé « Partenaires public » ;
- **Niveau 5** : accès réservé aux responsables du CSC. Ce genre d'accès ne donne droit qu'aux requêtes permettant les analyses de dépendances et d'ED. Le CSC n'a donc pas accès directement aux données des réseaux, mais uniquement à une information pré-analysée en fonction d'une situation simulée.

2.4 Conception

La conception est une étape assez vague qui encapsule plusieurs aspects tels que la conception des études de cas, le diagramme de l'application, le modèle de la BD, les objets de programmation et tout autre aspect qui doit être représenté visuellement pour obtenir une meilleure idée de la manière dont tous les éléments du système seront intégrés. Normalement, c'est la conception de la BD et la conception de l'application qui sont faites pour toute application, qu'elle soit statique ou interactive.

2.4.1 Conception de la base de données

La conception de la BD débute une fois que l'analyse des requis, l'analyse fonctionnelle et la définition des niveaux des accès sont complétées. La conception est orientée objet. Cela signifie que chaque objet (ou entité) doit être défini individuellement et ensuite relié aux autres objets selon des relations bien spécifiques. Le résultat de cette conception est un digramme nommé *Entity Relationship Diagram* (ERD).

Entités

La première étape consiste à définir les entités en tenant compte de la vue générale désirée pour la structure de la BD. Chaque entité possède des attributs qui la décrivent. Une fois que toutes les entités sont définies, il faut établir les relations entre ces entités. Normalement, durant ce processus, de nouvelles entités sont créées dans le but d'optimiser et de normaliser la BD.

Relations

Les entités peuvent être reliées des trois façons suivantes :

- Un-à-un ;
- Un-à-plusieurs ;
- Plusieurs-à-plusieurs.

De manière générale, les entités qui sont reliées par des relations un-à-un dans les 2 directions sont combinées dans une seule table. Par contre, les relations plusieurs-à-plusieurs ne peuvent être représentées dans une BD. Pour cela, elles doivent être converties en des relations un-à-plusieurs. Plusieurs exemples illustreront ce point dans la description des tables qui viendra plus tard. Les relations un-à-plusieurs sont les plus répandues.

À la fin de cette étape, une représentation globale de la structure de la BD doit être faite pour raffiner les relations, résoudre les relations plusieurs-à-plusieurs et éliminer les relations redondantes. La figure 2.1 représente la structure de la BD de DOMINO (diagramme ERD). Les paragraphes qui suivent la figure décrivent l'ensemble des entités de la BD de DOMINO et les relations entre elles.

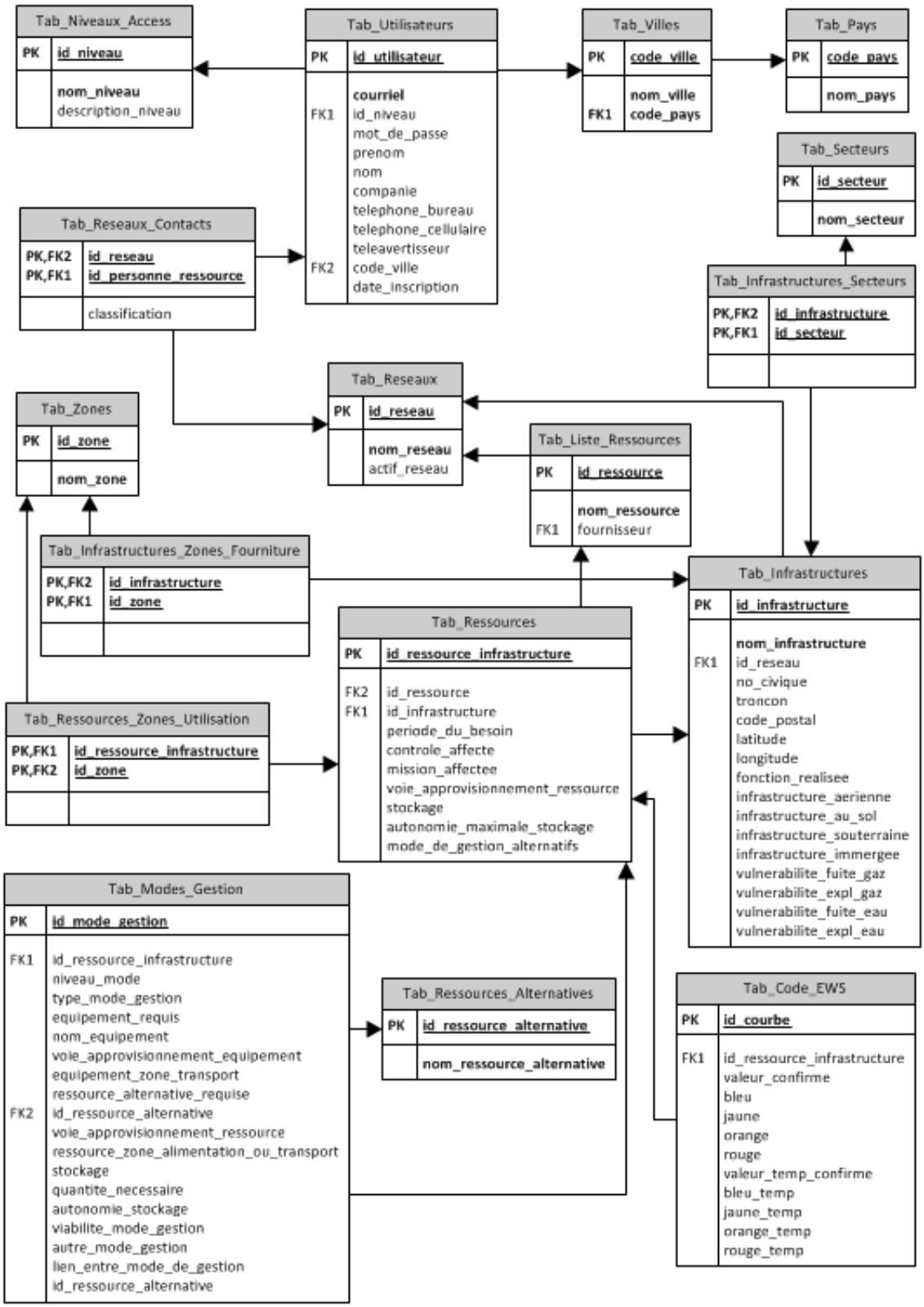


Figure 2.1 - *Entity Relationship Diagram* de la BD du prototype web DOMINO

Tab_Niveaux_Access est la table qui permet de stocker tous les niveaux d'accès que le système permet à ses utilisateurs. La clé primaire est id_niveau et elle se caractérise par un nom d'accès distinct pour chaque niveau et un descriptif du niveau (à titre informatif).

Tab_Utilisateurs est la table qui permet de stocker tous les utilisateurs qui ont accès au système. Chaque utilisateur est caractérisé par un identifiant (qui est la clé primaire) et un courriel (qui doit être unique). Donc, un même courriel ne peut être utilisé que par un seul utilisateur. Et, puisque chaque utilisateur possède un seul niveau d'accès (id_niveau) qui relie la table Tab_Utilisateurs à la table Tab_Niveaux_Access, chaque courriel associé à un utilisateur ne peut avoir qu'un seul niveau d'accès. Finalement, chaque utilisateur possède un mot de passe, un nom, un prénom, un nom d'organisation à laquelle il appartient, un numéro de téléphone au bureau, un numéro de cellulaire, un numéro de téléavertisseur, une ville (éventuellement l'outil pourra intégrer plusieurs municipalités) et une date d'inscription au système. À noter que certains champs peuvent demeurer vides au besoin.

La relation entre Tab_Utilisateurs et Tab_Niveaux_Access est du type un-à-plusieurs. En d'autres termes, un utilisateur ne peut avoir qu'un seul niveau d'accès, mais un niveau d'accès peut être assigné à plusieurs utilisateurs. Techniquement, cela signifie que le champ id_niveau de la table Tab_Utilisateurs est une clé étrangère.

Tab_Villes est la table qui permet de stocker les villes qui sont intégrées au système. Pour le moment, cette table ne contient que la ville de Montréal, mais d'autres villes pourront être intégrées au système dans le futur. Chaque ville est caractérisée par un code (qui correspond à la clé primaire), un nom unique et un code de pays.

La relation entre Tab_Utilisateurs et Tab_Villes est du type un-à-plusieurs. En d'autres termes, un utilisateur ne peut être assigné qu'à une seule ville, mais une ville peut être assignée à plusieurs utilisateurs.

Tab_Pays est la table qui permet de stocker les pays qui sont intégrés au système. Chaque pays est caractérisé par un code (qui correspond à la clé primaire) et un nom unique. Techniquement, cela signifie que le champ code_ville de la table Tab_Pays est une clé étrangère.

La relation entre Tab_Villes et Tab_Pays est du type un-à-plusieurs. En d'autre termes, une ville ne peut appartenir qu`à un seul pays, mais un pays peut avoir plusieurs villes. Donc le champ code_pays de la table Tab_Villes est une clé étrangère.

Tab_Reseaux est la table qui permet de stocker tous les réseaux qui sont partenaires du CRP. Chaque réseau est caractérisé par un id_niveau qui correspond à la clé primaire, un nom unique et un champ booléen appelé actif_reseau, qui est responsable de rendre le réseau actif s'il est à 1, et inactif s'il est à 0. Cet attribut sera utilisé dans certaines requêtes pour pouvoir filtrer les informations en éliminant les réseaux inactifs (donc qui ne veulent pas participer dans certaines analyses).

La relation entre Tab_Reseaux et Tab_Utilisateurs est une relation du type plusieurs-à-plusieurs. Cela signifie qu'un réseau peut avoir un ou plusieurs utilisateurs et qu'un utilisateur peut être associé à plusieurs réseaux. Puisqu'il s'agit ici d'une relation plusieurs-à-plusieurs, cette relation doit être ramenée à une relation du type un-à-plusieurs. Pour cela, la table Tab_Reseaux_Contacts a été créée.

Tab_Reseaux_Contacts est une table qui a été créée pour résoudre la relation plusieurs-à-plusieurs décrite précédemment. Dans ce cas, un id_utilisateur et un id_reseau sont associés pour former ensemble une clé primaire. Chacune de ces combinaisons est distinguée avec une classification qui permet d'assigner plusieurs personnes-ressources à un seul réseau ou la même personne-ressource à plusieurs réseaux distincts.

Tab_Infrastructures est la table qui permet de stocker les infrastructures des réseaux. Chaque infrastructure est caractérisée par un id_infrastructure qui est la clé primaire, un nom qui est unique, un id_reseau qui indique à quel réseau appartient l'infrastructure, d'autres informations relatives à la localisation de l'infrastructure (numéro civique, tronçon, code postal, latitude, longitude) et les fonctions réalisées par l'infrastructure. D'autres champs booléen permettent d'indiquer si l'infrastructure est aérienne, au sol, souterraine, immergée ou si l'infrastructure est vulnérable à une fuite/explosion de gaz naturel ou une fuite/explosion d'une conduite d'eau.

La relation entre Tab_Reseaux et Tab_Infrastructures est une relation du type un-à-plusieurs. Cela signifie qu'un réseau peut avoir une ou plusieurs infrastructures, mais une infrastructure ne peut appartenir qu'à un seul réseau. Donc, le champ id_reseau de la table Tab_Infrastructures est une clé étrangère.

Tab_Secteurs est la table qui permet de stocker tous les secteurs de la zone d'étude (de la municipalité). Chaque secteur est caractérisé par un identifiant id_secteur qui est la clé primaire et un nom qui est unique.

La relation entre Tab_Infrastructures et Tab_Secteurs est une relation plusieurs-à-plusieurs puisqu'une infrastructure pourrait s'étendre sur un ou plusieurs secteurs (concept de cartographie floue expliqué préalablement) et qu'un secteur peut contenir une ou plusieurs infrastructures. Pour résoudre cette relation du type plusieurs-à-plusieurs, la table Tab_Infrastructures_Secteurs a été créée.

Tab_Infrastructures_Secteurs est une table qui a été créée pour résoudre la relation du type plusieurs-à-plusieurs décrite précédemment. Dans cette table chaque infrastructure identifiée par l'id_infrastructure qui est une clé étrangère provenant de la table Tab_Infrastructures est associée à un secteur identifié par un id_secteur qui lui aussi est une clé étrangère provenant de la table Tab_Secteurs. Ce faisant, il est possible de localiser une infrastructure dans plusieurs secteurs et de localiser dans un seul secteur, plusieurs infrastructures différentes.

Tab_Liste_Ressources est la table qui permet de stocker les types de ressources. Chaque type de ressource est identifié par un id_ressource qui est la clé primaire, un nom unique et un fournisseur.

La relation entre Tab_Liste_Ressources et Tab_Reseaux est du type un-à-plusieurs. Un réseau peut fournir une ou plusieurs ressources. Une ressource ne peut être fournie que par un seul réseau. L'attribut fournisseur est une clé étrangère associée à l'identifiant des réseaux dans la table Tab_Reseaux. À noter que dans DOMINO, une ressource est interprétée comme étant une ressource fournie par un réseau (combinaison d'une ressource et d'un réseau), ainsi, deux ressources identiques fournies par deux réseaux différents sont en fait deux ressources différentes. Cela permet d'éviter qu'une même ressource puisse être fournie par deux réseaux différents ce qui induirait forcément des erreurs au moment d'analyser les dépendances entre les réseaux.

Tab_Ressources est la table qui permet de stocker les ressources utilisées par les infrastructures des réseaux. L'identifiant est id_ressource_infrastructure qui est relié à une ressource de la Tab_Liste_Ressources par le champ id_ressource et à une infrastructure de la table Tab_Infrastructures par le champ id_infrastructure. Chaque ressource est caractérisée par une série de sept paramètres qui permettent de connaître le niveau de dépendance de l'infrastructure par rapport aux ressources qu'elles utilisent.

La relation entre Tab_Ressources et Tab_Infrastructures en est une du type un-à-plusieurs. Autrement dit, une infrastructure peut utiliser plusieurs ressources différentes. Donc, le champ id_infrastructure de la table Tab_Ressources est une clé étrangère. De plus, la relation entre Tab_Ressources et Tab_Liste_Ressources en est aussi une du type un-à-plusieurs. Chaque ressource de la table Tab_Liste_Ressources est associée à une ou plusieurs ressources utilisées, Donc, le champ id_ressource de la table Tab_Ressources est également une clé étrangère.

Tab_Zones est la table qui contient toutes les zones d'alimentation des réseaux. Chacune est identifiée par un identifiant id_zone (qui est la clé primaire) et un nom unique.

La relation entre Tab_Zones et Tab_Ressources_Infrastructures est du type plusieurs-à-plusieurs puisque chaque ressource peut être utilisée dans une ou plusieurs zones, et chaque zone peut constituer la zone d'utilisation d'une ou plusieurs ressources. Pour résoudre cette relation, la table Tab_Ressources_Zones_Utilisation a été créée.

Tab_Ressources_Zones_Utilisation est une table qui a été créée pour résoudre la relation plusieurs-à-plusieurs décrite précédemment. Cette table contient un identifiant id_ressource_infrastructure provenant de la table Tab_Ressources et un identifiant id_zone provenant de la table Tab_Zones. Ces deux identifiants sont les clés étrangères. Ensemble, ils constituent une clé primaire. De cette façon, la relation du type plusieurs-à-plusieurs est ramenée à deux relations du type un-à-plusieurs.

La relation entre Tab_Zones et Tab_Infrastructures est aussi du type plusieurs-à-plusieurs puisque chaque infrastructure peut avoir une ou plusieurs zones d'alimentation (ou fourniture), et chaque zone peut constituer la zone d'alimentation d'une ou plusieurs infrastructures. Pour résoudre cette relation, la table Tab_Infrastructures_Zones_Fourniture a été créée.

Tab_Infrastructures_Zones_Fourniture est une table qui a été créée pour résoudre la relation plusieurs-à-plusieurs décrite précédemment. Cette table contient un identifiant id_infrastructure provenant de la table Tab_Infrastructures et un identifiant id_zone provenant de la table Tab_Zones. Ces deux identifiants sont les clés étrangères. Ensemble, ils constituent une clé primaire. De cette façon, la relation plusieurs-à-plusieurs est ramenée à deux relations du type un-à-plusieurs.

Ces deux tables Tab_Ressources_Zones_Utilisation et Tab_Infrastructures_Zones_Fourniture permette alors à une même zone d'être à la fois une zone d'utilisation de ressource et une zone de fourniture de ressource. En effet, une ressource est fournie par une infrastructure d'un réseau sur une zone d'alimentation et est utilisée par les infrastructures des autres réseaux sur cette même zone d'alimentation (que l'on nomme alors zone d'utilisation pour éliminer toute ambiguïté possible).

Tab_Ressources_Alternatives est la table qui contient toutes les ressources alternatives qui peuvent être utilisées par les infrastructures des réseaux. Chacune est caractérisée par un identifiant id_ressource_alternative (qui est la clé primaire) et d'un nom unique.

Tab_Modes_Gestion est la table qui permet de stocker les modes de gestion (ressources alternatives) utilisées par chacune des infrastructures des réseaux. Cette table fait la description des modes de gestion de chaque ressource associée à une infrastructure. Chaque mode de gestion est identifié par un id_mode_gestion (qui est la clé primaire) et possède une série d'attributs qui permettent de caractériser le mode de gestion comme les équipements requis s'il y a lieu, la voie d'approvisionnement de ces équipements, les ressources alternatives requises pour le fonctionnement de ces équipements, etc.

La relation entre Tab_Modes_Gestion et Tab_Ressources est du type un-à-plusieurs. Donc, pour chaque ressource utilisée par une infrastructure, plusieurs modes de gestion peuvent être assignés. Par exemple, advenant une panne électrique, une infrastructure pourrait avoir un premier mode de gestion correspondant à des batteries et un deuxième mode de gestion correspondant à des génératrices. Donc le champ id_ressource de la table Tab_Modes_Gestion est une clé étrangère qui associe Tab_Modes_Gestion à Tab_Ressources. La relation entre Tab_Modes_Gestion et Tab_Ressources_Alternatives est aussi du type un-à-plusieurs puisqu'une même ressource alternative peut être utilisée par un ou plusieurs modes de gestion.

Tab_Code_EWS est la table qui contient les codes *Early Warning System* (EWS) pour chaque ressource utilisée. Ce code permet de traduire la dépendance d'une infrastructure à une ressource sous la forme de courbe de dépendance selon le code de couleurs expliqué au chapitre 1. L'identifiant de cette table est id_courbe (qui est la clé primaire) et la clé étrangère est id_ressource_infrastructure.

La clé étrangère id_ressource_infrastructure de la table Tab_Modes_Gestion est une clé unique. Donc, la relation entre Tab_Ressources_Infrastructures et Tab_Code_EWS est du type un-à-un : chaque ressource utilisée par une infrastructure possède une seule courbe de dépendance. Ainsi, si une infrastructure d'un réseau utilise trois ressources différentes, alors il y aura, pour cette infrastructure, trois courbes de dépendances (une par ressource utilisée).

2.4.2 Améliorations apportées à la BD

Le but de la nouvelle structure de la BD est d'apporter des améliorations au niveau de l'optimisation de la BD elle-même et des requêtes. La structure de la BD de DOMINO version bureau était constituée de cinq tables seulement (Figure 2.2).

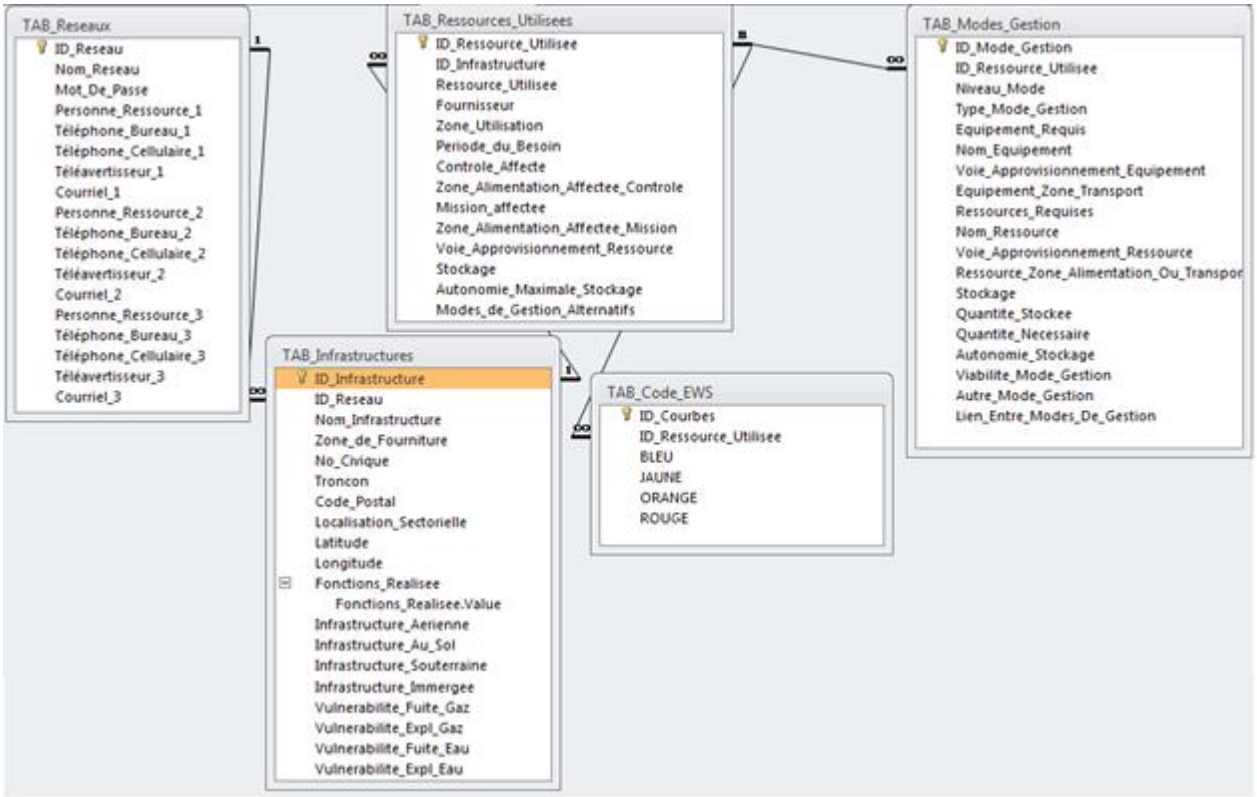


Figure 2.2 - *Entity Relationship Diagram* de la BD du prototype Access de DOMINO

La première table (TAB_Reseaux) englobait plusieurs informations dont le nom du réseau, un mot de passe unique pour l'ensemble des personnes-ressources d'un même réseau ainsi que les coordonnées de ces personnes. La nouvelle version, comme il a été montré dans la section précédente, est beaucoup plus complexe et permet, entre autre, d'assigner des mots de passe différents aux personnes-ressources d'un même réseau tout en gérant les informations auxquelles chacune de ces personnes ont accès en leur assignant individuellement un niveau d'accès qui peut être différent. Dans la structure de DOMINO web, chaque utilisateur a un identifiant qui l'associe à un niveau d'accès différent des autres même au sein de la même organisation. De plus, ces utilisateurs sont séparés de la table des réseaux pour éviter la duplication et les champs multiples dans une même ligne. Par exemple, si on prend le cas du nombre de personnes-ressources. Certains réseaux possèdent une seule personne-ressource alors que d'autres en possèdent trois. Ainsi, plutôt que de mettre ces informations en tant qu'attributs dans une même table qui comporterait alors trois colonnes dont certaines demeureraient vides pour les réseaux n'ayant qu'une ou deux personnes-ressources, il est préférable de déplacer ces informations dans une

nouvelle table qui aura alors l'identifiant du réseau et comme autre attribut une personne-ressource. De cette façon, un réseau qui n'aurait qu'une seule personne-ressource aurait une ligne de données dans la table correspondante aux personnes-ressources, alors qu'un réseau qui aurait trois personnes-ressources aurait trois lignes de données dans la même table.

La deuxième table est celle des infrastructures (TAB_Infrastructures) qui englobait les infrastructures des réseaux avec leurs zones de fourniture, leur localisation sectorielle et les informations propre à chacune d'elles. Le principal inconvénient de cette structure est qu'il n'était pas possible de localiser une infrastructure d'un réseau sur plusieurs secteurs. Il fallait donc dupliquer (voir quadrupler) l'information dans la base de données lorsqu'une même infrastructure se trouvait à la frontière entre deux ou quatre secteurs.

La table des ressources utilisées (TAB_Ressources_Utilisees) englobait quant à elle toutes les ressources utilisées par toutes les infrastructures des réseaux. Bien qu'elle ne présentait pas d'inconvénients majeurs, cette table était extrêmement grande et donc très « lourde » à gérer, surtout avec la multiplication des informations reliées aux problèmes soulevé précédemment et relié à la localisation d'une même infrastructure sur plusieurs secteurs. La nouvelle structure est beaucoup plus « légère » puisque les ressources alternatives sont listées une seule fois dans la table et un lien est fait chaque fois vers la nouvelle table qui contient les paramètres spécifiques à l'utilisation des ressources par chaque infrastructure des réseaux.

La table des modes de gestion (TAB_Modes_Gestion) englobait l'ensemble des informations sur les ressources alternatives utilisées par les infrastructures des réseaux. Puisqu'elle n'était pas dynamique, cette table ne pouvait contenir que trois modes de gestion différents pour chaque ressource utilisée par une infrastructure. Aussi, puisque toutes les informations de tous les modes de gestion de toutes les infrastructures se retrouvait dans cette table, celle-ci était aussi très grande (trois fois plus grande que la table des ressources utilisées puisque pour chaque ressource utilisée, jusqu'à trois modes de gestion différents pouvait être définis).

Finalement, la table contenant les codes EWS (TAB_Codes_EWS) ne présentait pas d'inconvénients majeurs si ce n'est qu'elle dupliquait les informations reliées aux infrastructures localisées sur plus d'un secteur.

Parmi les autres améliorations effectuées, notons que le fait de séparer les zones d'alimentation des tables Tab_Infrastructures et Tab_Ressources présente le grand avantage de centraliser les informations sur les zones dans une même table et d'éviter les erreurs possibles dans les entrées. Dans la version Access de DOMINO, le nom des zones d'utilisation et de fourniture des ressources était entré manuellement à chaque fois (pour chaque ressource utilisée et fournie). Ainsi, une erreur de frappe pouvait faire en sorte qu'une même zone soit interprétée comme deux zones complètement distinctes par le système. Par exemple, une zone nommée « zone de centre-ville » dans la table des infrastructures, et présente dans la table des ressources sous le nom « zone du centre-ville », serait considérée dans une requête comme deux zones différentes et ainsi engendrer des erreurs dans les analyses produites par l'outil. En ayant une seule table avec le nom des zones (*idem* pour les secteurs) écrit une seule fois, on évite ce genre d'erreur, en plus de normaliser davantage la BD. Cette façon de faire donnera également la possibilité d'ajouter des zones d'alimentation ou des secteurs, même si on n'y retrouve aucune infrastructure des autres réseaux à l'intérieur.

En ce qui concerne les requêtes, plusieurs changements ont dû être effectués pour tenir compte de la nouvelle structure de la BD. Aussi, quelques requêtes ont été nouvellement créées pour satisfaire les besoins des partenaires et d'autres ont été optimisées pour fournir des résultats plus efficaces, plus rapides et plus précis. En outre, la possibilité de générer les ED d'ordre 3 est sans aucun doute une avancée majeure par rapport à la version Access de DOMINO. Cette requête est en fait une suite de requêtes que le système prépare et renvoie à la BD dans une seule connexion pour retourner les résultats des ED de 1er, 2e et 3e ordre. Cela évite les accès multiples à la BD qui induisent des délais supplémentaires dans la réponse du système.

La nouvelle structure de DOMINO présente donc des améliorations substantielles par rapport à sa version Access. Il faut toutefois faire remarquer que plusieurs travaux ont dû être réalisés pour en

arriver à une structure de la BD qui soit plus normalisée et plus optimale. La normalisation est un processus important dont le but est de réduire le nombre d'informations dupliquées dans une table.

2.4.3 Conception de l'application

La conception de l'application consiste à créer un plan sur lequel on indique toutes les pages accessibles par un utilisateur, quel que soit le niveau d'accès. Durant cette conception, on trouve des façons d'optimiser davantage les fonctionnalités, d'en combiner quelques-unes ou d'en diviser d'autres. La conception permet de donner un meilleur aperçu du produit final et réduit les risques de devoir apporter de trop grands changements lors de la phase de programmation (en raison d'éléments auxquels on aurait porté une attention insuffisante). Plusieurs versions ont été nécessaires à cette étape pour finalement en arriver à la version finale confirmée dont le diagramme est représenté à la figure 2.3.

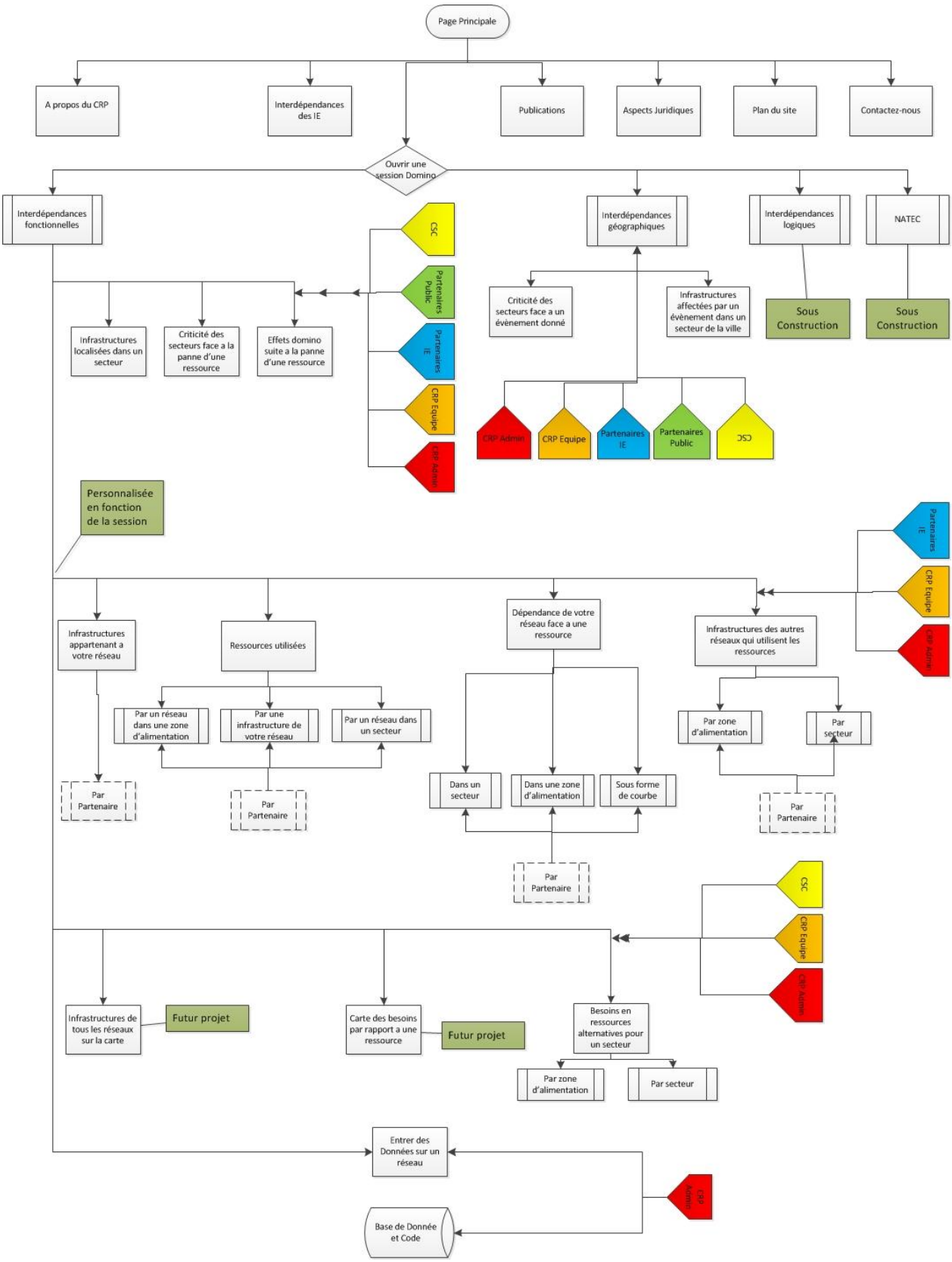


Figure 2.3 - Diagramme du prototype web DOMINO

Dans le diagramme illustré à la figure 2.3, toutes les sections du système sont représentées, incluant les pages statiques, les fonctionnalités, les sous-sections, les accès et les commentaires pertinents s'il y a lieu.

Le premier accès à l'application sera la page d'accueil, soit la page principale. De cette page, l'utilisateur pourra consulter les pages statiques qui contiennent des informations à propos du CRP, des interdépendances entre les IE, les publications du centre de recherche, les aspects juridiques reliés à l'utilisation de l'outil et d'autres informations connexes. C'est aussi à partir de cette page qu'un usager pourra ouvrir une session DOMINO en entrant son courriel et son mot de passe spécifique.

Une fois l'utilisateur identifié et authentifié, la session sera personnalisée en se basant sur le niveau d'accès préalablement autorisé à cet usager. Le contenu de l'application est présentement divisé en 4 modules principaux : les interdépendances fonctionnelles, les interdépendances géographiques, les interdépendances logiques et les risques naturels et technologiques (NATEC). Tel qu'il l'a déjà été mentionné, les deux derniers modules ne faisaient pas partie des travaux effectués dans le cadre de ce projet.

Pour les interdépendances géographiques, les informations sont communes à l'ensemble des réseaux. Elles ne seront donc pas plus largement expliquées dans la suite de ce projet puisqu'elles ne présentent pas un grand intérêt : il ne s'agit que de requêtes simples qui permettent d'afficher directement les informations contenues dans les différentes tables de la BD sous la forme de rapports. Les travaux futurs du CRP dans le domaine des interdépendances géographiques pourront venir s'intégrer dans cette section.

Pour les interdépendances fonctionnelles, les fonctionnalités sont principalement divisées en 4 catégories : les informations sur les infrastructures, les informations sur les ressources utilisées, les informations sur les analyses de dépendances et les informations sur les analyses des ED.

Chaque catégorie comporte plusieurs fonctionnalités qui varient selon le niveau d'accès autorisé à l'usager.

Dans le diagramme de la figure 2.3 illustrée précédemment, l'administrateur du CRP (niveau d'accès indiqué par la couleur rouge) a accès à toutes les fonctionnalités de l'outil ainsi qu'au code de l'application et à la BD. Les autres membres du CRP (niveau d'accès indiqué en orange) ont accès aux mêmes fonctionnalités que l'administrateur, mais non pas accès au code de l'application et à la BD. Les autres membres du CRP (associés de recherche, étudiants, stagiaires, etc.) ont un accès qui peut être modulé en fonction des recherches sur lesquelles chacun d'eux est appelé à travailler. Ainsi, un stagiaire qui n'effectuerait qu'un stage d'été de deux mois pourrait se voir accordé uniquement un accès limité comme celui réservé aux responsables du centre de sécurité civile (CSC).

L'accès des « partenaires des IE » (niveau 3), des « partenaires public » (niveau 4) et du CSC (niveau 5) est limité à des fonctionnalités bien spécifiques. Les fonctionnalités telles que les infrastructures localisées dans un secteur, la criticité des secteurs face à la panne d'une ressource et la simulation des ED suite à la panne d'une ressource sont des fonctionnalités qui sont accessibles à tous les niveaux d'accès. Par contre, la fonctionnalité « infrastructures localisées dans un secteur » est dynamique de manière à changer de contenu en fonction de l'usager. Ainsi, un gestionnaire du réseau de télécommunications ne pourrait pas avoir accès aux infrastructures du réseau d'eau potable localisées dans un secteur spécifique.

D'autres fonctionnalités telles que l'identification des infrastructures appartenant à un réseau présente les mêmes caractéristiques de « filtrage des données » selon l'usager. Ainsi, le CRP peut choisir le réseau pour lequel il veut connaître les informations. Par contre, les partenaires ont seulement accès aux données de leur propre réseau. Le même concept est adopté pour les fonctionnalités relatives aux ressources utilisées (par un réseau dans une zone d'alimentation, par un réseau dans un secteur et par une infrastructure d'un réseau), aux dépendances des réseaux face aux ressources (dans un secteur, dans une zone d'alimentation, sous forme de courbe) et aux infrastructures des autres réseaux qui utilisent les ressources (par zone d'alimentation, par

secteur). L'idée de base demeure toujours de respecter les contraintes liées à la confidentialité des informations et de s'assurer que les informations sur un réseau demeure la propriété de ce réseau. Tous les résultats de ces fonctionnalités sont fournis sous forme de rapports en version PDF sauf les courbes de dépendances et d'ED qui sont directement fournies sur une page web.

Finalement, les fonctionnalités relatives à la visualisation des infrastructures de tous les réseaux sur la carte géographique et la carte géographiques des besoins en ressources alternatives (qui seront des fonctionnalités à développer dans les projets futurs du CRP) seront accessibles seulement par le CRP et le CSC. Il faut noter que pour les fonctionnalités qui nécessitent la génération de courbes de dépendance et d'ED, ce prototype web vient améliorer les courbes pour les rendre plus visuelles.

2.4.4 Identification des ED du troisième ordre

En plus du problème d'accessibilité que l'application web permet théoriquement de résoudre et des améliorations apportées à la BD, le nouveau prototype apporte aussi plusieurs améliorations à l'application et ses fonctionnalités. L'une des améliorations les plus importantes est l'identification et la simulation des ED du troisième ordre : la version préalable de DOMINO traitant seulement les ED de premier et deuxième ordre.

L'ensemble des résultats (ED de premier, deuxième et troisième ordre) sera affiché dans un même graphique sous la forme d'une courbe d'ED. En effet, lors de la panne d'une ressource dans un secteur, quelques infrastructures des réseaux seront affectées par l'indisponibilité de cette ressource (ED de premier ordre), chacune selon un degré de gravité différent (identifié par le code de couleurs). Si certaines de ces infrastructures tombent en défaillance après un certain temps, cela peut affecter le fonctionnement d'autres infrastructures d'autres réseaux durant les 72 heures considérées par l'analyse (ED de deuxième ordre puis de troisième ordre).

Dans le but de lancer la simulation des ED, la fonctionnalité « Analyse des effets domino » a été développée dans l'application. Pour exécuter une requête, l'utilisateur choisit la ressource dont la panne est constatée ainsi que le secteur où cette panne a lieu. Ces deux paramètres permettent d'aller puiser dans les tables appropriées les informations permettant de générer la courbe des ED. Le premier résultat est la liste des infrastructures affectées directement par la panne de la ressource ainsi que les zones alimentées en ressource par ces infrastructures. Ce résultat sera conservé dans une table temporaire. Une comparaison entre les zones de fournitures et les zones d'alimentation d'autres infrastructures est faite pour identifier les infrastructures affectées indirectement par ces pannes potentielles. Le résultat est conservé dans une deuxième table temporaire. Finalement, comme pour les ED de deuxième ordre, une troisième requête utilisera le résultat de la deuxième requête afin d'identifier les infrastructures situées dans les zones d'alimentation des infrastructures affectées par l'ED d'ordre 2 pour permettre l'identification des ED d'ordre 3.

Les figures 2.4, 2.5 et 2.6 illustrent le raisonnement expliqué au paragraphe précédent. La figure 2.4 présente un ED d'ordre 1 engendré par la défaillance de la ressource « Eau » dans un certain secteur de la zone d'étude (information confidentielle ne pouvant être divulguée. La figure montre que deux infrastructures du réseau de télécommunications entrent en défaillance pendant quelques heures (état orange) avant de devenir inopérante (état rouge). Concrètement, cela se traduit par la perte des télécommunications dans les deux zones d'alimentation desservies par ces deux infrastructures. Pour des raisons de confidentialité, les noms des infrastructures affectées ont dû être noircis dans la figure.

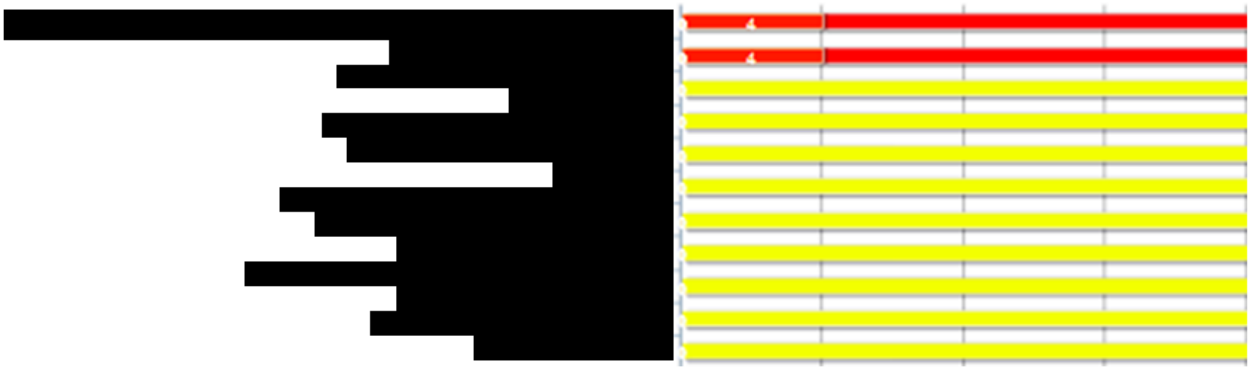


Figure 2.4 - Courbes d'ED du premier ordre suite à une panne d'eau dans un secteur

Pour identifier les ED du second ordre, il faut se baser sur les infrastructures affectées par les ED du premier ordre. Comme il l'a été expliqué précédemment, les IE affectées par les ED du second ordre sont celles qui utilisent les ressources fournies par les deux infrastructures affectées par les ED de premier ordre. C'est-à-dire que les infrastructures affectées par un ED de deuxième ordre doivent obligatoirement être situées dans les zones d'alimentation de ces deux infrastructures et utiliser la ressource en question (ici, les télécommunications). La deuxième requête prend donc en compte ces deux nouveaux paramètres comme données d'entrées pour simuler les ED de deuxième ordre. La figure 2.5 montre les ED de premier et deuxième ordre. Les courbes associées aux ED de deuxième ordre sont celles qui possèdent une première section en vert sur la courbe. Effectivement, ces infrastructures n'ont pas été affectées par la panne de la première ressource. Ainsi, on remarque que plusieurs nouvelles infrastructures sont affectées par la panne de la ressource « Télécommunications » dans les deux zones d'alimentation considérées, mais qu'une seule présente un potentiel d'ED de troisième ordre. Il s'agit d'une infrastructure de transport. Encore une fois, pour des raisons de confidentialité, les noms des infrastructures ont dû être noircis dans la figure.

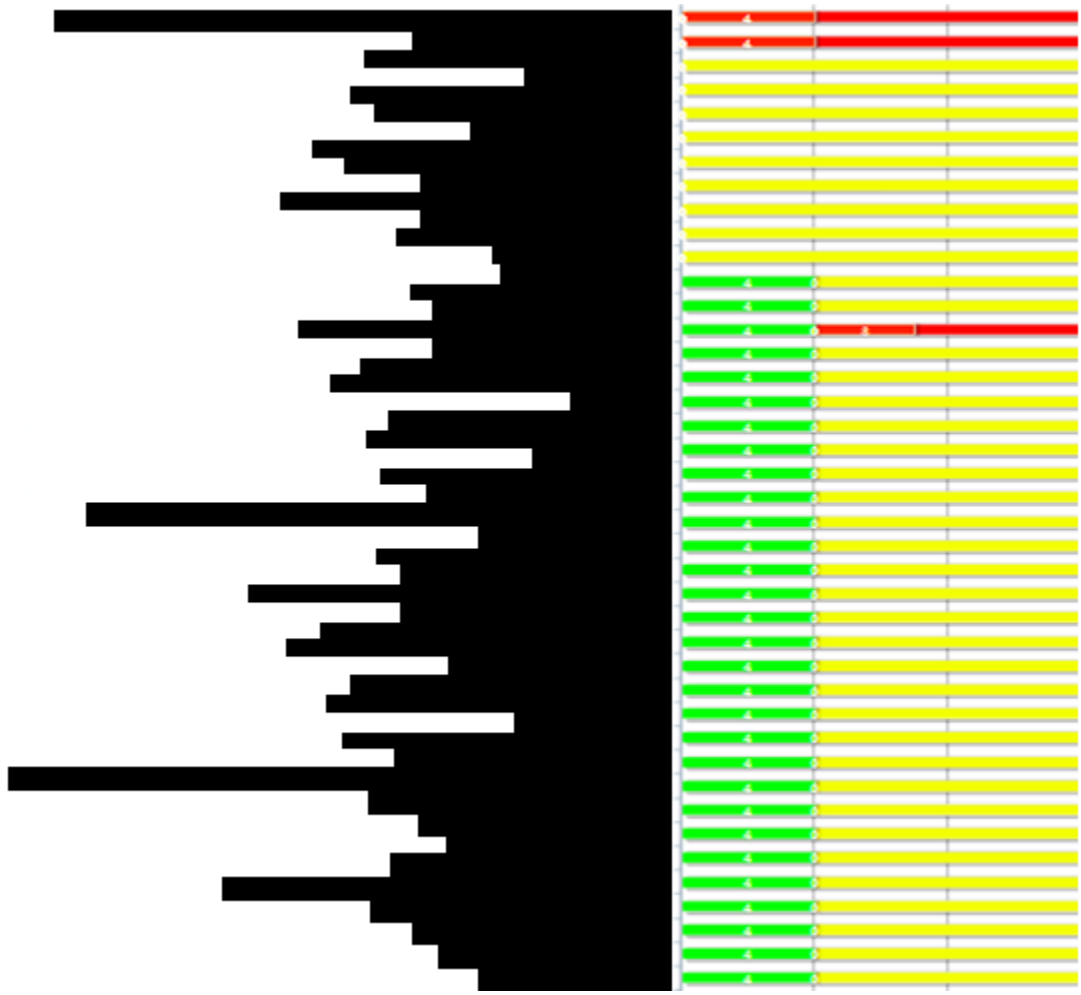


Figure 2.5 - Courbes d'ED du deuxième ordre suite à une panne d'eau dans un secteur

Pour la simulation des ED de troisième ordre, il faut prendre les résultats issus de la requête permettant de simuler les ED de deuxième ordre et procéder comme pour la précédente. La figure 2.6 montre les ED du troisième ordre.

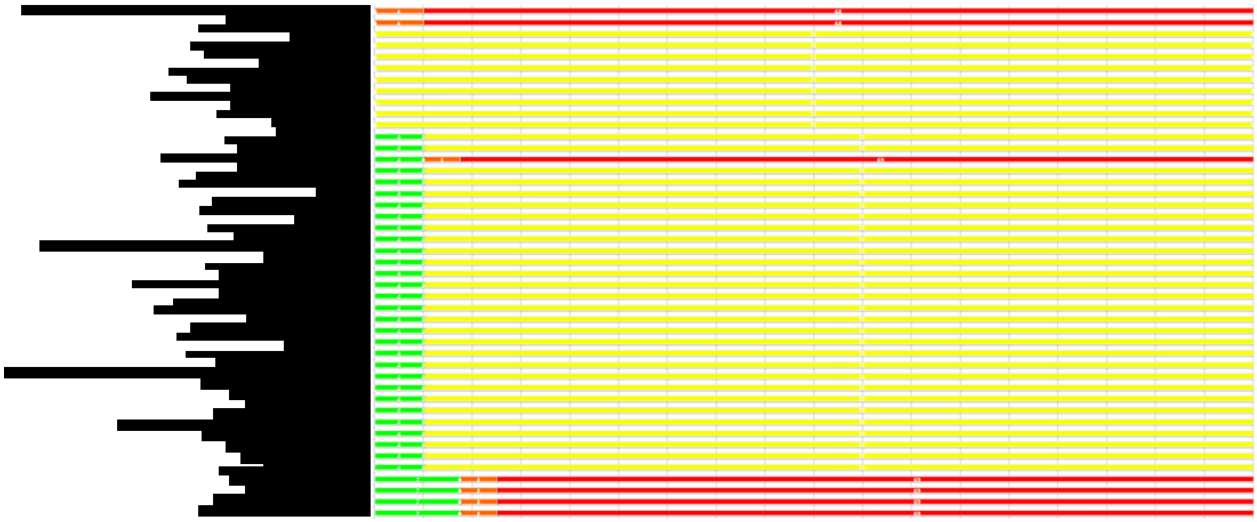


Figure 2.6 - Courbes d'ED du troisième ordre suite à une panne d'eau dans un secteur

Sur cette figure, on remarque que la panne de l'infrastructure de transport affectée par la panne de télécommunications risque d'affecter 4 nouvelles infrastructures après un certain nombre d'heures.

La génération des ED de troisième ordre apporte donc de nouvelles informations qui permettent aux gestionnaires du CSC et des IE d'avoir une idée encore plus claire de la situation. Il s'agit donc d'un apport considérable par rapport à l'ancienne version de DOMINO. Le problème posé par Access dans la génération des ED de troisième ordre a donc été résolu en affichant sur un même graphique (de type *highcharts*) le résultat de deux requêtes différentes en tant que deux objets distincts.

2.5 Développement

La phase de conception permettra de traduire en code les requis du client pour créer l'application. Le développement de la BD vient en premier puisqu'elle est à la base de l'application. Pour le développement et l'hébergement de l'application il faut un serveur web. Un serveur web est

simplement un ordinateur dont le rôle est de livrer des pages web. Pour fonctionner comme serveur web, l'ordinateur doit être équipé d'un logiciel de serveur web comme Apache[3] ou « *Internet Information Server* » (IIS) de Microsoft, pour ne nommer que ceux-là. Dans le cas de DOMINO, le serveur choisi est un serveur Apache fonctionnant sous Linux[4]. Le serveur est installé à l'École Polytechnique de Montréal. Le choix du système Linux a été fait en raison des multiples avantages qu'il procure, notamment :

- Faible coût d'implémentation : Le fait que l'application développée ne sera en fait qu'un prototype, il n'est pas pertinent de dépenser de l'argent et du temps pour obtenir des licences. Linux et la plupart de ses logiciels sont de type *General Public License* (GNU) qui ne présentent donc pas de problèmes liés à l'expiration des licences ;
- Système opérationnel stable : Linux n'a pas besoin d'être redémarré périodiquement pour maintenir sa performance. Il ne « gèle » pas et n'est pas affecté par des problèmes de ralentissement dus au manque de mémoire vive ;
- Haute performance : Linux offre une performance constante sur les postes de travail et sur les réseaux. Il peut gérer un nombre anormalement élevé d'utilisateurs simultanés ;
- Convivialité : Linux a été développé via l'Internet. Par conséquent, il supporte bien les fonctionnalités des réseaux comme les systèmes client-serveur qui peuvent être facilement installés sur un serveur Linux. Il peut effectuer des tâches comme les sauvegardes rapidement et de manière fiable ;
- Multitâches : Linux est conçu pour faire plusieurs opérations en même temps. Ainsi, par exemple, un grand travail d'impression en arrière-plan ne ralentira pas l'exécution des autres opérations ;
- Sécurité : Linux est l'un des systèmes d'exploitation les plus sécurisé. Les systèmes flexibles d'autorisation d'accès aux fichiers empêchent l'accès par les visiteurs ou les

---

[3] Apache est un logiciel de serveur web qui fonctionne sur Linux. En 2009, il est rendu le premier serveur web qui dépasse les 100 million sites usagers.

[4] Linux est un système opérationnel comme Unix, qui est open source et gratuit.

virus indésirables. Les utilisateurs de Linux ont la possibilité de sélectionner et de télécharger des logiciels en toute sécurité et très souvent gratuitement.

Sur le serveur lui-même, les plateformes PHP[5] et MySQL[6] sont installés comme logiciels pour l'implémentation de l'application. Après une analyse des différentes options possibles pour les logiciels pouvant être utilisés, PHP a été choisi comme langage de programmation pour les raisons suivantes :

- Open Source : PHP est disponible gratuitement. La communauté de type *open source* des développeurs de PHP offre un support technique et s'améliore constamment. PHP vient aussi en GPL et la plupart de ses associatives comme MySQL, Text Editors et serveur Apache le sont aussi ;
- Versatilité (*cross-platform*) : PHP est compatible avec les systèmes opérationnels (Linux, Windows, Solaris, OpenBSD, Mac OSX, etc.) et les serveurs web (Apache, IIS, iPlanet etc.). Il peut donc être facilement déployé sur plusieurs plateformes ;
- Convivialité : PHP donne plus de flexibilité dans le développement que les langages de programmation tels que C, C++ et ASP, et contribue globalement à accroître le trafic vers le site ;
- Rapidité : PHP a été conçu pour le développement web. Donc, l'accès à GET et POST et le travail avec HTML et les URLs sont des fonctionnalités préconstruites dans PHP. Il est donc vraiment adapté pour la réalisation de page web ;

---

[5] PHP est un langage de script côté serveur conçu pour le développement web, mais aussi utilisé comme un langage de programmation généraliste. PHP est maintenant installé sur plus de 244 millions de sites Web.

[6] MySQL également appelé «Mon Sequel » est la base de données relationnelle *open source* la plus largement utilisée (depuis 2008) qui fonctionne comme un serveur fournissant un accès multi-utilisateurs à un certain nombre de bases de données.

- Accès à d’autres outils : PHP facilite l’utilisation d’autres outils à l’intérieur des applications web. Cette caractéristique permettra de plus facilement intégrer les modules ArcGIS dans le futur ;
- Sécurité : PHP offre une sécurité accrue et aide à prévenir les attaques malicieuses. Ces niveaux de sécurité peuvent être ajustables dans le fichier .ini de PHP.

Pour la BD, MySQL, qui est un Système de Gestion de Bases de Données Relationnelles (SGBDR) a été choisi comme plateforme. Au fil des années, les bases de données MySQL ont été les plus performantes par rapport aux différentes bases de données qui sont disponibles sur le marché. Voici quelques avantages de ce logiciel :

- Rentable : MySQL est un système *open source*. Donc, n’importe quel développeur peut l'utiliser tel quel sous GPL. Cela donne aux développeurs la possibilité de créer des bases de données MySQL gratuitement. En même temps, des modifications peuvent être apportées au code et celui-ci peut être personnalisé selon les besoins ;
- Opérable sur toutes les plateformes : Un des grands avantages de MySQL est qu’il est opérable en multiplateformes (telles que Linux, Windows et Solaris) sans effets secondaires notables sur ses performances. De plus, la présence d'API permet son intégration avec C, C ++, Perl, Java et Python assez facilement ;
- Sécurisé : La configuration des BD sur MySQL est très sûre. Les mots de passe qui sont stockés sont toujours cryptés, limitant donc l'accès non autorisé à la BD.

Concernant le serveur mis en place pour le prototype web DOMINO, les spécifications techniques du serveur (de la machine) sont fournies au tableau 2.1.

Tableau 2.1 - Spécifications techniques du serveur de l'application web DOMINO

Spécifications hardware	Pentium core 2 duo 3.2 GHz, 4 G RAM, disque ssd 120 G
Système opérationnel	Linux CentOS 6.2 64
Serveur Web	Apache v. 2.2.15, php x86_64 v. 5.3.3
Serveur BD	mysql-server (serveur) x86_64 v. 5.1.61 mysql (client) x86_64 v. 5.1.61
Interface et accès	• PHPMyAdmin v. 3.5.1 • La machine est accessible via SSH-SFTP de partout et via le canal ssl (https) sur le réseau local de Polytechnique • L'interface graphique de gestion du serveur MySQL est accessible via PHPMyAdmin avec un compte administrateur • L'alias DNS est nommé: https://domino.mgi.polymtl.ca et pointe à la page principale de l'application

Puisque le prototype développé servira initialement à des fins d'utilisation internes, l'accès au port 80 (qui est http) sera coupé jusqu'à l'implémentation de DOMINO. Ceci pour des raisons de sécurité, mais aussi dans l'attente d'avoir obtenu toutes les autorisations requises des partenaires pour permettre l'accès à distance à DOMINO.

Utilisant *Putty* qui est un SSH client pour les plateformes Windows et Unix, la traduction du ERP commence en créant les tables une à une, en spécifiant le type des attributs, les clés, et en respectant l'ordre dans lequel les tables doivent être créées pour construire les relations.

Une fois les tables créées, phpMyAdmin, qui un outil gratuit et *open source* écrit en PHP et destiné à gérer l'administration de MySQL sur un navigateur Web, a été utilisé pour s'assurer que la structure de la BD est conforme à l'ERP.

Une fois la BD développée, il s'agit de la remplir avec les données concernant les IE. Ces données étaient déjà disponibles au CRP, mais des données fictives ont d'abord été utilisées pour valider le modèle. Il est par contre important de mentionner que les données contenues dans DOMINO proviennent strictement des gestionnaires des différentes IE. En effet, ce sont les seuls aptes à fournir une information pertinente concernant leurs infrastructures et les ressources nécessaires à leur fonctionnement. Ce sont également les seuls à posséder l'expertise pour traduire sous forme de courbes de dépendances les conséquences d'une panne de ressource sur leur fonctionnement (Robert & Morabito, 2011). Il faut aussi noter que les gestionnaires des IE n'ont pas à remplir tous les champs d'informations (selon la nature de ces informations et leur confidentialité) dans le système puisque le système a été conçu de manière à fonctionner avec des champs vides. Néanmoins, il convient de préciser que plus l'information saisie dans le système est précise et complète, plus les résultats des analyses d'ED sont précis.

Afin d'accroître la sécurité, une vérification des *cookies* est faite sur toutes les pages pour vérifier le contenu des sessions concernant les accès et les entrées de données. Ainsi, si un accès non autorisé survient sur une page, le système sort de la session en vidant tous les *cookies* et redirige l'usager vers la page d'accueil où son nom d'utilisateur et son mot de passe lui seront redemandés. De plus, si le système demeure inactif pour plus de 15 minutes, le système redirige également l'usager vers la page d'accueil où son nom d'utilisateur et son mot de passe lui seront redemandés en vidant tous les *cookies*. Ceci permet d'assurer une sécurité supplémentaire advenant le cas où un utilisateur oublierait de fermer sa session sur un poste de travail.

Concernant les fonctionnalités qui permettent de tracer les courbes, le code saisi les paramètres d'entrées spécifiés par l'utilisateur et renvois une requête MySQL au serveur qui exécute et retourne les résultats au code de PHP. Ce dernier fait le lien avec l'outil graphique et génère des courbes dynamiques que l'utilisateur peut imprimer, sauvegarder ou modifier. À la fin de chaque

fonctionnalité, le système vide les *cookies* de la session, mais ne vide pas l'identification de l'utilisateur, sauf en cas de fermeture de session. Ainsi, aucune donnée n'est jamais enregistrée sur aucun poste, ce qui accroît une fois de plus la sécurité de l'outil. Il s'agit de plus d'une contrainte formulée par les gestionnaires des IE : en aucun temps, les données sources ne doivent se retrouver ailleurs que dans la BD.

Pour la génération des rapports, l'outil FPDF a été utilisé. Les fichiers PDF prennent les résultats des requêtes de MySQL et les affichent dynamiquement. Ils sont personnalisés en fonction de l'usager (de la session ouverte) et les résultats sont triés par réseau ou bien par secteur (ou zone d'alimentation) selon le choix de l'usager et selon la nature des informations générées. De plus, les utilisateurs peuvent imprimer ou sauvegarder ces rapports qui comportent une notice légale concernant l'utilisation qui peut être faite des informations générées. Comme il l'a été mentionné précédemment, les informations contenues dans DOMINO et les résultats des simulations ne doivent servir à aucune autre fin que celle liées à ce projet. Cette notice légale vise donc à le rappeler et à lier l'utilisateur à cette clause. Finalement, sur le plan technique, puisque la structure de la BD a changé et que les données sont maintenant stockées dans des tables distinctes, les requêtes permettant de réaliser les rapports sont plus complexes puisqu'ils doivent maintenant joindre plusieurs tables à travers l'utilisation de la fonction *INNER JOIN*.

Une filtration importante des données est soigneusement faite sur toutes les pages accessibles à un utilisateur donné. Cette filtration est faite au niveau des requêtes qui ne recherchent dans la BD que les données spécifiques à chaque accès et à chaque fonctionnalité tout en tenant compte des paramètres d'entrées sur lesquels sont basées ces requêtes. Ceci pour s'assurer que chaque utilisateur ait bien accès uniquement aux informations auxquelles il peut avoir accès.

Pour rendre les pages dynamiques, au lieu de créer la même page plusieurs fois (pour chaque type d'accès), le contenu des pages est dynamiquement généré en fonction de l'accès accordé à l'utilisateur. Pour cela, le système compare le niveau de l'accès correspondant à l'identifiant de l'utilisateur ayant ouvert la session avec les niveaux d'accès présents dans la BD et génère le contenu spécifique au niveau d'accès octroyé à cet utilisateur.

Tel qu'il l'a été expliqué dans la section 2.4.1, la table Tab_Reseaux contient l'attribut actif_reseau (paramètre booléen) qui est responsable de rendre le réseau actif ou inactif. Cela veut dire que si ce booléen est égal à 1, les données reliées à ce réseau vont être affichés dans les requêtes, sinon (le booléen est égale 0), le réseau est considéré comme inactif et les données reliées à ce réseau ne figurent pas dans les résultats de la requête. Cela permet aussi d'ajouter ou de retirer un réseau des analyses sans d'ED sans avoir à faire de manipulations complexes dans la BD ce qui risquerait de la compromettre. Les figures en annexe présente les différentes interfaces de DOMINO version web.

CHAPITRE 3 TESTS ET VALIDATIONS

La phase de tests est la dernière étape avant de pouvoir délivrer le prototype. Cette phase est nécessaire afin de vérifier que le système et la BD forment un produit fonctionnel et conforme aux requis du système étudié en premier lieu et que les résultats produits correspondent bien aux résultats attendus. La phase de tests comporte une première validation faite à l'interne par les experts du CRP. Cette validation vise à confirmer que le système fourni les bons résultats et que la gestion des accès est fonctionnelle et répond aux contraintes exprimées dans le cahier des charges. Par la suite, une validation est faite avec les partenaires du CRP. Cette validation permettra de présenter le prototype de la plateforme web DOMINO aux partenaires du CRP et d'aborder les défis reliés à l'implémentation de l'outil (mise en ligne et opérationnalisation à la ville de Montréal). Cette deuxième validation permettra d'ouvrir les discussions sur l'orientation future de l'espace de coopération mis sur pied par le CRP et sur le développement d'un cadre régissant le partage d'information entre les IE : cadre essentiel pour assurer la pérennité de DOMINO.

3.1 Validation à l'interne du CRP

Tout logiciel peut comporter des erreurs, la plupart seront rapidement identifiées lors de la phase de tests tandis que d'autres *bugs* surviendront dès les premiers mois d'exploitation de l'application web. Une fois que le code a été développé, il doit être testé pour s'assurer que le produit final est conforme aux requis du client identifiés lors de la première phase et s'assurer de l'absence de problèmes informatiques lors de l'exécution de l'ensemble des fonctions. Cette phase est très importante puisque les erreurs peuvent y être présentes discrètement, quelques-unes ne sont pas si importantes, mais d'autres sont dangereuses puisqu'elles peuvent conduire à des résultats complètement faux. Or, puisque ces résultats pourront mener à des actions à prendre au niveau des organisations (comme mobiliser des personnes en vue d'une intervention ou mettre en place des mesures pour protéger certaines infrastructures), il est fondamental de s'assurer que ces résultats soient cohérents et exacts. Cette validation est d'abord faite par le programmeur à partir de données de travail (données fictives) tout au long du processus de programmation des différentes requêtes, et ensuite par le personnel du CRP qui travaille sur les interdépendances

entre les IE à Montréal depuis plusieurs années et qui est familier avec les résultats qui devraient être produits par l'outil. Ce travail a d'abord consisté à saisir les données réelles des partenaires dans la nouvelle application et de constater, par une série de tests et de simulations, que les résultats des requêtes sont exacts. Suite à cette phase de tests, quelques modifications statiques ont été demandé et d'autres plus importantes au niveau des requêtes. Cela a permis d'obtenir un produit final répondant aux exigences fixées.

La figure 3.1 présente un des nombreux exemples de simulations réalisés par le CRP pour valider l'outil. Sur cette figure, on voit le résultat de la simulation d'une panne d'eau dans un secteur de la ville de Montréal tel que fournit par la version Access de DOMINO.

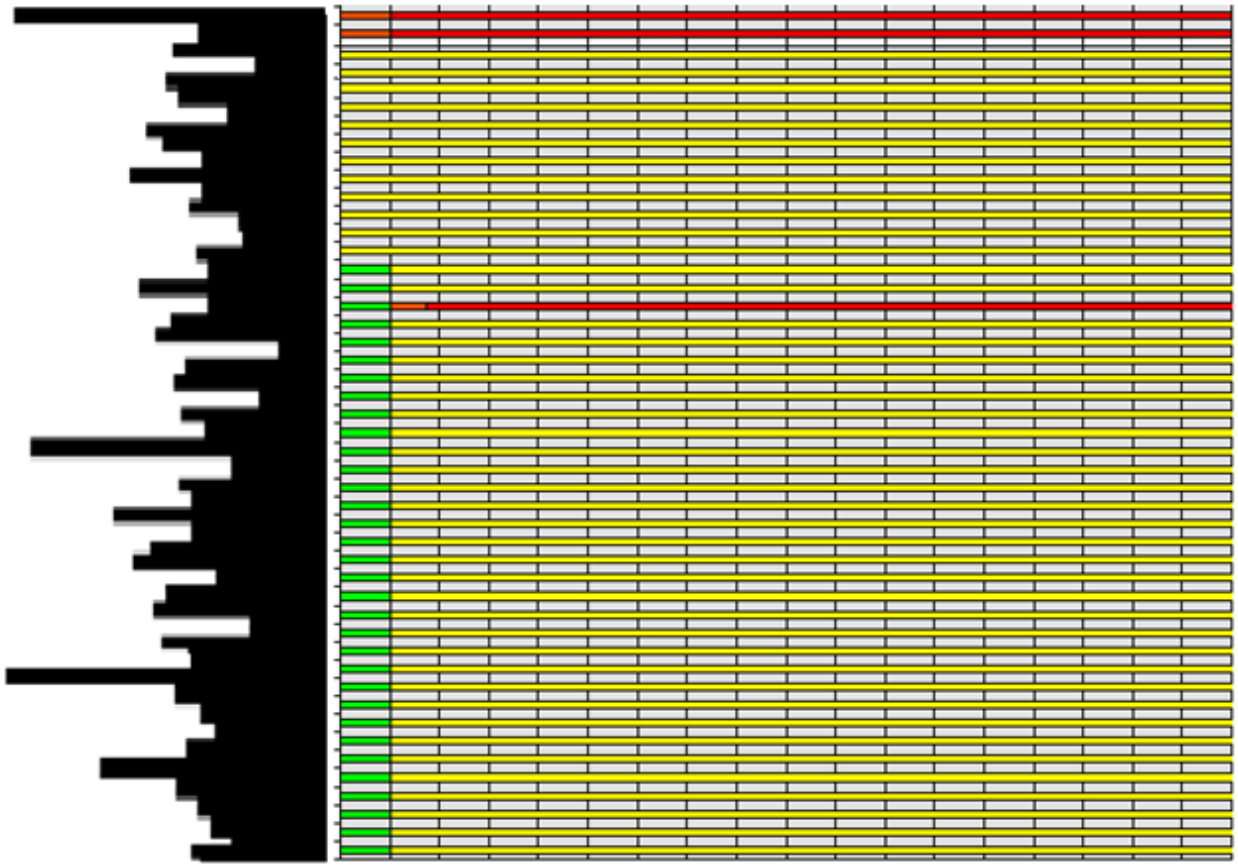


Figure 3.1 - Simulation d'un ED réalisée par DOMINO version Access

La figure 3.2 illustre la même requête, mais cette fois, réalisée par la nouvelle version de DOMINO.

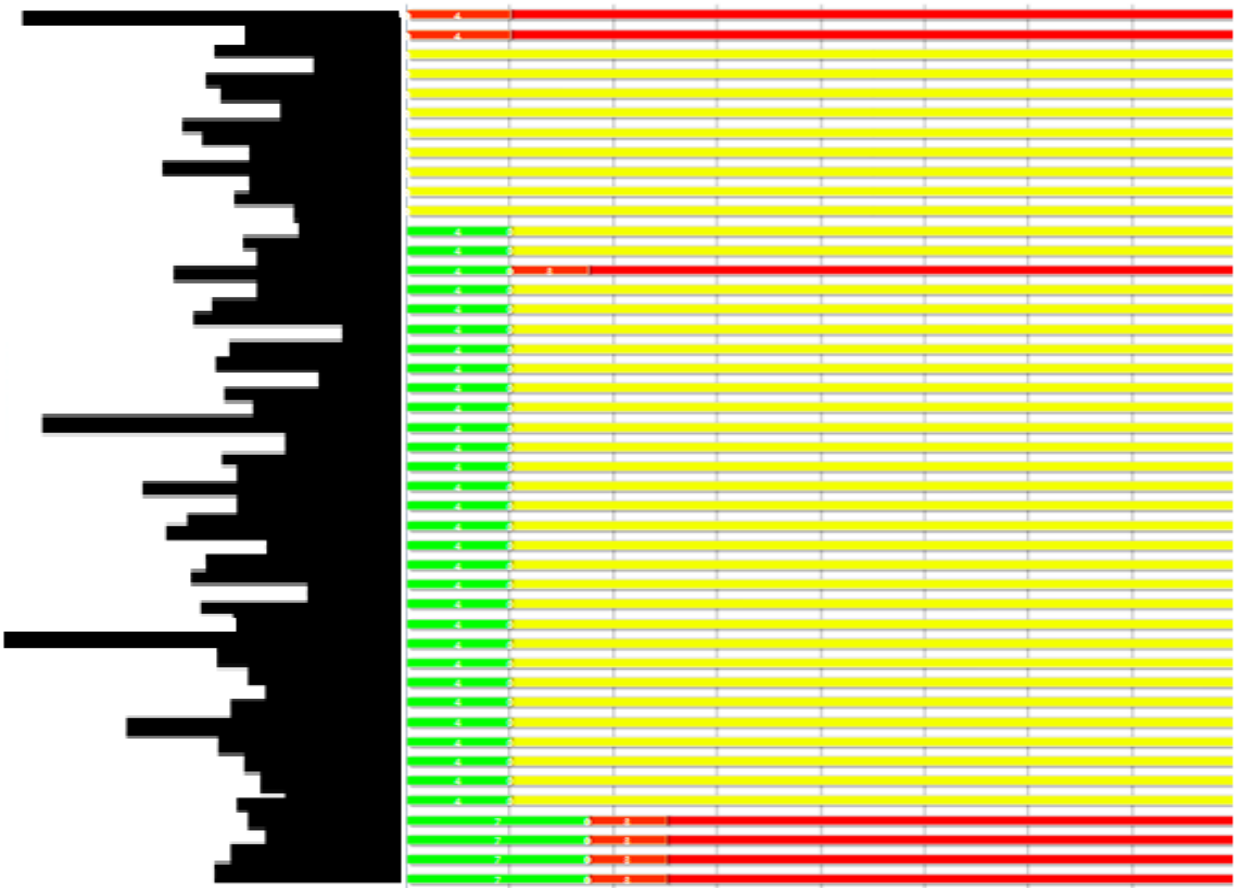


Figure 3.2 - Simulation d'un ED réalisée par DOMINO version web

En comparant les deux figures (3.1 et 3.2) on remarque que les deux résultats sont identiques à cette différence que la version web de DOMINO fournit également les ED de troisième ordre (4 infrastructures au bas de la courbe).

3.2 Validation auprès des partenaires

Une fois que la vérification et la validation du bon fonctionnement du SE ont été effectuées au sein du CRP, il a été nécessaire de présenter l'outil aux partenaires : les experts des IE et les gestionnaires du CSC. Pour cela, les partenaires du CRP ont été invités à une rencontre de travail

en mai 2013. Les gestionnaires présents autour de la table représentaient les réseaux et organisations suivants : Bell, Hydro-Québec, Gaz Métro, Agence Métropolitaine de Transport (AMT), Société de Transport de Montréal (STM), Ville de Montréal (Réseau d'eau potable), CSC de la ville de Montréal ainsi que le Ministère de la Sécurité Publique du Québec (MSP) et le Ministère de Transport Québec (MTQ).

La rencontre a débuté par un rappel de DOMINO version Access (couplé avec ArcGIS), montrant ainsi la problématique d'accessibilité que cette version génère. Par la suite, une démonstration de la nouvelle version de DOMINO a été réalisée. Cette démonstration a permis de démontrer la fonctionnalité du produit et de montrer l'intégration concrète des niveaux d'accès dans l'application. Elle a aussi permis d'amener sur la table la question de la sécurité. Cette question est primordiale puisqu'elle devra permettre d'atteindre un consensus qui permettra d'opérationnaliser DOMINO.

3.2.1 Identification de la problématique de sécurité

DOMINO est une application web qui consiste en un ensemble de fonctionnalités qui permettent globalement d'analyser les interdépendances entre les IE et d'analyser les ED susceptibles de se produire lors de la défaillance de l'une d'elles. Cette application est installée sur un serveur (ou éventuellement sur plusieurs serveurs miroirs (*mirroring*) qui sont accédés à distance par les gestionnaires des IE partenaires du CRP afin de simuler différentes situations. Une gestion de DOMINO est nécessaire pour les mises à jour continuelles du système et les mises à jour des données.

Dans ce contexte, la question de la sécurité a été abordée en trois points : la sécurité des liens avec l'application (connectivité Internet), la sécurité de l'hébergement (du serveur) et la sécurité de l'application (gestion des accès et gestion du système).

3.2.1.1 Connectivité Internet

Il existe plusieurs façons pour se connecter à une application web. Les méthodes les plus répandues et celles qui ont été retenues comme possibles dans le cadre d'un partage d'informations multi-organisationnelles sont la connectivité non-sécurisée (http), la connectivité sécurisée encryptée (https) et la connexion de type VPN. Le tableau 3.1 compare les différents types de connectivités possibles avec leurs avantages et inconvénients respectifs. Un choix devra éventuellement être fait par les partenaires en se basant sur le niveau de sécurité recherché et en tenant compte des caractéristiques de l'application.

Tableau 3.1 - Connectivités possibles pour DOMINO

	Non sécurisé	**Sécurisé (encrypté)**	**VPN**
Accès via des appareils mobiles	OUI	OUI	OUI
Nécessite une configuration spécifique	NON	NON	OUI : Configuration nécessaire pour chaque appareil
Cryptage des données échangées	NON	OUI	OUI
Coûts ($)	Aucun	Faibles	Plus élevés
Vitesse de communication	Rapide	Rapide (ralentissement si beaucoup d'informations)	Rapide (ralentissement si beaucoup d'utilisateurs)
Accessibilité	Très bonne. Aucune configuration nécessaire	Très bonne. Aucune configuration nécessaire	Complexe : Chaque utilisateur doit avoir un compte VPN. Des organisations ne veulent pas établir de tels accès.
Évolution dans le temps	Très facile	Facile	Plus complexe en raison des multiples configurations

Comme on peut le voir sur ce tableau, le mode accès non sécurisé ne demande pas de configuration spécifique ce qui facilite l'accès de plusieurs utilisateurs (grande accessibilité),

offre une vitesse d'accès rapide et permet une évolution très facile dans le temps en raison du très peu de configuration à réaliser. Par contre, les données transmises ne sont pas encryptées. Pour l'accès sécurisé (encrypté) les données sont encryptées ce qui offre une plus grande sécurité. Toutefois, lorsque les informations échangées sont plus grandes, la vitesse est moins bonne. Rappelons que les informations échangées entre l'application DOMINO et les usagers est restreinte ce qui fait en sorte que la vitesse n'est pas un facteur si contraignant. Finalement, la connexion VPN nécessite une configuration spécifique sur chaque poste qui désire se connecter à l'application et chaque utilisateur doit avoir un compte VPN ce qui réduit l'accessibilité et la rend beaucoup plus complexe. L'évolution dans le temps devient également plus complexe en raison de l'augmentation des configurations devant être effectuées sur les différents appareils des utilisateurs. Cette solution présente un inconvénient majeur : en situation d'urgence, un usager qui devrait accéder au système à partir d'un point non configuré ne pourrait pas. Aussi, la vitesse de communication est inversement proportionnelle à l'augmentation du nombre d'utilisateurs.

3.2.1.2 Hébergement des serveurs

En ce qui concerne l'hébergement, il existe divers types d'hébergements possibles pour cette application lesquels peuvent être regroupés en deux grandes catégories d'hébergement : les hébergements par des prestataires de services et les hébergements « maison » offert par un des partenaires de travail (École Polytechnique ou tout autre partenaire du CRP). Le tableau comparatif 3.2 permet d'illustrer les avantages et inconvénients de chacun d'eux.

Tableau 3.2 - Types d'hébergements possibles pour DOMINO

	Prestataires de services	**Hébergement « maison »**
Sécurité physique	Renforcée (selon les prestataires)	D'élevée à renforcée (varie selon l'organisation)
Sécurité informatique	Renforcée (selon les prestataires)	D'élevée à renforcée (varie selon l'organisation)
Coût ($)	Variables selon le niveau de sécurité garanti contractuellement	Plus faibles
Accessibilité à l'application	De l'ordre de 99.95% du temps	Tributaire de ressources internes de l'organisation. Tributaire des engorgements possibles en cas de crise
Contrôle de l'hébergement des données et informations	Aucun	Très bon

Les divers types de serveurs possibles pour DOMINO présentés dans ce tableau comparatif sont le fruit d'un *brainstorming* sur la nature possible de l'hébergement pour une telle application. Le tableau montre les avantages et inconvénients de chacun. Les prestataires de services offrent une sécurité physique et informatique renforcées (proportionnellement aux coûts normalement) et un temps de disponibilité du serveur (*up time*) de 99.95% ce qui est primordial pour une telle application qui doit être accessible en tout temps et surtout en situation d'urgence. Par contre, il n'y a aucun contrôle sur l'hébergement des données : celles-ci peuvent se retrouver n'importe où sur la planète. Concernant l'hébergement « maison », il présente un bon contrôle sur les données, mais peut être tributaire des engorgements possibles en cas de crise. De plus, la sécurité physique, informatique et l'accessibilité sont tributaires des ressources internes de l'organisation.

3.2.1.3 Gestion des accès et des informations

En ce qui concerne la gestion des accès et des informations, l'application DOMINO web est munie d'un système d'identification basé sur l'utilisation d'identificateur et de mot de passe qui permet des accès spécifiques aux informations. Par contre, le niveau de sécurité peut être davantage renforcé à la demande des partenaires. Par exemple, on pourrait introduire dans DOMINO un module qui associerait les identifiants et les mots de passe à l'utilisation de questions personnelles ou même une procédure d'authentification en deux étapes ou encore introduire des clés de session individuelles, etc. Ces solutions très techniques sont envisageables. L'important sur ces mesures est qu'il faut toujours rechercher un équilibre entre le niveau de sécurité souhaité et l'accessibilité désirée.

Comme il l'a été largement explicité dans la section 2.3 de ce mémoire, la gestion des accès en ce qui concerne les usagers du système est largement prise en compte dans DOMINO par l'entremise des cinq différents niveaux d'accès. On pourrait aussi rajouter d'autres niveaux d'accès à la demande des partenaires, mais l'une des questions qui demeure importante et qui n'est pas de nature technique est : « Qui sera le gestionnaire de cet application ? ».

Puisque les données dans DOMINO ne sont pas des données brutes, mais surtout des données provenant d'expertises, il apparaît évident que les mises à jour des informations et la maintenance de l'application constituent une problématique majeure. D'une part puisque l'entité responsable de ces opérations aura accès à l'ensemble du système (et donc aux données) et d'autres part puisque les manipulations dans la BD et dans l'application peuvent corrompre le système si elles ne sont pas effectuées adéquatement. Une entrée de données inadéquate peut générer des erreurs et corrompre l'ensemble des informations de la BD. Les changements dans la BD nécessitent une certaine expertise pour assurer la cohérence des informations (comprendre l'impact des valeurs entrées et des seuils pour savoir réellement à quoi correspondent les informations entrées). De plus, de nouvelles requêtes et analyses devront être réalisées afin de répondre aux besoins évolutifs des partenaires et ainsi maintenir en vie l'application. Cela suppose donc de modifier le code pour pouvoir programmer de nouvelles requêtes.

Ces questions adressent directement la problématique de la nature du gestionnaire de l'application. Le gestionnaire ayant un accès complet et sans restriction à l'ensemble des données, cette question doit être répondue avant la suite des travaux. Jusqu'à présent, le gestionnaire avait été le CRP puisqu'il était en charge du développement de la méthodologie et de l'outil, mais cela se faisait dans le cadre d'un projet de recherche. L'implémentation réelle de l'outil et sa gestion à long terme pourrait nécessiter d'identifier un nouveau gestionnaire. Cette entité pourrait être le MSP, le CSC, le CRP ou un consultant. Il est toutefois important de noter que l'un des dangers associé au gestionnaire est l'utilisation des informations à d'autres fins que celles pour lesquelles elles ont été partagées. Comme il l'a été mentionné plus tôt, ces informations ont une valeur énorme. Elles peuvent concéder un avantage concurrentiel important pour celui qui les possède, mais elles peuvent aussi représenter un risque important pour les organisations si celles-ci sont divulguées. Il faut noter que le gestionnaire de la BD et le développeur de la BD peuvent être deux entités distinctes : Le premier ayant accès aux données et le second ayant accès au code. Quoi qu'il en soit, l'identité du gestionnaire est une question à laquelle il faudra indéniablement répondre avant la phase de l'implémentation.

3.2.2 Recommandations des partenaires

Suite à la présentation de l'outil et de la problématique de sécurité engendrée par l'outil et à l'aide des commentaires émis par les partenaires, plusieurs constats ont pu être établis.

D'abord, relativement aux trois points discutés précédemment, les partenaires semblent orienter unanimement leur choix vers une connectivité sécurisée et cryptée de type https en raison de la simplicité de mise en place et de la facilité de gestion à long terme. La connexion non sécurisée de type http a été rejetée d'emblée. Quant à la connexion de type VPN inter-organisationnel, il apparaît clairement que cette solution ne pourrait être appliquée puisque les organisations n'accepteraient pas que les postes de travail à l'interne d'une organisation puissent être configurés pour être directement reliés à des postes à l'externe appartenant à une autre organisation en raison de leurs politiques relatives à la sécurité informatique. Il faut bien comprendre que ce type de connexion crée un pont entre les postes, si bien que les postes ainsi

reliés font partie du même réseau. De plus, ce type de connexion demande une configuration de chacun des postes qui peut être complexe (surtout au niveau des applications mobiles) et cela peut représenter un obstacle à long terme dans la gestion des accès. Finalement, cette solution présente l'inconvénient majeur de limiter l'accès à l'outil : en situation d'urgence, un usager qui voudrait se connecter à DOMINO à partir d'un poste non configuré ne pourrait pas le faire, ce qui n'est absolument pas souhaitable. Par contre, l'option d'utiliser un mode hybride (VPN et https) semble être privilégiée dans le cas où un gestionnaire devrait accéder à DOMINO à partir d'un poste personnel (ex. : postes à la maison). Dans ce cas, un usager pourrait se connecter à son organisation à partir de son domicile via une connexion VPN et ensuite utiliser une connexion https pour se connecter à l'application DOMINO. D'ailleurs, la plupart des gestionnaires autour d'IE possède déjà une connexion VPN liant leur poste personnel au réseau informatique de leur organisation. Cette solution offre une double protection puisque l'accès via VPN à l'organisation soumettra l'accès à DOMINO aux mêmes politiques de sécurité appliquées par l'organisation pour tous les accès Internet. De plus, cette solution n'implique aucune mesure supplémentaire puisque les configurations requises ont déjà été faites (ou pourront facilement être faites pour les gestionnaires des organisations qui ne possèdent pas de liaison VPN avec leur organisation).

Pour ce qui est de l'hébergement du serveur, la majorité des partenaires semblent privilégier l'hébergement de type « maison », au moins à court terme. En effet, l'idée de voir leurs données hébergées sur un serveur sur lequel on n'a pas de contrôle et dont on ne connaît pas vraiment les personnes qui peuvent y avoir accès ne plaît pas aux partenaires. Bien que cette dernière solution présente des avantages au niveau de la garantie du temps de disponibilité du serveur (*up time*), le fait que DOMINO ne soit pas un outil destiné à être utilisé quotidiennement fait en sorte que ce temps de disponibilité n'est pas un facteur essentiel pour les partenaires. Ainsi, les partenaires ne semblent pas privilégier un hébergement à un endroit plutôt qu'à un autre. Toutes les options d'hébergement présentées par le CRP ont été qualifiées de potentielles selon les coûts et l'orientation que prendra l'opérationnalisation de DOMINO à long terme. Si le projet demeure d'envergure Montréalaise, alors DOMINO pourra continuer d'être hébergé par le CRP ou même le CSC ou encore tout autre partenaire qui voudra bien accepter de l'héberger. Par contre, bien qu'elles ne soient pas encore officiellement impliquées dans le projet, les autres grandes municipalités de la région métropolitaine ont manifesté un intérêt pour DOMINO. De plus, la

plupart des organisations partenaires du CRP dépassent les frontières de Montréal (les grands réseaux d'infrastructures sont souvent établis dans l'ensemble de la province, voire du pays). Puisqu'il est donc impensable d'avoir un outil DOMINO pour chaque municipalité, l'idée que les données soient hébergées au MSP semble plaire à plusieurs. En outre, le MSP possède déjà un cadre bien défini relatif à la protection des données qui sont dans ses serveurs ce qui semble en rassurer plusieurs. Une demande a d'ailleurs été officiellement adressée au MSP pour connaître leurs niveaux de sécurité pour l'hébergement et les accès.

Finalement, relativement à la gestion des accès et des informations (gestionnaire), les partenaires ne semblent pas privilégier, *a priori*, une avenue plutôt qu'une autre. Dans tous les cas, on estime que le CRP ou le MSP pourrait être les gestionnaires de la future application DOMINO. À court terme par contre, les partenaires semblent être d'accord sur le fait que le gestionnaire des données et le développeur de l'application devrait être le CRP en raison de son expertise et de sa connaissance du système. Le MSP pourrait fournir un support au niveau de l'hébergement et de l'opérationnalisation de DOMINO pour s'assurer que le jour où on veuille transférer la gestion de DOMINO vers le MSP, l'outil puisse être pris en charge sans trop de modifications au niveau du code. Sur le long terme, en fonction de l'envergure géographique que prendra le déploiement de DOMINO, il est donc préférable que le gestionnaire de l'application soit une entité dont la mission est la sécurité civile. Si le projet demeure Montréalais, alors le CSC pourrait prendre ce rôle ; si le projet prend une portée nationale, alors le MSP est cette entité.

3.2.3 Accessibilité versus sécurité

L'utilisation de l'application web DOMINO demande un compromis entre la sécurité des informations contenues dans la BD et l'accessibilité pour les personnes à l'interne des réseaux. Or, la sécurité des informations et l'accessibilité sont deux paramètres inversement proportionnelles : plus la sécurité augmente, plus l'accessibilité diminue, et inversement. Pour cela, il sera important de comprendre où doit se situer l'équilibre entre ces deux paramètres dans le cas de DOMINO. Le partage de l'information est l'objectif ultime visé par DOMINO puisque l'information toute seule ne sert à rien. Une sécurité absolue de DOMINO décourage les

organisations en raison de sa complexité ; une accessibilité absolue à DOMINO décourage les organisations en raison de la confidentialité de leurs informations. Ainsi, la recherche d'un point d'équilibre est nécessaire.

Pour cela, une attention majeure doit être accordée à l'aspect «cyber sécurité», principalement dans le but d'assurer la sécurité des systèmes et des IE. Une bonne partie de cette sécurité repose sur les questions d'authentification, la gestion des identités, la vulnérabilité au *hacking/phishing/programs* malveillants et ainsi de suite. Ces mesures peuvent êtres problématiques pour les personnes qui se servent de la technologie de l'information pour rendre les informations accessibles aux parties concernées. Plusieurs statistiques indiquent que la sécurité exhaustive au niveau des systèmes informatiques décourage les utilisateurs d'utiliser ces applications dans leur travail quotidien. Or l'objectif primordial de n'importe quelle sécurité appliquée à un système est la capacité de prévenir n'importe quel accès indésirable tout en permettant un accès autorisé aux informations qui peuvent être accédées par des parties spécifiques. Cependant, rendre l'information accessible, tout en conservant la confidentialité, est l'un des principaux défis de la mise en œuvre de systèmes d'information. Pour concevoir un système informatique qui est responsable du partage des informations confidentielles, l'accessibilité et la confidentialité de l'information doivent être adressées en parallèle. Un équilibre entre les deux est nécessaire, car l'échec de chacun de ceux-ci peuvent influencer négativement l'utilisation du système. Suite aux discussions avec les partenaires il a été déduit que l'accessibilité est favorisée tout en laissant un niveau de sécurité élevé. Le tableau 3.3 illustre l'échelle de sécurité *versus* accessibilité et le positionnement des partenaires dans le portrait.

Tableau 3.3 - Échelle de sécurité *versus* accessibilité

SÉCURITÉ	extrêmement élevée	très élevée	élevée	normale	
	peu importante	importante	très importante	extrêmement importante	**ACCESSIBILITÉ**

3.3 Cadre de partage d'information entre les IE

Au cours de la réunion de validation, l'importance du MSP dans le projet d'opérationnalisation de DOMINO a été soulevée à plusieurs reprises par les partenaires. Il faut bien comprendre que, présentement, DOMINO est appliqué seulement à la ville de Montréal. Par contre, une opérationnalisation de DOMINO à grande échelle demande forcément une volonté gouvernementale qui ne peut être matérialisée que par l'implication du MSP dans ce projet. Or, l'un des freins majeurs à l'implémentation et à l'opérationnalisation de DOMINO est qu'il n'existe pas au Québec, ni même au Canada, une directive établie et appuyée par un contexte législatif clair qui encadre le partage et la gestion des informations relatives à la protection des IE.

La problématique du partage d'information entre des organisations diverses, qu'elles soient publiques ou privées, est bien réelle. Ces informations sont la propriété des différentes IE et ces dernières sont très réticentes à les partager. Cette réticence a largement été explicitée par Robert et Morabito (2012) et elle est principalement due au fait que le partage d'information représente une vulnérabilité supplémentaire pour les organisations du point de vue de la compétitivité comme du point de vue des risques inhérents à une utilisation inappropriée de l'information (mauvaises interprétation des données, utilisation à d'autres fins, utilisation pour commettre des actes de malveillance, etc.). Néanmoins, tous s'entendent pour dire que pour comprendre les

interdépendances et les phénomènes d'ED et dans le but de mieux gérer collectivement les risques associés à leur défaillance, il est impératif pour les organisations de partager les informations pertinentes. En effet, le partage d'informations confidentielles sur les IE offre plusieurs avantages dont principalement de permettre une plus grande coordination entre les différents intervenants impliqués dans la sécurité civile. Globalement, le partage d'informations entre les autorités fédérales, provinciales et locales :

- prépare mieux chaque niveau à l'évaluation des vulnérabilités des IE, à la réparation de ces vulnérabilités et la réponse aux menaces et aux attaques ;
- améliore l'expertise technique du secteur privé en augmentant le flux d'informations aux différentes entités du secteur privé, qui contrôlent une grande partie des IE ;
- permet une intervention et un rétablissement plus rapide et plus efficace en situation d'urgence.

Cependant, l'effort nécessaire afin de promouvoir un grand niveau de partage n'est pas sans risques. Plus l'information est partagée, plus les chances de voir cette information disponible augmente et plus la probabilité d'être victime d'un acte de malveillance augmente aussi. Par conséquent, des mesures de sécurité accrues sont nécessaires lors du partage de l'information. En outre, le partage de l'information dans le secteur, surtout dans le secteur privé, peut conduire à la divulgation accidentelle de renseignements commerciaux confidentiels à des concurrents (Gallagher & Neugebauer, 2010).

De plus, le partage des informations confidentielles entre les secteurs public et privés peut conduire à la divulgation de renseignements au public qui est à la fois involontaire et indésirable. La publication de ces informations permettra d'exposer des entités de ces secteurs à des risques non désirés. Le fait que des informations puissent tomber dans les mains de concurrents, est souvent la raison la plus citée pour ne pas partager des informations. Le secteur privé n'est pas la seule entité circonspecte quant à la divulgation de renseignements. Les organismes gouvernementaux souhaitent également la confidentialité de leurs informations. Ainsi, il importe

de définir un cadre régissant le partage d'information entre, non seulement les gestionnaires des IE entre elles, mais aussi entre les IE et le gouvernement (Gallagher & Neugebauer, 2010).

Ainsi, certains pays ont pris conscience que tant et aussi longtemps qu'un cadre normatif strict ne viendrait pas formaliser ce processus de partage, les organisations resteraient campées sur leur position et resterait fermé à toute forme de partage de données. Différents pays ont donc mis en place des modèles de sécurité pour les systèmes informatiques utilisés dans le partage des informations confidentielles entre ces infrastructures. Le Québec pourrait s'inspirer de ces modèles de collaboration et de partage d'information existants ailleurs et développer un cadre similaire répondant à ses propres besoins. Deux de ces modèles sont abordés dans les sections suivantes. Le premier est le modèle américain et le second est le modèle australien. À titre de comparaison, le modèle canadien est aussi présenté, bien qu'il ne s'agisse pas d'un modèle en soit, mais plutôt d'une stratégie nationale appuyées par un plan d'action.

3.3.1 Modèle américain

Aux États-Unis, le *Department of Homeland Security* (DHS) a mis sur pied un programme appelé *Protected Critical Infrastructure Information Program* (PCII) dont le but est de privilégier les échanges d'informations volontaire entre les propriétaires et gestionnaires des IE et le gouvernement en protégeant physiquement les données provenant des IE contre les intrusions dans les systèmes, mais aussi en les protégeant au niveau de leur utilisation. La protection PCII signifie que les partenaires de la sécurité peuvent être assurés que le partage de l'information avec le gouvernement n'exposera pas les données sensibles. Le DHS utilise le PCII pour analyser et sécuriser les IE, identifier les vulnérabilités et développer les évaluations des risques et améliorer les mesures de préparation et de rétablissement (U.S. Department of Homeland Security, 2011).

En plus de créer ce programme de protection des informations, le DHS a créé le *National Protection and Programs Directorate* (NPDD) qui est l'entité responsable de tout ce qui est en relation avec la sécurité nationale dont les échanges entre les gestionnaires des IE et l'État. La

figure 3.3 montre la structure du DHS et la position du NPPD à l'intérieur de celle-ci. La figure 3.4 montre, quant à elle, la structure du NPDD.

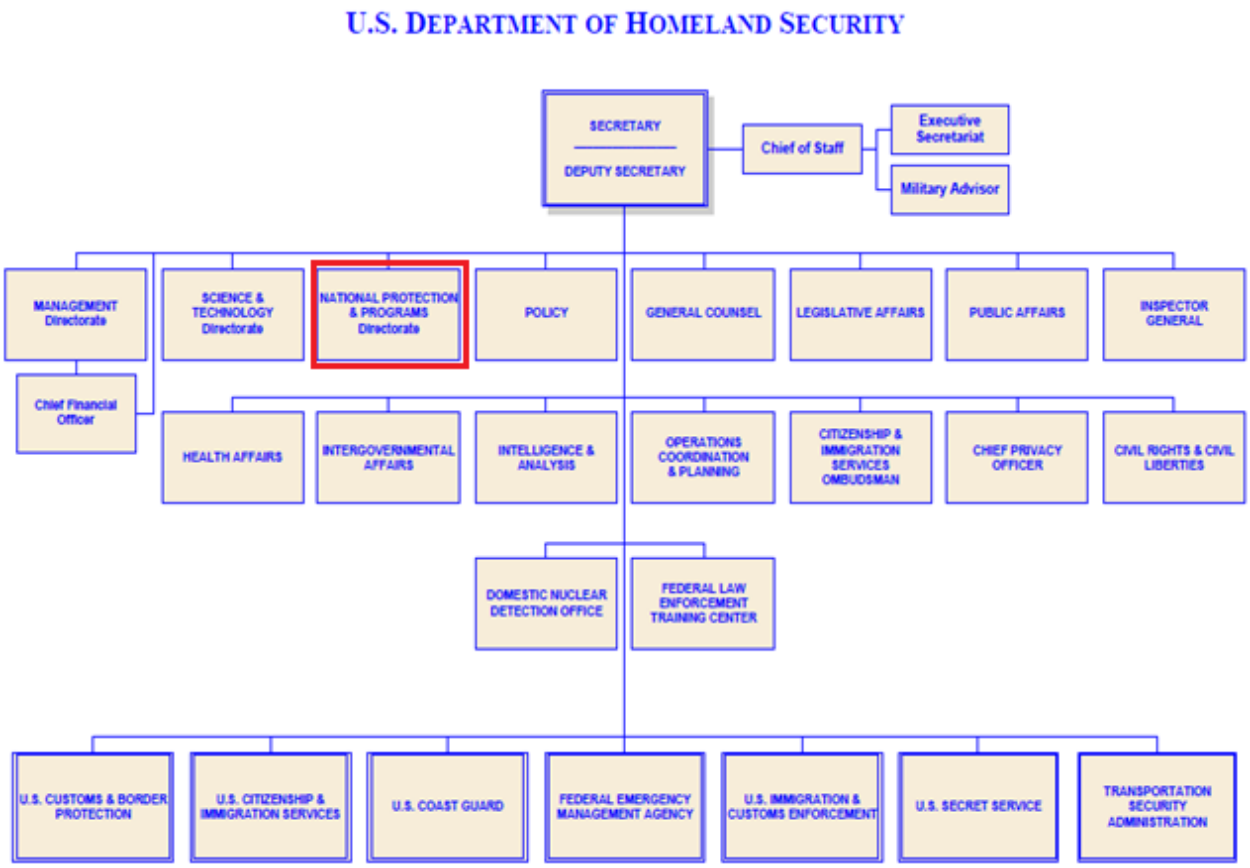


Figure 3.3 - Structure du *U.S. Department of Homeland Security*
(*U.S. Department of Homeland Security*, 2008)

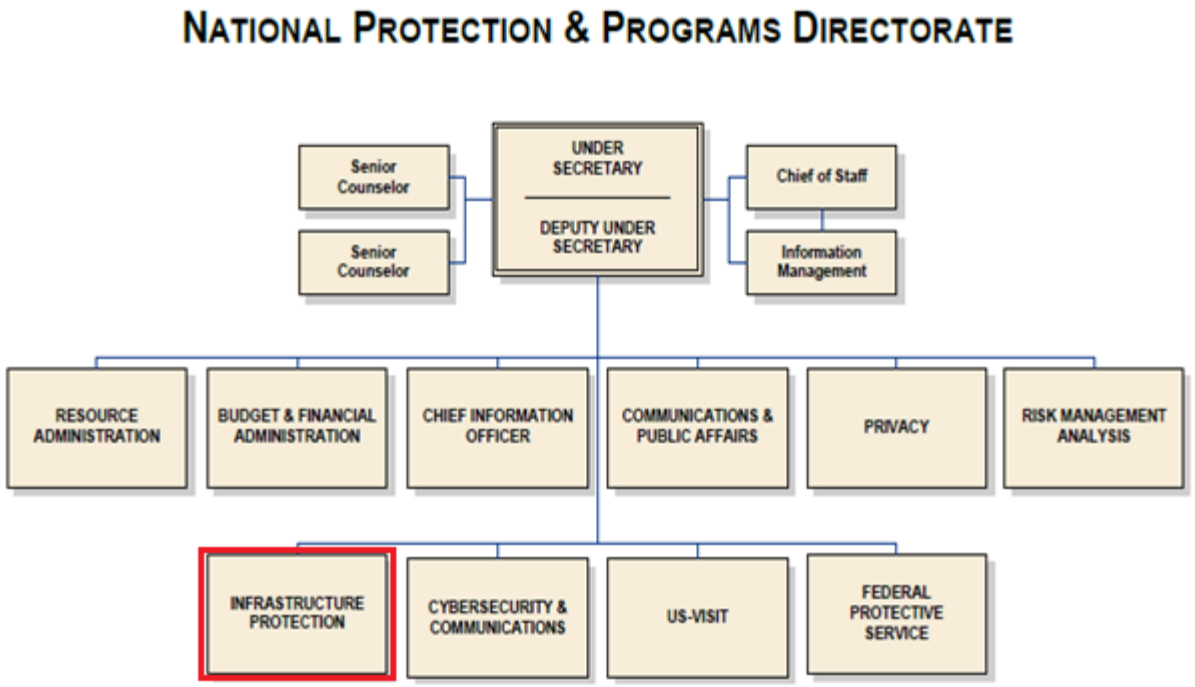


Figure 3.4 - Structure du *National Protection & Programs Directorate* (*U.S. Department of Homeland Security*, 2011)

Sous le NPDD, le DHS a créé plusieurs divisions dont l'Infrastructure *Protection* (IP). Plusieurs programmes d'évaluation des risques sous la responsabilité de l'IP du NPDD sont réalisés par différents organismes gouvernementaux dont les laboratoires nationaux de recherche tels que le *Argonne National Laboratory* et le *Los Alamos National Laboratory* qui travaillent entre autre sur la protection et la résilience des IE. Tous les échanges qui visent à collecter des informations sur les infrastructures et leurs vulnérabilités pour permettre au DHS de les utiliser à des fins d'amélioration de la protection et de la résilience des IE (tels que l'*Enhanced Critical Infrastructure Protection Security Surveys* (ECIPSS) qui vise à récolter des informations directement à partir de sondage réalisés auprès des gestionnaires des IE) sont placés sous l'égide du programme PCII et sont sous la responsabilité de l'*Infrastructure Information Collection.* La figure 3.5 présente la structure du IP (U.S. Department of Homeland Security, 2011).

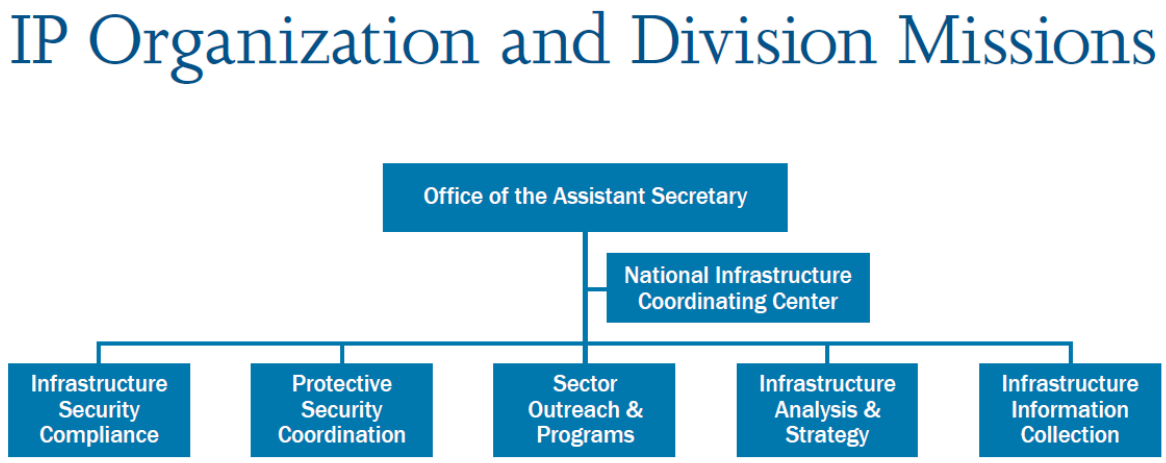


Figure 3.5 - Organisations et divisions du *Infrastructure Protection* (*U.S. Department of Homeland Security*, 2012)

Dans cette structure, la division *Infrastructure Information Collection* (IIC) mène les efforts du département concernant la gestion des informations concernant les IE. Cette division est aussi responsable de s'assurer que les données nécessaires sur les infrastructures sont disponibles aux partenaires de la sécurité civile en identifiant les sources d'information et le développement d'applications à utiliser et analyser les données. La division *Protective Security Coordination* est quant à elle responsable de développer des programmes et des initiatives visant à renforcer la protection et la résilience des IE du pays dont la réduction de la vulnérabilité des IE, l'accroissement des connaissances au niveau des interdépendances et la mise en œuvre de stratégie assurant la coordination nationale des programmes de protection des IE pour faciliter la mobilisation en situation d'urgence.

3.3.2 Modèle australien

En Australie, l'*Australian Government's Critical Infrastructure Protection Modelling and Analysis Program* (CIPMA) est une importante initiative nationale qui vise à renforcer la protection des IE et accroître leur résilience. Les objectives de cette initiative sont d'accroître la coordination entre les réseaux en situation de planification et d'intervention, de permettre aux IE de mettre en place des mesures de rétablissement réactives et flexibles et de favoriser le développement d'une culture organisationnelle visant le renforcement des capacités d'agilité et de

souplesse permettant aux organisations de s'adapter plus facilement aux situations imprévues et d'assurer la fourniture d'un niveau de service minimum pendant les interruptions, les urgences et les catastrophes (*Critical Infrastructure Resilience strategy* (CIR)) (Australian Government, 2012).

Bien que la majorité des IE en Australie soit détenue par le secteur privé, le gouvernement australien a un ensemble complexe de rôles, de responsabilités et d'intérêts dans le CIR. Dans le cadre du CIPMA, le gouvernement a mis en place le *Trusted Information Sharing Network* (TISN). Il s'agit d'un cadre d'échange d'informations confidentielles entre les IE dont la politique est basée sur le principe de confiance mutuelle. Les informations échangées dans le cadre du TISN permettent aux propriétaires et exploitants d'IE de discuter de la vulnérabilité des IE avec les agences gouvernementales concernées. Les initiatives dans le cadre de cette stratégie nationale aident les IE à mieux prévenir, se préparer, réagir et se rétablir d'un incident. La figure 3.6 montre la structure du TISN (Australian Government, 2012).

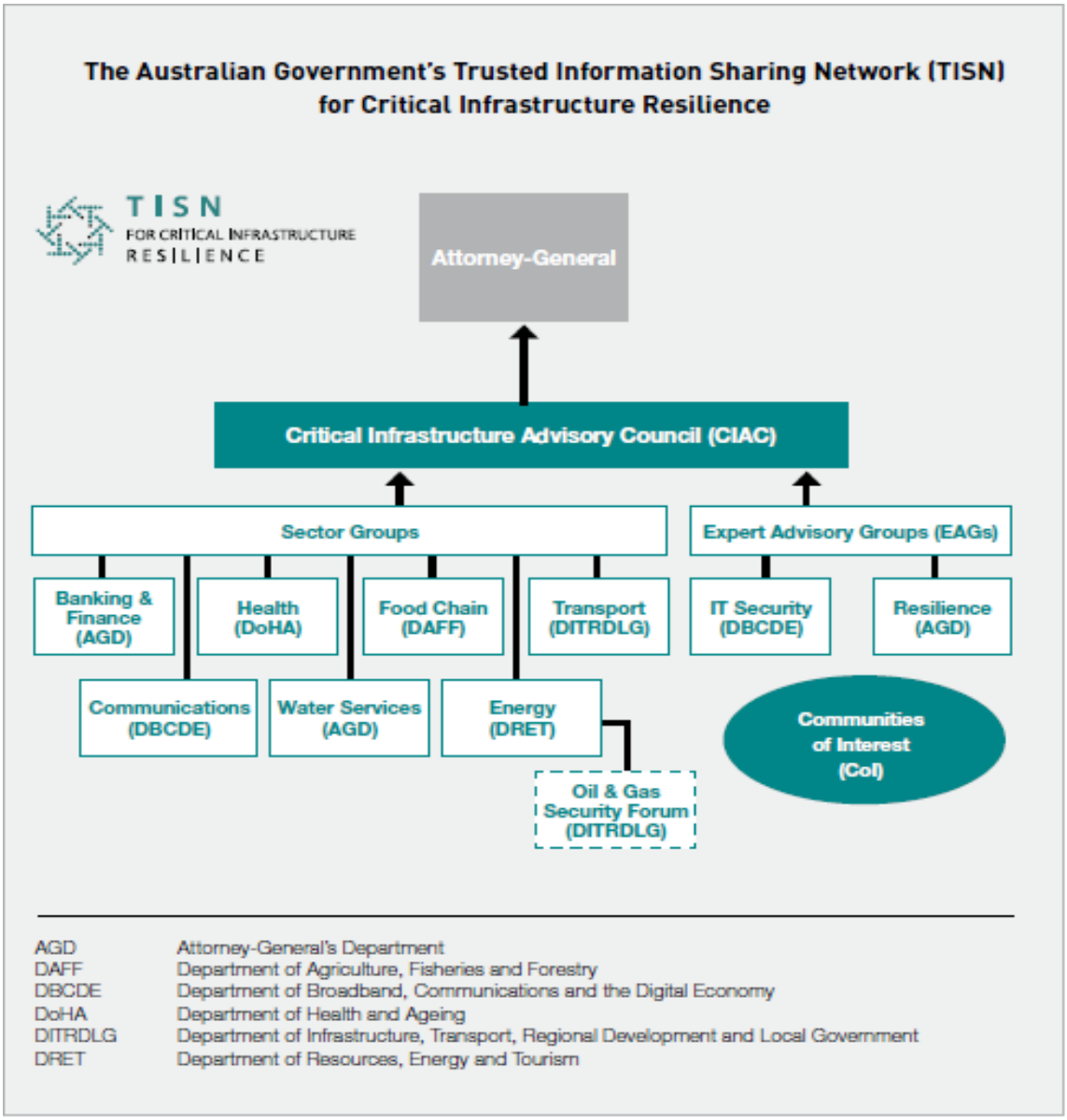


Figure 3.6 - *Trusted Information Sharing Network* du gouvernement australien (Australian Government, 2012)

Au sein de cette structure, l'*Attorney General's Department* (AGD) est l'organisme responsable de la politique des IE dans le gouvernement australien. Il coordonne la mise en œuvre de la stratégie CIR en partenariat avec un nombre d'organismes gouvernementaux australiens, et en collaboration avec l'État et le secteur privé. La mise en œuvre est réalisée à travers six impératifs

stratégiques complémentaires[7] dont le premier vise à développer des partenariats entreprise-gouvernement efficaces avec les propriétaires et exploitants d'IE et s'intègre directement dans les lignes directrices du TISN. Puisqu'une proportion importante des IE de l'Australie est détenue ou exploitée sur une base commerciale privée, un partenariat entreprise-gouvernement est nécessaire pour aider à renforcer la confiance et la fiabilité de l'exploitation continue des IE nationales. Le TISN comprend des représentants des IE nationales ainsi les représentants des États et des Territoires australiens et du gouvernement.

Dans cette structure, les groupes sectoriels (*Sector Groups*) forment le pont entre le gouvernement et les propriétaires individuels et exploitants des IE australiennes. Leur but est d'aider les propriétaires et opérateurs à partager des informations sur les questions relatives aux menaces, aux vulnérabilités et à identifier les mesures et les stratégies appropriées pour atténuer les risques associés aux interdépendances et à la défaillance des IE et renforcer les capacités de résilience au sein des organisations. Le TISN est l'élément le plus visible du partenariat entreprise-gouvernement et fournit un mécanisme important pour favoriser la coopération entre les acteurs publics et privés sur les questions mutuellement importantes (Australian Government, 2012).

Toujours dans cette structure, les *Expert Advisory Groups* (EAGs) donnent des conseils d'expertise sur les aspects généraux des IE. Ces groupes comprennent à la fois des experts de l'intérieur et de l'extérieur du TISN.

---

[7] Les six impératifs sont : (1) conduire un partenariat entreprise-gouvernement efficace avec les propriétaires et exploitants d'IE ; (2) développer et promouvoir une compréhension commune de la résilience organisationnelle ; (3) aider les propriétaires et exploitants d'IE d'identifier, d'analyser et de gérer les dépendances intersectorielles ; (4) fournir des conseils de qualité en temps opportun sur les questions relatives à la résilience des IE ; (5) mettre en œuvre la stratégie de cyber sécurité du gouvernement australien visant à maintenir un environnement d'opération électronique sécurisé, résilient et fiable ; (6) soutenir les programmes de la résilience des IE offerts par les États et territoires australiens.

Il existe aussi une série d'autres activités qui se produisent en dehors de la TISN qui soutiennent un partenariat efficace de gouvernement-entreprises. Par exemple, la fourniture de renseignements et d'autres informations liées à la sécurité, tels que les évaluations de la menace terroriste. Une grande partie de ce travail est menée par le comité national de lutte contre le terrorisme. Ce travail contribue à accroître la prise de conscience de la menace terroriste, avec un large éventail de propriétaires d'IE. Le résultat est que les propriétaires et les opérateurs sont en mesure de prendre de meilleures décisions de gestion des risques et de prendre des mesures efficaces d'atténuation des risques en réponse aux menaces (Australian Government, 2012).

3.3.3 Modèle canadien

Au Canada, le modèle de partage d'information entre les gestionnaires des IE et le gouvernement ne repose pas sur un modèle aussi précis que les modèles américain et australien, mais plutôt sur une stratégie nationale. Cette stratégie présente une approche fédérale, provinciale et territoriale globale de collaboration visant à créer des partenariats dont l'objectif est de renforcer la résilience des IE et leur permettre de faire face ensemble aux risques. Pour favoriser l'établissement de ces partenariats, la stratégie propose des mécanismes pour accroître l'échange de l'information entre les IE du Canada même si elle reconnaît que chaque partie (gouvernements, ministères, organismes et propriétaires d'IE) exerce ses responsabilités au renforcement de la résilience des IE au Canada (Sécurité Publique Canada, 2009).

La stratégie encourage la meilleure utilisation possible des mécanismes de coordination et de consultation entre les ministères et organismes fédéraux compétents, les provinces, les territoires, les associations nationales et les intervenants clés des secteurs des IE en mettant en place des réseaux sectoriels. Elle vise la promotion de l'échange de l'information, la détermination des questions d'intérêt national, régional ou sectoriel et l'élaboration d'outils et de pratiques exemplaires pour renforcer la résilience (prévention, atténuation, préparation, intervention et rétablissement) des IE.

Pour ce faire, le gouvernement canadien a créé le Forum National Intersectoriel (FNI). La figure 3.7 illustre la composition de ce forum.

Figure 3.7 - Composition du FNI
(Sécurité Publique Canada, 2009)

Composé essentiellement d'organisations des secteurs privé et public, le but du FNI est d'établir et promouvoir la collaboration entre les réseaux sectoriels dans le but de faciliter les échanges d'information. Un processus d'échange d'information amélioré et conforme aux lois et aux politiques fédérales, provinciales et territoriales devrait éventuellement venir encadrer la communication d'information utile sur les risques et sur l'état général des biens essentiels pour permettre aux parties d'évaluer les risques et de prendre les mesures appropriées. La divulgation d'information pour des motifs de sécurité nationale est déjà encadrée par des dispositions législatives fédérales provinciales et territoriales concernant l'accès à l'information utilisant un protocole commun d'échange d'information sous le sceau du secret (comme la loi sur la gestion des urgences du gouvernement du Canada de 2007 ou la loi de l'accès à l'information provinciale). Ce protocole sera élaboré dans le cadre d'une approche favorisant la collaboration,

notamment une collaboration entre tous les ordres de gouvernement. Les améliorations apportées au processus d'échange d'information comprendront notamment une gamme plus étendue de produits d'information protégés (évaluations des risques, rapports d'incident, pratiques exemplaires, leçons retenues, outils d'évaluation), de meilleurs mécanismes de diffusion (tels que des portails Internet dédiés aux informations sur les IE) et une protection accrue des renseignements échangés et des documents d'informations sur les risques contre la divulgation non autorisée.

La stratégie doit être mise en œuvre parallèlement au plan d'action sur les IE par les gouvernements (Figure 3.8). L'objectif ultime étant de favoriser la collaboration des IE et des autorités compétentes pour renforcer la résilience des IE du Canada.

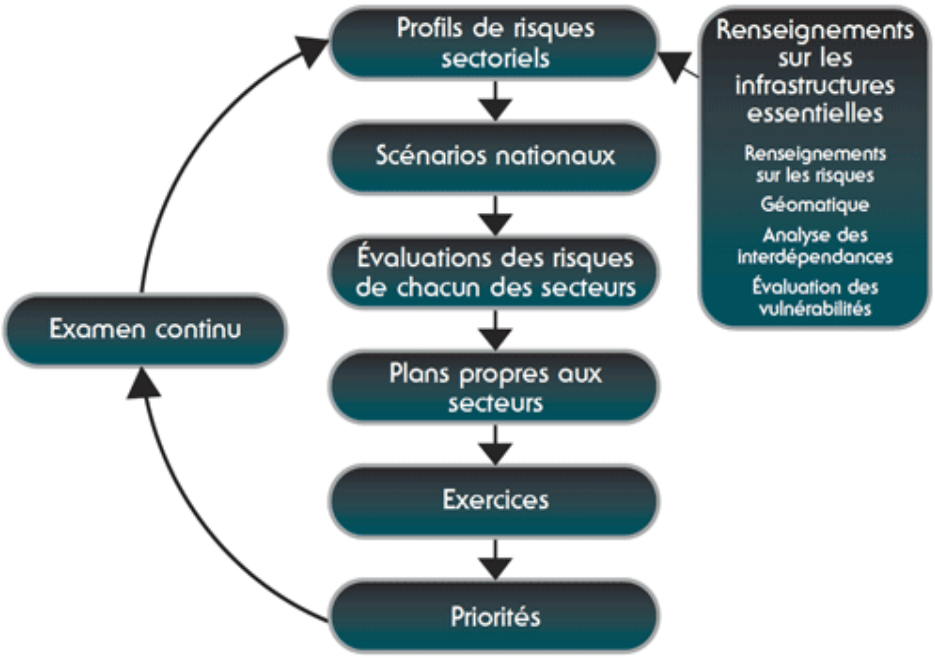


Figure 3.8 - Diagramme du plan d'action sur les IE
(Sécurité Publique Canada, 2009)

Ainsi, il existe plusieurs modèles sur lesquels il est possible de venir s'appuyer pour favoriser les échanges d'informations entre les IE. Certains sont beaucoup plus complexes que d'autres, mais

pour le Québec, il s'agit de s'inspirer de ces modèles pour venir soutenir et encadrer les efforts permettant de maintenir en vie l'espace de coopération formé par le CRP et les responsables des IE. Cette initiative importante née « de la base » grâce essentiellement à des contributions volontaires des gestionnaires d'IE locales et des responsables de la sécurité civile municipale et des contributions dans le cadre de projets de recherche universitaires ont permis de développer DOMINO : un outil intéressant qui donne un aperçu de ce qu'il est possible d'accomplir en partageant des informations privilégiées. Pour la suite de ce projet et pour maintenir les efforts visant à opérationnaliser DOMINO à grande échelle, les gestionnaires des IE ont maintenant besoin d'avoir un appui qui vienne du haut.

CHAPITRE 4 DISCUSSION

Les travaux développés dans ce mémoire sont une réponse à la problématique associée au partage d'information entre les IE et au manque d'outils concret permettant la gestion des interdépendances entre ces infrastructures. Ce chapitre vise à faire quelques recommandations en vue d'une future implémentation de DOMINO.

Sur le plan technique, il convient de rappeler que l'outil issu des travaux présentés dans ce mémoire est un prototype. Actuellement, les fonctions développées dans ce prototype ne permettent à l'utilisateur de choisir qu'une seule ressource défaillante dans un seul secteur. Par contre, il serait intéressant de connaître les ED engendrés par la panne d'une ou plusieurs ressources sur un ou plusieurs secteurs (permettre les sélections multiples). Aussi, le prototype web développé n'intègre pas le support cartographique comme le faisait la version antérieure de l'outil. Or, la possibilité de pouvoir visualiser directement sur la carte la propagation spatiale et temporelle des ED est vraiment ce qui distingue l'outil et ce qui intéresse les responsables des IE et du CSC. Le système, couplé à une carte, apporte beaucoup de précision et une meilleure compréhension des ED. Il est donc primordial de réintégrer cette possibilité dans la version web de DOMINO. Pour cela, les résultats produits par DOMINO devront être couplés à des outils géographiques qui devront être compatibles avec les outils déjà existant chez les réseaux. Idéalement, le système pourrait permettre l'interaction directement à partir de la carte.

Aussi, il faudra travailler à rendre l'outil assez flexible pour qu'il puisse être intégré aux outils déjà existants au sein des IE. Cela pour éviter que les partenaires ne se retrouvent devant plusieurs systèmes avec lesquels devoir interagir. DOMINO ne doit pas être vu comme un outil supplémentaire, mais plutôt comme un outil complémentaire. Une plus grande interaction avec le système peut être développée pour qu'il puisse s'alimenter directement à partir des systèmes en place dans les organisations. Le développement de nouvelles capacités telles que la validation des simulations en situation d'urgence serait intéressant : un partenaire pourrait confirmer ou

modifier une valeur selon la situation réelle et donner accès aux autres réseaux aux simulations modifiées en fonction de la réalité.

Une autre modification devrait être apportée au système pour tenir compte du fait qu'un utilisateur (identifié par un courriel dans le système) pourrait être responsable pour deux réseaux différents. Actuellement, le système associe une adresse courriel à un réseau. Dans une prochaine version du système, il faudra prendre en considération le fait que quelques utilisateurs peuvent être administrateurs de plusieurs réseaux et, pour cela, ils doivent avoir l'option de choisir la session sur laquelle ils veulent travailler plutôt que d'utiliser à chaque fois un courriel différent.

Finalement, dans ses futurs travaux, le CRP devra pouvoir intégrer dans DOMINO d'autres modules pour adresser d'autres problématiques tels que les aléas naturels et technologiques et les autres types d'interdépendances (logiques et cybernétiques). Le but étant de rendre DOMINO utile dans plusieurs situations pouvant conduire à la défaillance des IE et d'en faire un outil important pour le CSC et les gestionnaires d'IE (que ce soit en planification pour la réalisation d'exercice, qu'en intervention). De plus, il faudra penser à intégrer les réseaux dépendants, la population, les autres grandes IE et d'autres municipalités.

Sur le plan de l'accessibilité et de la sécurité, trois problématiques majeures sont engendrées du fait de partager les informations : l'accessibilité aux informations via internet, l'hébergement des informations et l'administration de ces informations par le gestionnaire de la BD et/ou le développeur de l'application. Le CRP a présenté aux partenaires plusieurs possibilités pour surmonter ces problématiques. Sur le plan de l'hébergement et de la connectivité, il semble que les organisations arriveront assez facilement à un consensus. Sur le plan du gestionnaire, il semble que des discussions plus profondes devront avoir lieu selon l'envergure que prendra l'opérationnalisation de DOMINO. Si DOMINO est appelé à rester un outil destiné à la ville de Montréal, alors un modèle de collaboration devra être mis de l'avant avec les responsables des IE et du CSC de Montréal pour assurer la pérennité de l'outil. Si DOMINO est appelé à avoir une portée plus nationale, alors l'implication du gouvernement par l'entremise du MSP est essentielle pour assurer la participation des IE. Les gouvernements ont la particularité d'être en mesure de

nouer de fortes relations avec les différentes entités pour aider à faciliter le partage des informations confidentielles en mettant en place des processus et des cadres législatifs promouvant ces formes de partage. Aux États-Unis, le DHS a mis en place le PCII et le NPPD dont le but est la protection d'échange d'informations volontaire entre les propriétaires et gestionnaires des infrastructures et le gouvernement. En Australie le CIPMA vise à renforcer la protection des IE de l'Australie, et d'améliorer la résilience de leur économie et leur société. Via le TISN, le gouvernement met en place des stratégies impératives pour le partage des informations confidentielles. Par contre, au Canada, il n’existe pas encore un modèle défini. Par contre une stratégie nationale est mise en place qui présentera une approche fédérale, provinciale et territoriale globale de collaboration pour renforcer la résilience des IE et qui permettra aux partenaires de faire face ensemble aux risques via un forum national intersectoriel. Plusieurs modèles sont donc disponibles et il s’agit de s’inspirer de ces modèles pour en développer un propre au Québec.

CONCLUSION

Les IE jouent un rôle critique au niveau du développement économique et social de la société. Ces systèmes complexes ont pour but de répondre aux besoins des populations et des sociétés en leur fournissant les ressources essentielles à leur bien-être et à leur fonctionnement.

Or, les IE sont caractérisées par un haut niveau d'interdépendances. De nombreux événements survenus partout autour du globe sont venus le rappeler. Les IE peuvent subir des défaillances résultantes de causes internes ou externes et, en raison de leur nature complexe et leurs interrelations, engendrer des défaillances en cascade pouvant sérieusement nuire à la population, aux activités socio-économiques ou à l'environnement. Ces interdépendances sont par conséquent une vulnérabilité pour le fonctionnement de nos sociétés et ils doivent être pris en compte dans les processus de gestion et de prévention des risques.

Le partage d'information entre les gestionnaires des IE et les responsables du CSC peut assurer une coordination entre les différentes parties prenantes et résulter en une bonne gestion des risques inhérents aux interdépendances. Dans ce contexte, le CRP a développé une méthodologie d'évaluation des interdépendances entre les IE basée sur une approche par conséquences. Cette approche de gestion des risques a été formalisée suite aux travaux menés depuis plus de 10 ans par le CRP et ont permis de développer DOMINO afin d'anticiper les ED entre les IE et rendre ces dernières moins vulnérables aux défaillances.

DOMINO est un système de modélisation des ED dont la base repose sur l'information. Cette information concerne les IE et leurs dépendances aux ressources qu'elles utilisent. Mise en commun, cette information permet d'obtenir des informations cruciales pour la gestion des risques liées aux ED. Or, pour être utilisable, cette information doit être partagée. L'objectif des travaux présentés dans ce mémoire concernaient précisément ce partage des informations confidentielles reliées aux interdépendances entre les IE.

La version Access de DOMINO ne permettait pas un partage fluide des résultats. Or, à l'ère des technologies de l'information et des communications, la réalisation de cet objectif passait assurément par le développement d'outils accessibles via l'Internet et les nouvelles applications mobiles. Ainsi, pour atteindre cet objectif, il a été nécessaire de développer la version web de DOMINO.

Le système développé au cours des travaux exposés dans ce mémoire tire son originalité du fait qu'il n'existe pas, à l'heure actuelle, un outil accessible en ligne permettant la simulation des interdépendances entre les IE et des ED résultant de la défaillance de l'une d'elles. Du moins, les recherches effectuées dans le cadre de ces travaux et celles effectuées dans le cadre des travaux du CRP n'ont pas permis de trouver de tels outils en ligne. DOMINO permet d'effectuer ce travail d'identification et d'anticipation des ED de manière automatisée. Le fait que DOMINO soit maintenant disponible en version web (éventuellement mis en ligne) permettra aux partenaires d'y accéder directement via leurs propres organisations et de l'utiliser dans leur gestion des risques.

Dans un premier temps, il a été nécessaire d'étudier les requis des clients qui sont les futurs utilisateurs du système et d'établir l'analyse fonctionnelle et la gestion des accès au système. Par la suite, en se basant sur le concept de la BD développée lors de travaux précédents, il a fallu modifier cette BD pour l'adapter aux besoins des futurs utilisateurs du système et l'optimiser pour une meilleure analyse des résultats. Une fois la nouvelle BD conçue puis établie, plusieurs étapes ont été nécessaires pour mener au développement du prototype DOMINO web. La conception du système a été définie et le développement a été fait en utilisant PHP et MySQL de concert avec plusieurs autres langages secondaires pour la génération des rapports, des graphes et la dynamique de l'interface.

Pour s'assurer du bon fonctionnement du prototype développé et pour valider son utilisation et les problèmes qui en sont reliés, le prototype a été soumis à une phase de tests et de validation. Une première phase de validation (à l'interne du CRP) a permis de valider le bon fonctionnement de l'outil et la justesse des résultats qu'il produit. Une deuxième phase de validation (auprès des

partenaires) a permis de soulever quelques-uns des nombreux défis qui devront être soulevés avant de rendre une telle application réellement opérationnelle sur une municipalité. Ces défis traitent principalement de l'équilibre à rechercher entre accessibilité et confidentialité. Les différentes problématiques qui sont entrevues pour une implémentation future de l'outil ont été exposées devant les partenaires pour en tirer leurs principales recommandations. De nombreuses remarques ont été formulées par ces derniers, au niveau de la sécurité des données contenues dans la BD et de la gestion éventuelle d'un tel outil. Celles-ci devront être adressées par le CRP dans le cadre d'un futur projet visant l'implémentation de DOMINO dans la ville de Montréal et devront conduire à un cadre de travail formel assurant la pérennité de l'outil. La participation des nombreux partenaires du CRP et l'implication du MSP seront nécessaires à la réussite de l'implémentation de DOMINO à Montréal et, éventuellement, dans d'autres municipalités du Québec.

RÉFÉRENCES

ASSOCIATED PRESS (2011), « Les exportations japonaises au ralenti », La Presse, 20 Avril 2011, [En ligne] http://affaires.lapresse.ca/dossiers/seisme-au-japon/201104/20/01-4391849-les-exportations-japonaises-au-ralenti.php, (Page consultée le 5 Janvier 2013).

BARRON, J. & GOODMAN, J.D. (2012), "Northeast awakes to huge damage in storm's path: Millions without power"•, The New York Times, 30 Octobre 2012, [En ligne], http://soundofheart.org/galacticfreepress/content/northeast-awakes-huge-damage-storm%E2%80%99s-path-millions-without-power, (Page consultée le 9 Janvier 2013).

BOIN, A., LAGADEC, P., MICHEL-KERJAN, E. & OVERDIJK, W. (2003) 'Critical infrastructures under threat: learning from the anthrax scare', Journal of Contingencies and Crisis Management, Vol. 11, No. 3, pp.99–104.

BUREAU DE LA PROTECTION DES INFRASTRUCTURES ESSENTIELLES ET DE LA PROTECTION CIVILE. (2003). Infrastructures essentielles nationales. Bureau de la protection des infrastructures essentielles et de la protection civile, Division de la recherche et du développement. Site Internet du Portefeuille des Transports, de l'infrastructure et des Collectivités [En ligne], Canada.
http://www.infc.gc.ca/research-recherche/result/alt_formats/pdf/ocipep_f.pdf (consulté le 30 juin 2011).

CHOSSUDOVSKY, M. (2012), “Fukushima: A Nuclear War without a War: The Unspoken Crisis of Worldwide Nuclear Radiation” • , Global research online interactive reader series, I-Book No. 3, 25 Janvier 2012, [En ligne] http://www.globalresearch.ca/fukushima-a-nuclear-war-without-a-war-the-u unspoken-crisis-of-worldwide-nuclear-radiation/28870 (Page consultée le 17 Janvier 2013).

ETTORE MERLO, DOMINIC LETARTE, & GIULIANO ANTONIOL. Automated Protection of PHP Applications Against SQL-Injection Attacks. In , volume CSMR, Amsterdam, the Netherlands, pages 191-202, March 21-23 2007. IEEECOMPSP. [doi:10.1109/CSMR.2007.16]

GALLAGHER, S. & NEUGEBAUER, M. Critical infrastructure information sharing. Tiré de http://www1.maxwell.syr.edu/uploadedFiles/campbell/events/GallagherNeugebauer.pdf

GOLDSTEIN, J. & HAUSER, C. (2012), “As recovery continues, City’s death toll reaches 38”, The New York Times, 1er Novembre 2012, [En ligne] http://www.nytimes.com/2012/11/02/nyregion/after-hurricane-sandy-a-difficult-commute-in-new-york.html?pagewanted=all&_r=0, (Page consultée le 11 Janvier 2013).

GOMEZ-URBINA, A. (2007). Le pishing et les vulnérabilités sur Internet. In D. Li (dir.), Hacking Interdit. (2e édition, pp. 700-1000). Micro Application, ISBN10 : 2742963022

KRUTZ, R. L. (2006). Securing SCADA systems. John Wiley & Sons, Indianapolis, États-Unis, p 238.

MACCHIA, J.R. (2012), “Fukushima. Le tsunami. Puis la catastrophe nucléaire. Un an après, le point sur les conséquences dans l’industrie automobile », France Info, 9 mars 2012.

MARTI, J. R., VENTURA, C. E., HOLLMAN, J. A., SRIVASTAVA, K. D. & JUÁREZ, H. (2007), I2Sim Modelling and Simulation Framework for Scenario Development, Training, and Real-Time Decision Support of Multiple Interdependent Critical Infrastructures during Large Emergencies. The University of British Columbia. Tiré de http://www.i2sim.ca/

MUFSON, S. (2012), "Nuclear power reactors shut down during hurricane Sandy", The Washington Post, 30 Octobre 2012, [En ligne] http://articles.washingtonpost.com/2012-10-30/business/35498621_1_water-intake-structure-oyster-creek-nrc, (Page consultée le 9 Janvier 2013).

NICOLET, R., TRUDEAU, N., DENIS, H., BERNIER, C., CLOUTIER, L., DICAIRE, A. & AL. (1999). Pour affronter l'imprévisible: les enseignements du verglas de 98. Rapport de la Commission scientifique et technique chargée d'analyser les évènements relatifs à la tempête de verglas survenue du 5 au 9 janvier 1998 (442 p.), Canada, Les Publications du Québec.

PARFOMAK, P. W. (2005), « Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options », Washington, Congressional Research Service, The Library of Congress.

RINALDI, S. M., PEERENBOOM, J. & KELLY, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine, Vol. 21, pp. 11-25, 2001.

ROBERT, B., MORABITO, L. & QUENNEVILLE, O. (2007). The preventive approach to risks related to interdependent infrastructures. International Journal of Emergency Management, Vol. 4, No. 2, pp. 166-182.

ROBERT, B. & MORABITO, L. (2008) 'The operational tools for managing physical interdependencies among critical infrastructures', Int. J. Critical Infrastructures, Vol. 4, No. 4, pp.353–367.

ROBERT, B. & MORABITO, L. (2010) 'An approach to identifying geographic interdependencies among critical infrastructures', Int. J. Critical Infrastructures, Vol. 6, No. 1, pp.17–30.

ROBERT, B. & MORABITO, L. (2011) 'Reducing vulnerability of critical infrastructures: Methodological manual', Presses Internationales Polytechnique, ISBN 978-2-553-01597-7, 2011, 67 pages.

ROBERT, B. & MORABITO, L. (2012) 'Modeling interdependencies among critical infrastructures', Conference on critical infrastructure and cybersecurity, Ottawa, Canada, June 7-8, 2012.

ROBERT, B., DE CALAN, R. & MORABITO, L. (2008) 'Modelling interdependencies among critical infrastructures', Int. J. Critical Infrastructures, Vol. 4, No. 4, pp.392–408.

ROBERT, B., MORABITO, L. & CLOUTIER, I. (2012) 'Modeling and coordinating interdependent critical infrastructures in Montréal', CIP report, May 2012, p. 3-6.

ROBERT, B., MORABITO, L. & DEBERNARD, C. (2012) 'Simulation and anticipation of domino effects among critical infrastructures', Accepted for publication into the Int. J. Critical Infrastructures.

SÉCURITÉ PUBLIQUE CANADA. (2004). Énoncé de position du gouvernement du Canada relativement à une stratégie nationale pour la protection des infrastructures essentielles. Canada, Sécurité Publique Canada. Site internet de l'Association Canadienne des Eaux Potables et Usées [En ligne], Canada. http://www.cwwa.ca/pdf_files/CIP%20position%20paper_FRE.pdf (consulté le 18 septembre 2012).

SÉCURITÉ PUBLIQUE CANADA. (2006). Panne d'électricité en Ontario et aux États-Unis - Impacts sur les infrastructures essentielles : Analyse d'incident. Canada: Sécurité Publique Canada. Site internet du Ministère de la Sécurité Publique Canada [En ligne], Canada. http://www.publicsafety.gc.ca/prg/em/_fl/ont-us-power-f.pdf (consulté le 2 Octobre 2012).

SÉCURITÉ PUBLIQUE CANADA. (2009). Aller de l'avant avec la stratégie nationale et le plan d'action pour les infrastructures essentielles (p. 38). Sécurité Publique Canada. Site internet du Ministère de la Sécurité Publique Canada [En ligne], Canada. http://www.securitepublique.gc.ca/prg/em/cip/_fl/nat-strat-critical-infrastructure-fra.pdf (consulté le 5 août 2012).

SERINO, R. (2013), "Lessons from Sandy: A Word on Innovation"•, Federal Emergencu Management Agency, US Department of Homeland Security, 15 janvier 2013, [En ligne] http://www.fema.gov/blog/2013-01-15/lessons-sandy-word-innovation?goback=, (Page consultée le 21 Janvier 2013).

THE PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION. (1997). Critical Foundations: Protecting America's Infrastructures: The report of the president's commission on critical infrastructure protection. Etats-Unis, Government Printing Office 040-000-00699-1. Site Internet de la Federation of American Scientists [En ligne], États-Unis. http://www.fas.org/sgp/library/pccip.pdf (consulté le 20 Décembre 2011)

AUSTRALIAN GOVERNMENT (2012), TRUSTED INFORMATION SHARING NETWORK (TISN) [En ligne]. Disponible: http://www.tisn.gov.au. (Consulté le 25 Janvier 2013).

UNITED STATES DEPARTMENT OF ENERGY AND NATURAL RESOURCES CANADA (US DOE and NRC) (2004) 'Final report on the August 14, 2003 blackout in the United States and Canada: causes and recommendations', April, [online].

U.S. DEPARTMENT OF HOMELAND SECURITY (DHS) [En ligne]. Disponible: http://www.dhs.gov/. [Consulté le 20 Janvier 2013].

ANNEXE – INTERFACES DU SYSTÈME DOMINO WEB

CENTRE RISQUE & PERFORMANCE

Accueil | À propos du CRP | Interdépendances des IE | Publications | Aspects Juridiques | Plan du site | Contactez-nous

Bienvenue dans DOMINO

CENTRE RISQUE & PERFORMANCE

Le Centre risque & performance (CRP) préconise une approche par conséquences qui offre une vision globale et multidisciplinaire du risque. Par l'évaluation des conséquences potentielles liées à la dégradation d'une ressource ou la défaillance d'une infrastructure essentielle, le CRP se démarque des démarches classiques d'analyse de risques. Il répond directement aux besoins de ses partenaires publics et privés en développant des outils de planification des mesures d'urgence, de continuité opérationnelle et d'évaluation de la résilience organisationnelle.

L'évaluation des risques et leur intégration dans les mécanismes de gestion sont des problématiques en pleine émergence tant au Québec, au Canada que partout dans le monde. Dans ce vaste champ d'application, le CRP concentre ses travaux de recherche aux infrastructures essentielles représentées, entre autres, par les réseaux d'électricité, de gaz naturel, d'eau potable, d'eaux usées, de télécommunications et de transports.

DOMINO

DOMINO est un prototype de système de gestion des interdépendances et d'analyse des effets domino qui vise à évaluer la propagation dans le temps et l'espace des conséquences néfastes sur les réseaux d'une situation pouvant engendrer un effet domino. Le fonctionnement de l'outil repose sur une approche de gestion des risques basée sur les conséquences d'un événement perturbeur sans, à priori, s'attarder aux causes ayant menées à cet événement. Constitué d'une base de données liée à un système d'information géographique, DOMINO est un outil qui comprend plusieurs modules qui permettent des utilisations autant pour les gestionnaires des réseaux que pour les responsables de la sécurité civile. Il traite les interdépendances fonctionnelles en analysant les relations de type client/fournisseur existantes entre les réseaux. C'est un outil de planification et d'aide à la décision.

ACCÉDER À DOMINO

Copyright © 2013 École Polytechnique de Montréal - Centre risque & performance. Tous droits réservés.

CENTRE RISQUE & PERFORMANCE

Accueil | À propos du CRP | Interdépendances des IE | Publications | Aspects Juridiques | Plan du site | Contactez-nous

Ouvrir une session Domino

Utilisateur:

Mot de passe:

Entrer

Seules les personnes dûment autorisées peuvent accéder à DOMINO.
Pour demander un accès, veuillez communiquer avec nous à l'adresse ci-bas.
Veuillez noter que la demande d'un accès ne garantit pas qu'il sera accordé.

Pour demander un accès: benoit.robert@polymtl.ca

Copyright © 2013 École Polytechnique de Montréal - Centre risque & performance. Tous droits réservés.

CENTRE RISQUE & PERFORMANCE

Session de Bell Admin
Fermer la session

Retour au Menu Principal

Intérdependances des Infrastructures Essentielles

Interdépendances fonctionnelles | Interdépendances géographiques | Interdépendances logiques | Risques naturels et technologiques

Informations sur les infrastructures
- Infrastructures localisées dans un secteur
- Infrastructures appartenant à votre réseau
- Infrastructures des autres réseaux qui utilisent vos ressources
  - Dans un secteur
  - Dans une zone d'alimentation

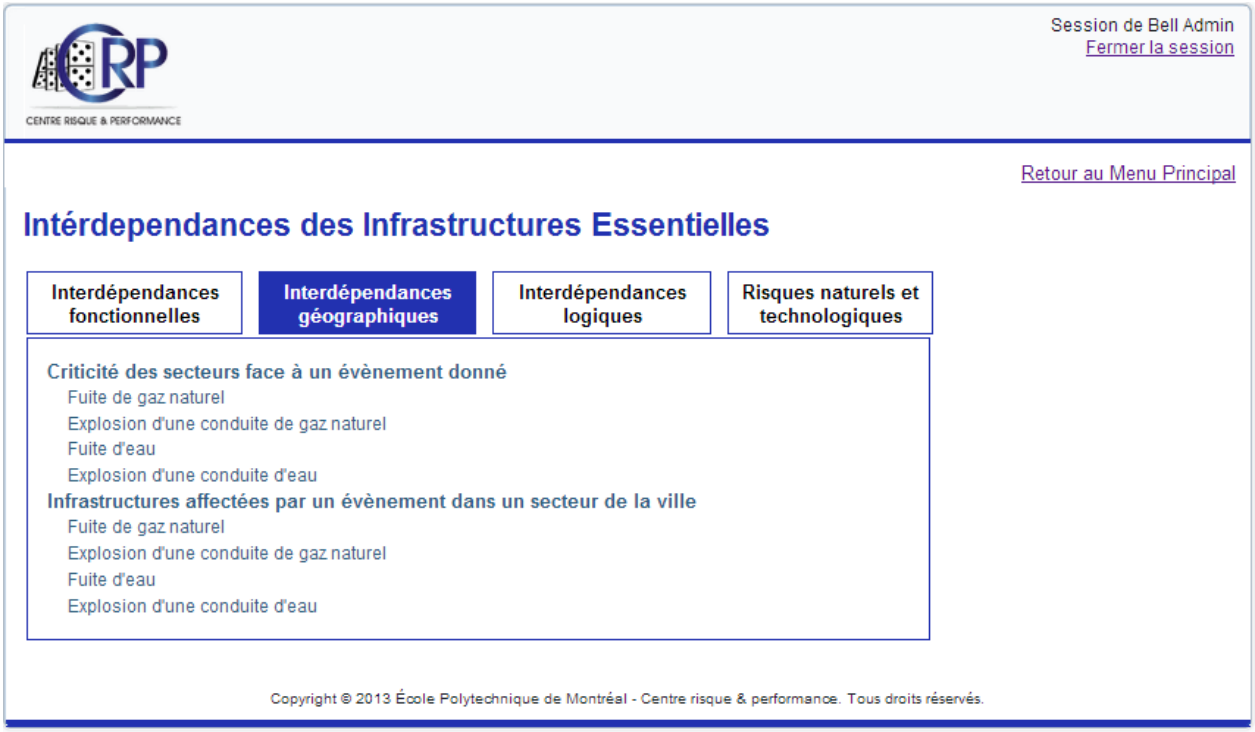
Informations sur les ressources
- Ressources utilisées
  - Par une infrastructure d'un réseau
  - Par un réseau dans un secteur
  - Par un réseau dans une zone d'alimentation
- Dépendance de votre réseau face à une ressource
  - Dans un secteur
  - Dans une zone alimentation
  - Sous forme de courbe

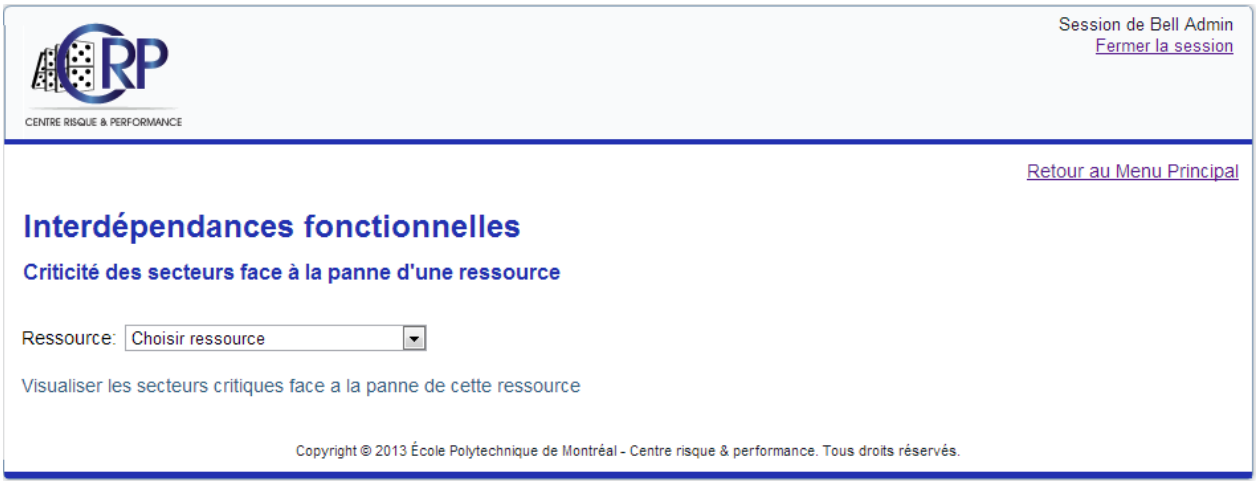
Analyse de dépendances et vulnérabilités
- Criticité des secteurs face à la panne d'une ressource

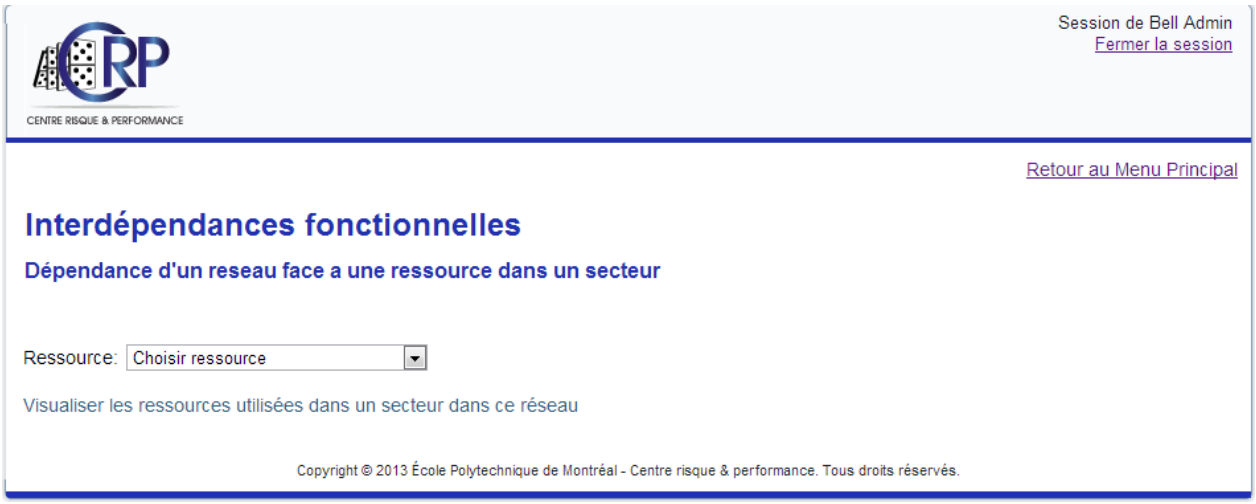
Analyse des effets domino

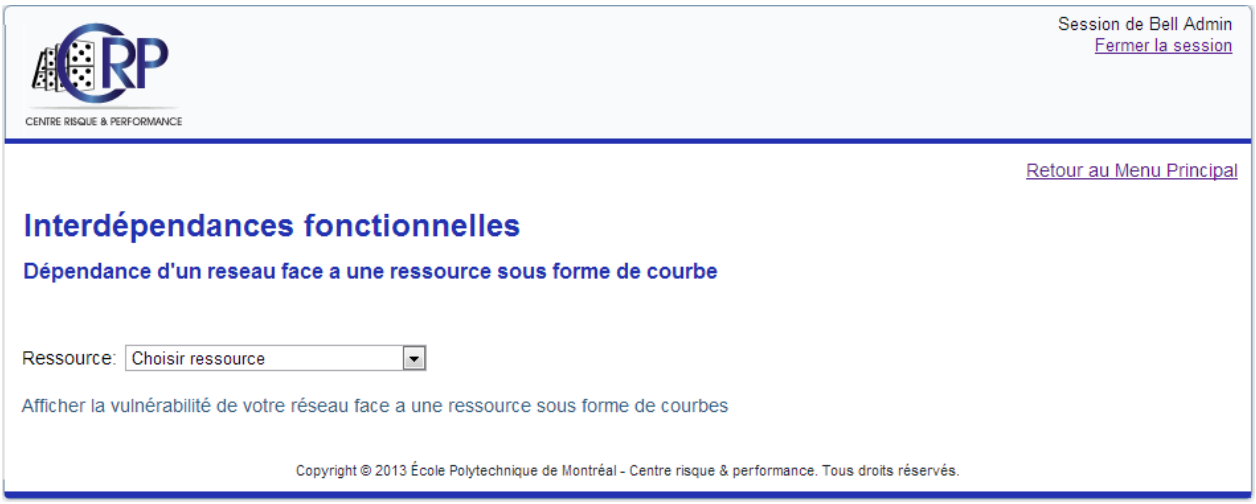
Copyright © 2013 École Polytechnique de Montréal - Centre risque & performance. Tous droits réservés.

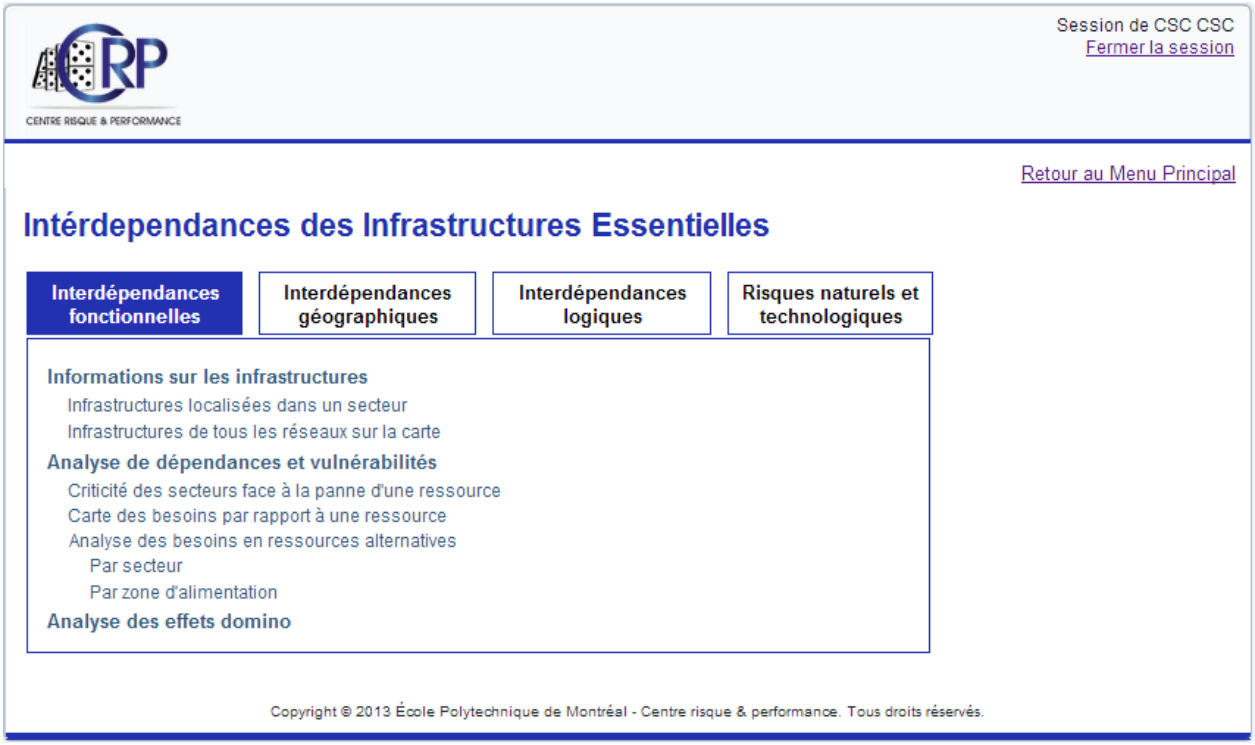
CENTRE RISQUE & PERFORMANCE
Session de CSC CSC
Fermer la session
Retour au Menu Principal
Interdépendances fonctionnelles
Effets Domino - Infrastructures dépendantes
Ressource: Eau de service
Secteur: AH24
Simuler les effets domino
Copyright © 2013 École Polytechnique de Montréal - Centre risque & performance. Tous droits réservés.

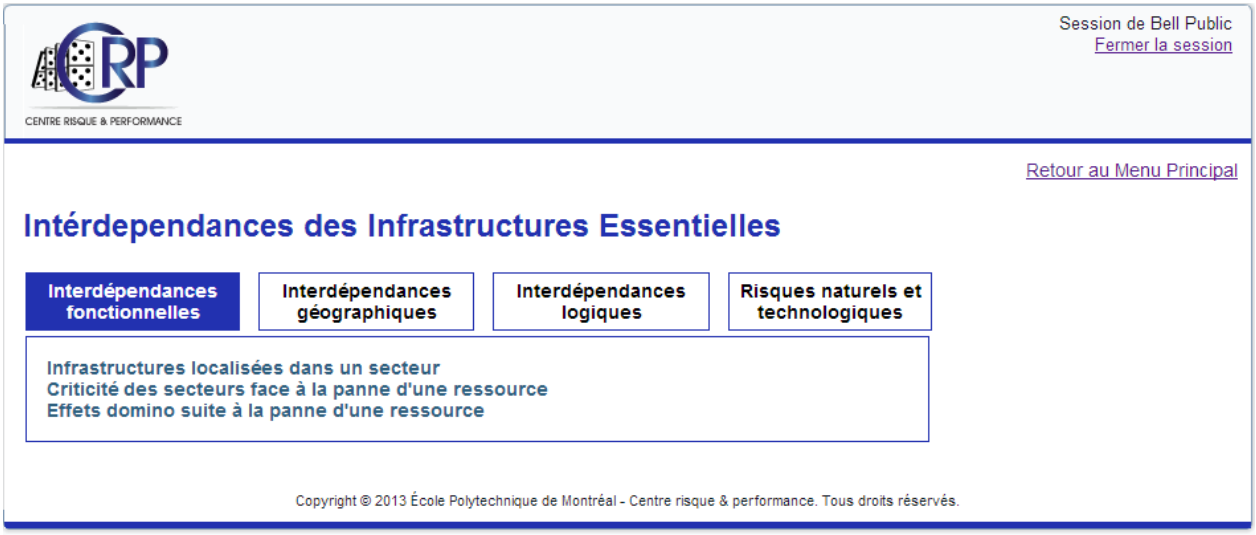

CENTRE RISQUE & PERFORMANCE
Session de Bell Admin
Fermer la session
Retour au Menu Principal
Intérdependances des Infrastructures Essentielles
Interdépendances fonctionnelles
Interdépendances géographiques
Interdépendances logiques
Risques naturels et technologiques
Criticité des secteurs face à un évènement donné
Fuite de gaz naturel
Explosion d'une conduite de gaz naturel
Fuite d'eau
Explosion d'une conduite d'eau
Infrastructures affectées par un évènement dans un secteur de la ville
Fuite de gaz naturel
Explosion d'une conduite de gaz naturel
Fuite d'eau
Explosion d'une conduite d'eau
Copyright © 2013 École Polytechnique de Montréal - Centre risque & performance. Tous droits réservés.


CENTRE RISQUE & PERFORMANCE
Session de Bell Admin
Fermer la session
Retour au Menu Principal
Interdépendances fonctionnelles
Criticité des secteurs face à la panne d'une ressource
Ressource: Choisir ressource
Visualiser les secteurs critiques face a la panne de cette ressource
Copyright © 2013 École Polytechnique de Montréal - Centre risque & performance. Tous droits réservés.


CENTRE RISQUE & PERFORMANCE
Session de Bell Admin
Fermer la session
Retour au Menu Principal
Interdépendances fonctionnelles
Dépendance d'un reseau face a une ressource dans un secteur
Ressource: Choisir ressource
Visualiser les ressources utilisées dans un secteur dans ce réseau
Copyright © 2013 École Polytechnique de Montréal - Centre risque & performance. Tous droits réservés.


CENTRE RISQUE & PERFORMANCE
Session de Bell Admin
Fermer la session
Retour au Menu Principal
Interdépendances fonctionnelles
Dépendance d'un reseau face a une ressource sous forme de courbe
Ressource: Choisir ressource
Afficher la vulnérabilité de votre réseau face a une ressource sous forme de courbes
Copyright © 2013 École Polytechnique de Montréal - Centre risque & performance. Tous droits réservés.


CENTRE RISQUE & PERFORMANCE
Session de CSC CSC
Fermer la session
Retour au Menu Principal
Intérdependances des Infrastructures Essentielles
Interdépendances fonctionnelles
Interdépendances géographiques
Interdépendances logiques
Risques naturels et technologiques
Informations sur les infrastructures
Infrastructures localisées dans un secteur
Infrastructures de tous les réseaux sur la carte
Analyse de dépendances et vulnérabilités
Criticité des secteurs face à la panne d'une ressource
Carte des besoins par rapport à une ressource
Analyse des besoins en ressources alternatives
Par secteur
Par zone d'alimentation
Analyse des effets domino
Copyright © 2013 École Polytechnique de Montréal - Centre risque & performance. Tous droits réservés.


CENTRE RISQUE & PERFORMANCE
Session de Bell Public
Fermer la session
Retour au Menu Principal
Intérdependances des Infrastructures Essentielles
Interdépendances fonctionnelles
Interdépendances géographiques
Interdépendances logiques
Risques naturels et technologiques
Infrastructures localisées dans un secteur
Criticité des secteurs face à la panne d'une ressource
Effets domino suite à la panne d'une ressource
Copyright © 2013 École Polytechnique de Montréal - Centre risque & performance. Tous droits réservés.

Enregistrement

Les champs avec * sont obligatoires

Nom *

Nom

Prénom

Courriel *

Mot de Passe *

Le mot de passe doit contenir au moins 1 lettre majuscule, 1 lettre minuscule et 1 chiffre. 6 caracteres minimum

Confirmer Mot de Passe *

Niveau *

Choisir Niveau

Ville *

Choisir ville

Téléphone au Bureau *

Exemple: 5142124564 poste 4012

Téléphone Cellulaire

Chiffres seulement

Téléavisateur

Chiffres seulement

Submit

Retour a la Accueil

Generated by pForm

DOMINO Admin

Fermer la session

Home | Réseaux | Infrastructures | Zones | Secteurs | Types de Ressources | Ressources Alternatives | Ressources

Gestion des Réseaux

Informations sur Réseaux

Nom *

Status Activf Inactif

Ajouter Personne Contact

Utilisateur : Choisir Utilisateu

Classification : Choisir Classifica

Ajouter une autre personne contact

Save

Gestion des Infrastructures

Informations sur les Infrastructures

Nom *

Réseau * Choisir Réseau

Zone * Choisir Zone

Secteur * Choisir Secteur

No Civique *

Troncon *

Code Postal *

Latitude *

Longitude *

Fonction réalisée *

Aerienne Oui Non

Au sol Oui Non

Souterraine Oui Non

Immergée Oui Non

Vulnérable à une fuite de Gaz Oui Non

Vulnérable à une explosion de Gaz Oui Non

Vulnérable à une fuite d'eau Oui Non

Vulnérable à une explosion d'une conduite d'eau Oui Non

Save

Gestion des Ressources

Informations sur les Ressources

Type de Ressource * Choisir Type de Ressource

Infrastructure * Choisir Infrastructure

Zone Choisir Zone

Période du besoin *

Control Affecté * Oui Non

Mission Affectée * Oui Non

Voie approvisionnement de Ressource *

Stockage *

Autonomie maximale de stockage *

Mode de gestion alternatif * Oui Non

Code EWS

Valeur confirmée Oui Non

Bleu Jaune Orange Rouge

Valeur temporaire confirmée Oui Non

Bleu Jaune Orange Rouge

Ajouter autre Mode de Gestion

Mode Gestion : Type Mode Gestion : Equipment requis : Oui Non Nom Equipment :

Code EWS

Valeur confirmée ◉ **Oui** ○ **Non**

Bleu | Jaune | Orange | Rouge

Valeur temporaire confirmée ◉ **Oui** ○ **Non**

Bleu | Jaune | Orange | Rouge

Ajouter autre Mode de Gestion

Mode Gestion : | Type Mode Gestion : | Equipment requis : ○ **Oui** ○ **Non** | Nom Equipment :

Voie Approvisionnement Equipement : | Equipment Zone Transport : | Resource Alternative requise : ○ **Oui** ○ **Non** | Ressource Alternative : Choisir Ressourc

Voie Approvisionnement de Ressource : | Resource Zone Alimentation ou Transport : | Stockage : ○ **Oui** ○ **Non** | Quantitee Stockee :

Quantite Necessaire : | Autonomie de Stockage : | Viabilite Mode de Gestion : | Autre Mode de Gestion : ○ **Oui** ○ **Non**

Lien entre Modes de Gestion :

Delete

Mode Gestion : | Type Mode Gestion : | Equipment requis : ○ **Oui** ○ **Non** | Nom Equipement :

Voie Aprovisionnement Equipement : | Equipement Zone Transport : | Ressource Alternative Requise : ○ **Oui** ○ **Non** | Resource Alternative : Choisir Ressourc

Voie Approvisionnement Ressource : | Resource Zone Alimentation ou Transport : | Stockage : ○ **Oui** ○ **Non** | Quantité Stockée :

Quantité Nécessaire : | Autonomie Stockage : | Viabilité Mode Gestion : | Autre Mode de Gestion : ○ **Oui** ○ **Non**

Lien entre Modes de Gestion :

Ajouter autre mode de gestion

Save